Audit Report

OIG-20-003

INFORMATION TECHNOLOGY: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2019 Performance Audit

October 25, 2019

Office of Inspector General

Department of the Treasury

This Page Intentionally Left Blank

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 25, 2019

MEMORANDUM FOR **DAVID F. EISNER**
ASSISTANT SECRETARY FOR MANAGEMENT

ERIC OLSON
DEPUTY ASSISTANT SECRETARY FOR INFORMATION SYSTEMS AND CHIEF INFORMATION OFFICER

FROM: Larissa Klimpel /s/
Director, Cyber/Information Technology Audit

SUBJECT: Audit Report – *Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2019 Performance Audit*

The purpose of this memorandum is to transmit the following reports:

- *Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2019 Performance Audit*, dated October 25, 2019, (Attachment 1); and

- *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*, dated September 24, 2019 (Attachment 2).

The Federal Information Security Modernization Act of 2014 (FISMA) requires that Federal agencies have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices, and to report the results to the Office of Management and Budget (OMB). OMB delegated its responsibility to the Department of Homeland Security (DHS) for the collection of annual FISMA responses. FISMA also requires that the agency Inspector General (IG) or an independent external auditor perform the annual evaluation as determined by the IG.

To meet our FISMA requirements, we contracted with KPMG LLP (KPMG), a certified independent public accounting firm, to perform this year's annual FISMA audit of Treasury's unclassified systems, except for those of the Internal Revenue

Service (IRS), which were evaluated by the Treasury Inspector General for Tax Administration (TIGTA). KPMG conducted its audit in accordance with generally accepted government auditing standards. In connection with our contract with KPMG, we reviewed its report and related documentation and inquired of its representatives. Our review, as differentiated from an audit performed in accordance with generally accepted auditing standards, was not intended to enable us to conclude on the effectiveness of Treasury's information security program or its compliance with FISMA. KPMG is responsible for its report and the conclusions expressed therein.

In brief, KPMG reported that consistent with applicable FISMA requirements, OMB policy and guidance, and the National Institute of Standards and Technology (NIST) standards and guidelines, Treasury's information security program and practices for its unclassified systems were established and have been maintained for the 5 Cybersecurity Functions and 8 FISMA program areas. However, the program was not effective according to DHS criteria and as KPMG identified 4 deficiencies within 1 of the 5 Cybersecurity Functions and within 4 of the 8 FISMA program areas. Accordingly, KPMG made 14 recommendations to the responsible officials to address the identified deficiencies.

With respect to IRS's unclassified systems, TIGTA reported that IRS's information security program generally aligned with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines. However, due to program components not being at an acceptable maturity level, IRS's information security program was not fully effective.

Appendix III of the attached KPMG report includes *Department of the Treasury's Consolidated Response to DHS's FISMA 2019 Questions for Inspectors General*.

If you have any questions or require further information, you may contact me at (202) 927-0361.

Attachments

ATTACHMENT 1

Department of the Treasury
Federal Information Security Modernization Act
Fiscal Year 2019 Performance Audit
October 25, 2019

This Page Intentionally Left Blank

Department of the Treasury
Federal Information Security Modernization Act
Fiscal Year 2019 Performance Audit

October 25, 2019

KPMG LLP
8350 Broad Street, Suite 900
McLean, VA 22102

Department of the Treasury
Federal Information Security Modernization Act
Fiscal Year 2019 Performance Audit

Table of Contents

FISMA Performance Audit Report

Contents

KPMG LLP
Suite 900
8350 Broad Street
McLean, VA 22102

Richard K. Delmar
Acting Inspector General
Department of the Treasury
1500 Pennsylvania Avenue NW
Room 4436
Washington, DC 20220

Re: Department of the Treasury's Federal Information Security Modernization Act Fiscal Year 2019 Performance Audit

Dear Mr. Delmar:

This report presents the results of our independent performance audit of the Department of the Treasury's (Treasury or Department) information security program and practices for its unclassified systems. The Federal Information Security Modernization Act of 2014 (FISMA) requires Federal agencies, including Treasury, to have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices, and to report the results of the evaluations to the Office of Management and Budget (OMB). The Department of Homeland Security (DHS) is responsible for the operational aspects of Federal cyber security, such as establishing government-wide incident response and operating CyberScope[1] to collect FISMA responses. Appendix III, *Department of the Treasury's Consolidated Response to DHS's FISMA 2019 Questions for Inspectors General*, provides Treasury's response to the CyberScope questionnaire. We also considered applicable OMB policy and guidelines and the National Institute of Standards and Technology (NIST) standards and guidelines. FISMA requires that the agency Inspector General (IG) or an independent external auditor perform the annual evaluation as determined by the IG. The Treasury Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct an audit of Treasury's information security program and practices for its unclassified systems.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS).[2] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objective for this performance audit was to assess the effectiveness of Treasury's information security program and practices for its unclassified systems for the period July 1, 2018 through June 30, 2019. We performed our fieldwork from April 23, 2019 to September 6, 2019. As part of our audit, we responded to the

[1] CyberScope, operated by DHS on behalf of OMB, is a web-based application designed to streamline information technology (IT) security reporting for Federal agencies. It gathers and standardizes data from federal agencies to support FISMA compliance. In addition, OIGs provide an independent assessment of effectiveness of an agency's information security program. Offices of Inspectors General must also report their results to DHS and OMB annually through CyberScope.

[2] As an Independent Public Accounting firm, we are required to follow standards set forth by American Institute of Certified Public Accountants (AICPA). In addition to conducting our audit in accordance with Generally Accepted Government Auditing Standards established by the U.S. Government Accountability Office, we complied with standards established by the AICPA.

DHS's *Fiscal Year (FY) 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (FY 2019 FISMA Reporting Metrics), Version 1.3, dated April 9, 2019, and assessed the maturity levels on behalf of the Treasury OIG. The scope of our work did not include the Internal Revenue Service (IRS), as that bureau was evaluated by the Treasury Inspector General for Tax Administration (TIGTA). The findings from the TIGTA report are included in Appendix III, *Department of the Treasury's Consolidated Response to DHS's FISMA 2019 Questions for Inspectors General*. Additional details regarding the scope of our independent performance audit are included in Appendix I, *Objective, Scope, and Methodology*. Appendix II, *Status of Prior-Year Findings,* summarizes Treasury's progress in addressing prior-year recommendations. Appendix IV, *Approach to Selection of Subset of Systems,* describes how we selected systems for review, and Appendix V contains a *Glossary of Terms* used in this report.

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, Treasury established and maintained its information security program and practices for its unclassified systems for the 5 Cybersecurity Functions[3] and 8 FISMA Metric Domains.[4] However, the program was not effective according to DHS criteria and as reflected in the 4 deficiencies within 1 of the 5 Cybersecurity Functions and within 4 of the 8 FISMA Metric Domains that we identified as follows:

Cybersecurity Function: Protect

1. Controls over security baseline configurations, vulnerability scanning, and flaw remediation was not consistently followed at Bureau of Engraving and Printing (BEP) and the Bureau of the Fiscal Service (Fiscal Service). (Configuration Management)
2. Access management, personal screening, and data encryption controls were not fully implemented at Departmental Offices (DO), Fiscal Service, and the United States Mint (Mint). (Identity and Access Management)
3. Privacy program was not fully established at the Mint. (Data Privacy and Protection)
4. Specialized security training requirements were not consistently implemented at the Mint. (Security Training)

We made 14 recommendations related to these control deficiencies that, if effectively addressed by management, should strengthen the respective bureaus', offices', and Treasury's information security programs. In a written response, the Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO) agreed with our findings and recommendations and provided planned corrective actions that were responsive to the intent of our recommendations (see Management Response).

These findings and recommendations did not include the results from TIGTA's evaluation of the IRS's security program and practices.[5]

In addition, we assessed Treasury's information security program and practices for its unclassified systems as Consistently Implemented (Level 3), which was ineffective according to DHS criteria. See Appendix III for *Department of the Treasury's Consolidated Response to DHS's FISMA 2019 Questions for Inspectors General* with overall results. The FY 2019 FISMA IG Reporting Metrics define an effective information security program as Managed and Measurable (Level 4). See Table 2 of this report for description of maturity levels.

---

[3] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency developed the FY 2019 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. The eight IG FISMA Metric Domains are aligned with the five information security functions of identify, protect, detect, respond, and recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

[4] As described in the *DHS's FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics,* Version 1.3, dated April 9, 2019, the eight FISMA Metric Domains are: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

[5] 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 (Reference number 2019-20-082), dated September 24, 2019

We caution that projecting the results of our audit to future periods is subject to the risk that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate.

Sincerely,

KPMG LLP

October 25, 2019

BACKGROUND

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. FISMA requires Federal agencies to develop, document, and implement an agency-wide 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, contractor, or other source. The act assigns specific responsibilities to agency heads and IGs in complying with requirements of FISMA. The act is supported by OMB, DHS, agency security policy, and risk-based standards and guidelines published by NIST related to information security practices.

FY 2019 IG FISMA Reporting Metrics

For FY 2019, the OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) continued to organize the FY 2019 IG FISMA Reporting Metrics around five information security functions[6] outlined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*[7] (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. In addition, the FY 2019 IG FISMA Reporting Metrics use the CIGIE maturity models for the eight metric domains: Risk Management (RM), Configuration Management (CM), Identity and Access Management (IA), Data Protection and Privacy (DP), Security Training (ST), Information Security Continuous Monitoring (ISCM), Incident Response (IR) and Contingency Planning (CP). **Table 1** shows the alignment of Cybersecurity Framework functions to the FY 2019 FISMA Metric Domains.

[6] In its *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, NIST created Functions to organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

[7] The President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

Table 1: *Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FISMA Metric Domains within the FY 2019 IG FISMA Reporting Metrics*

Cybersecurity Framework Security Functions	FISMA Metric Domains
Identify	Risk Management
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

The maturity models have five levels: Level 1: Ad-Hoc, Level 2: Defined, Level 3: Consistently Implemented, Level 4: Managed and Measurable, and Level 5: Optimized. The maturity level for a domain is determined by a simple majority, with the most frequently assessed level across the questions serving as the domain rating. A security program is considered effective if the majority of the FY 2019 IG FISMA Reporting Metrics are at least Level 4: Managed and Measurable. **Table 2** provides the descriptions for each maturity level.

Table 2: *Inspector General Assessed 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 Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 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.

Department of the Treasury Bureaus/Offices

Treasury consists of 12 operating bureaus and offices, including:

1 **Alcohol and Tobacco Tax and Trade Bureau (TTB)** – Responsible for enforcing and administering laws covering the production, use, and distribution of alcohol and tobacco products. TTB also collects excise taxes for firearms and ammunition.
2 **Bureau of Engraving and Printing (BEP)** – Designs and manufactures United States paper currency, securities, and other official certificates and awards.
3 **Bureau of the Fiscal Service (Fiscal Service)** – Promotes the financial integrity and operational efficiency of the U.S. government through exceptional accounting, financing, collections, payments, and shared services.
4 **Community Development Financial Institutions (CDFI) Fund** – Created to expand the availability of credit, investment capital, and financial services in distressed urban and rural communities.
5 **Departmental Offices (DO)** – Primarily responsible for policy formulation. DO, while not a formal bureau, is composed of offices headed by Assistant Secretaries, some of whom report to Under Secretaries. These offices include Domestic Finance, Economic Policy, General Counsel, International Affairs, Legislative Affairs, Management, Public Affairs, Tax Policy, and Terrorism and Financial Intelligence. The Office of Cybersecurity, within the Office of Management, is responsible for the development of information technology (IT) Security Policy. IT systems in support of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) are handled by DO.
   a. **Enterprise Application CyberSecurity** – Created as a result of organizational changes within DO, Enterprise Application CyberSecurity is primarily responsible for shared services applications.
   b. **Enterprise Infrastructure CyberSecurity** – Created as a result of organizational changes within DO, Enterprise Infrastructure CyberSecurity is primarily responsible for shared service infrastructure.
6 **Financial Crimes Enforcement Network (FinCEN)** – Supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes. It also provides United States policy makers with strategic analyses of domestic and worldwide trends and patterns.
7 **Internal Revenue Service (IRS)** – Responsible for determining, assessing, and collecting internal revenue in the United States. (Not within the scope of this audit.)
8 **Office of the Comptroller of the Currency (OCC)** – Charters, regulates, and supervises national banks and thrift institutions to ensure a safe, sound, and competitive banking system that supports the citizens, communities, and economy of the United States.
9 **Office of Inspector General (OIG)** – Conducts and supervises audits and investigations of Treasury's programs and operations except for IRS which is under the jurisdictional oversight of the Treasury Inspector General for Tax Administration and the Troubled Asset Relief Program (TARP), which is under the jurisdictional oversight of SIGTARP. The OIG also keeps the Secretary and the Congress fully and currently informed about problems, abuses, and deficiencies in Treasury's programs and operations.
10 **United States Mint (Mint)** – Designs and manufactures domestic, bullion, and foreign coins as well as commemorative medals and other numismatic items. The Mint also distributes United States coins to the Federal Reserve banks as well as maintains physical custody and protection of our nation's silver and gold assets.
11 **SIGTARP** – Has the responsibility to conduct, supervise, and coordinate audits and

investigations of the purchase, management, and sale of assets under the TARP. SIGTARP's goal is to promote economic stability by assiduously protecting the interests of those who fund the TARP programs (i.e., the American taxpayers).

12 **Treasury Inspector General for Tax Administration (TIGTA)** – Conducts and supervises audits and investigations of IRS programs and operations. TIGTA also keeps the Secretary and the Congress fully and currently informed about problems, abuses, and deficiencies in IRS programs and operations.

For the FY 2019 FISMA Unclassified performance audit, we selected the following bureaus and offices for testing: BEP, DO, Fiscal Service, Mint, OCC, and TTB. The sampling methodology is provided in Appendix IV, *Approach to Selection of Subset of Systems.* As in prior years, TIGTA evaluated IRS's information security program and practices. The findings of TIGTA's report are included in Appendix III, *Department of the Treasury's Consolidated Response to DHS's FISMA 2019 Questions for Inspectors General*.

We followed up on the status of prior-year findings for the in-scope bureaus and for TIGTA.

Department of the Treasury Information Security Management Program

Treasury Office of the Chief Information Officer (OCIO)

The Treasury CIO is responsible for providing Treasury-wide leadership and direction for all areas of information and technology management, as well as the oversight of a number of IT programs. Among these programs is Cyber Security, which has responsibility for the implementation and management of Treasury-wide IT security programs and practices. Through its mission, the OCIO Cyber Security Program develops and implements IT security policies and provides policy compliance oversight for both unclassified and classified systems managed by each of Treasury's bureaus. The OCIO Cyber Security Program's mission focuses on the following areas:

a. **Cyber Security Policy** – Manages and coordinates Treasury's cyber security policy for sensitive (unclassified) systems throughout Treasury, assuring these policies and requirements are updated to address today's threat environment, and conducts program performance, progress monitoring, and analysis.
b. **Performance Monitoring and Reporting** – Implements collection of Federal and Treasury-specific security measures and reports those to national authorities and in appropriate summary or dashboard form to senior management, IT managers, security officials, and bureau officials. For example, this includes preparation and submission of the annual FISMA report and more frequent continuous monitoring information through CyberScope.
c. **Cyber Security Reviews** – Conducts technical and program reviews to help strengthen the overall cyber security posture of Treasury and meet their oversight responsibilities.
d. **Enterprise-wide Security** – Works with Treasury's Government Security Operations Center to deploy new Treasury-wide capabilities or integrate those already in place, as appropriate, to strengthen the overall protection of Treasury.
e. **Understanding Security Risks and Opportunities from New Technologies** – Analyzes new information and security technologies to determine risks (e.g., introduction of new vulnerabilities) and opportunities (e.g., new means to provide secure and original functionality for users). OCIO seeks to understand these technologies, their associated risks and opportunities, and share and use that information to Treasury's advantage.
f. **Treasury Computer Security Incident Response Capability** – Provides incident

reporting with external reporting entities and conducts performance monitoring and analyses of the Computer Security Incident Response Center within Treasury and each bureau's Computer Security Incident Response Center.

g. **National Security Systems** – Manages and coordinates the Treasury-wide program to address the cyber security requirements of national security systems through the development of policy and program or technical security performance reviews.
h. **Cyber Security Sub-Council (CSS) of the CIO Council** – Operates to serve as the formal means for gaining bureau input and advice as new policies are developed, enterprise-wide activities are considered, and performance measures are developed and implemented; provides a structured means for information-sharing among the bureaus.

The Treasury CIO has tasked the Associate Chief Information Officer for Cyber Security (ACIOCS) with the responsibility of managing and directing the OCIO's Cyber Security program, as well as ensuring compliance with statutes, regulations, policies, and guidance. In this regard, *Department of the Treasury Information Technology Security Program* Treasury Directive Publication (TD P) 85-01, Appendix A, "Minimum Standard Parameters," serves as the Treasury IT security policy to provide for information security for all information and information systems that support the mission of Treasury, including those operated by another Federal agency or contractor on behalf of Treasury. In addition, as OMB periodically releases updates/clarifications of FISMA or as NIST releases updates to publications, the ACIOCS has responsibility to interpret and release updated policy for Treasury. The ACIOCS is also responsible for promoting and coordinating a Treasury IT security program, as well as monitoring and evaluating the status of Treasury's IT security posture and compliance with statutes, regulations, policies, and guidance. Lastly, the ACIOCS has the responsibility of managing Treasury's IT Critical Infrastructure Protection (CIP) program for Treasury IT assets.

Bureau CIOs

Organizationally, Treasury has a Treasury CIO and bureau-level CIOs. The bureau- level CIOs are responsible for managing the IT security program for their respective bureau, as well as advising the bureau head on significant issues related to the bureau IT security program. The bureau CIOs also have the responsibility for overseeing the development of procedures that comply with the Treasury OCIO's policy and guidance and federal statutes, regulations, policy, and guidance. The bureau Chief Information Security Officers (CISO) are tasked by their respective CIOs to serve as the central point of contact for the bureau's IT security program, as well as to develop and oversee the bureau's IT security program. This includes the development of policies, procedures, and guidance required to implement and monitor the bureau IT security program.

Department of the Treasury – Bureau OCIO Collaboration

The Treasury OCIO has established the CIO CSS, which is co-chaired by the ACIOCS and a bureau CIO. The CSS serves as a mechanism for obtaining bureau-level input and advises on new policies, Treasury IT security activities, and performance measures. The CSS also provides a means for sharing IT security-related information among bureaus. Included on the CSS are representatives from the OCIO and bureau CIO organizations.

OVERALL AUDIT RESULTS

Consistent with applicable FISMA requirements, OMB's policy and guidance, and the NIST standards and guidelines, Treasury established and maintained its information security program and practices for its unclassified systems for the 5 Cybersecurity functions and 8 FISMA Metric Domains. However, the program was not effective according to DHS criteria and as reflected in 4 deficiencies in 1 of the 5 Cybersecurity Functions and 4 out of the 8 FISMA Metric Domains that needed improvement.[8]

We have made 14 recommendations that, if effectively addressed by management, should strengthen the respective bureaus', offices', and Treasury's information security program and practices. The *Findings* section of this report presents the detailed findings and associated recommendations. We will follow up on the status of all corrective actions as part of the FY 2020 independent evaluation.

In addition, we assessed Treasury's information security program and practices for its unclassified systems as Consistently Implemented (Level 3), which was ineffective according to DHS criteria. See Appendix III for *Department of the Treasury's Consolidated Response to DHS's FISMA 2019 Questions for Inspectors General* with overall results. The FY 2019 FISMA IG Reporting Metrics define an effective information security program as Managed and Measurable (Level 4). See Table 2 of this report for description of maturity levels.

Additionally, we evaluated the prior-year findings from the FYs 2018, 2017, 2016, 2015, and 2011 FISMA performance audits, as well as the FYs 2014 and 2013 FISMA evaluations and noted that management had closed a total of 22 of 33 findings. See Appendix II*, Status of Prior-Year Findings*, for additional details.

In a written response to this report, the Deputy Assistant Secretary for Information Systems and CIO agreed with our findings and recommendations and provided planned corrective actions that were responsive to the intent of our recommendations (See Management Response).

[8] Treasury Inspector General for Tax Administration will provide a separate report evaluating the Internal Revenue Service's implementation of Treasury's information security program.

FINDINGS

Finding 1 – Controls over security baseline configurations, vulnerability scanning, and flaw remediation were not consistently followed at BEP and Fiscal Service.

NIST Special Publication (SP) 800-53, Revision (Rev.) 4, TD P 85-01, and bureau information security plans require bureaus to review and update the baseline configuration of information systems: a) annually; b) when required due to a system change to hardware, operating system, application, or major upgrade; and c) as an integral part of information system component installations and upgrades. NIST SP 800-53, TD P 85-01, and bureau security plans also require bureaus to remediate legitimate vulnerabilities within 90 days for low risk, 60 days for moderate risk, and 30 days for high and critical risks. Additionally, bureaus are required to develop, document, and maintain under configuration control, a current baseline configuration of the information system. Lastly, bureaus are required to identify, document, and approve any deviations from established configuration settings for information system components based on bureau operational requirements. This control falls under the Protect Cybersecurity Function and the Configuration Management FISMA Metric Domain.

We noted the following:

- BEP management did not consistently review, update, and approve configuration baselines for the BEP System 1 production database and operating system server in accordance with NIST SP 800-53, TD P 85-01, and BEP's security plans, as evidenced by the following:
  - BEP System 1 production database:
    - Management did not conduct annual reviews and updates to the configuration baseline document. Management last updated the configuration baseline on November 2, 2010. The *BEP Security Baseline Configuration Standard* is based on a version of Center for Internet Security (CIS) benchmarks for a database that is not deployed in the BEP environment.
    - Management did not formally approve the BEP System 1 production database baseline configuration document. The change control history for the document does not reflect approval since the initial draft on August 30, 2005 or last revision date on November 2, 2010.
  - BEP System 1 production operating system sever:
    - Management did not conduct annual reviews and updates to the BEP System 1 operating system standard configuration document. Management last updated the configuration baseline on September 24, 2013. The BEP System 1 operating system configuration standard is based on the Draft Windows Server 2012 STIG, Version 1, which does not reflect the current operating system deployed at BEP.
    - Management did not formally approve the BEP System 1 operating system standard configuration document. The document change history section of BEP System 1 operating system's standard configuration document does not reflect approval since the initial version was submitted to the Change Control Board (CCB) on September 24, 2013.

  BEP management stated that due to competing priorities, it did not commit the resources to review, update, and approve the baseline configuration standards for the BEP System production database and operating system server in adherence to the *BEP Minimum Standard Parameters* and NIST SP 800-53, Rev. 4. Not reviewing, updating, and approving baseline configurations in a timely manner could hamper BEP's ability to make sound risk

based decisions for confidentiality, integrity, and availability of their operational environment. Additionally, lack of configuration baseline review, updates, and approvals increase the risk that management is unaware of the current security posture of the environment for known and unknown weaknesses, thereby increasing the likelihood of computing resources being compromised. *(See Recommendations #1 and 2.)*

- BEP management could not provide evidence of the remediation of 5 high vulnerabilities identified during Security Content Automation Protocol (SCAP) configuration baseline compliance scans and 2 high vulnerabilities were identified during vulnerability scans for BEP System 1. As such, the status of the remediation of the vulnerabilities could not be verified. Management stated that these exceptions occurred due to competing priorities at the bureau. Not remediating system deviations from security configuration baselines and known vulnerabilities as required by the *BEP Minimum Standard Parameters* could result in the system not being adequately configured and vulnerable to exploitation. This may result in weaknesses that could lead to unauthorized access and/or software/hardware bugs that may cause errors, or increase the likelihood of exploitation, which could jeopardize the confidentiality, integrity, and availability of the BEP System 1 environment and indirectly the overall BEP operating environment. *(See Recommendation #3)*

- Fiscal Service did not formally document the security configuration baseline documentation or configuration baseline deviations for Fiscal Service System 1. Although management conducted security compliance scans using bureau-wide baselines, management did not specifically tailor the baselines used in the scans to Fiscal Service System 1. On August 6, 2019, Fiscal Service management stated this issue was identified during a recent assessment, and management is in the process of establishing a plan of action and milestones to address this issue. According to Fiscal Service management, due to competing priorities with a newly implemented policy and the new software tool, plus the operational nature of Fiscal Service System 1, it did not create and submit the Fiscal Service System 1 configuration baseline documentation and configuration baseline deviations for formal approval from the appropriate official in adherence to the Fiscal Service bureau-wide *IT Standard Operating Procedure.* Not having system-specific configuration baseline documents and configuration baseline deviations formally approved could hamper Fiscal Service's ability to make sound risk based decisions for the confidentiality, integrity, and availability of their operational environment. Also, lack of configuration baseline documentation and deviation approvals increase the risk that Fiscal Service management is unaware of the current security posture of the system-level environment for known and unknown weaknesses, thereby increasing the likelihood of making bureau-wide oversight and compliance risk decisions based on incomplete information. Additionally, not having current configuration documentation could lead to lack of continuity of operations in the event of personnel turnover. *(Recommendations #4 and 5.)*

The Deputy Assistant Secretary for Information Systems and CIO should work with the responsible officials to ensure the following recommendations are implemented.

We recommend that BEP management:

1. Commit resources to update and review annually and approve the existing security baseline configurations for the BEP System 1 production database and operating system server as required by BEP Minimum Security Parameters and NIST SP 800-53, Rev.4.

   Management Response: BEP will commit resources to update and review annually the

existing security baseline configurations for System 1 as required by security controls CM-2 of the BEP Minimum Baseline Security and NIST SP 800-53, Rev 4. Target completion date: January 30, 2020.

Auditor Comment: Management's response meets the intent of our recommendation.

2. Update the current BEP System 1 production database and operating system server security baseline configuration standards to reflect the current database and operating system versions deployed in the BEP environment.

   Management Response: BEP will commit resources to update and review annually the existing security baseline configurations for System 1 as required by security controls CM-2 of the BEP Minimum Baseline Security and NIST SP 800-53, Rev 4. Target completion date: January 30, 2020.

   Auditor Comment: Management's response meets the intent of our recommendation.

3. Assess and remediate vulnerabilities identified during SCAP configuration baseline compliance and vulnerability scanning within the required timeframes specified in the BEP Minimum Standard Parameters.

   Management Response: BEP will assess and remediate the identified vulnerabilities within the required timeframes specified. Target completion date: January 30, 2020.

   Auditor Comment: Management's response meets the intent of our recommendation.

We recommend that Fiscal Service management:

4. Complete the Fiscal Service System 1 configuration baseline documents and obtain formal approvals for the configuration documents.

   Management Response: Fiscal Service will complete the formal process to establish approved baseline configurations for System 1 components. Target completion date: March 31, 2020.

   Auditor Comment: Management's response meets the intent of our recommendation.

5. Identify Fiscal Service System 1 configuration baseline deviations and obtain approvals for the configuration baseline deviations from the appropriate official.

   Management Response: Fiscal Service will identify and document baseline deviations as part of the formal process to establish approved baseline configurations for System 1 components. Target completion date: March 31, 2020.

   Auditor Comment: Management's response meets the intent of our recommendation.

Finding 2 – Access management, personnel screening, and data encryption controls were not fully implemented at DO, Fiscal Service, and the Mint.

NIST SP 800-53, Rev. 4, and TD P 85-01 require bureaus and offices to review and reevaluate the appropriateness of non-privileged user accounts on an annual basis and privileged user accounts on a semiannual basis. Additionally, NIST SP 800-53, Rev. 4, requires bureaus and offices to implement cryptographic mechanisms for information systems to prevent unauthorized disclosure of information either in transition or at rest.

Also, NIST SP 800-53, Rev. 4., and TD P 85-01 require bureaus and offices to develop and document access agreements for organizational information systems; review and update the access agreements annually; and ensure that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access. Bureaus and offices are required to provide basic security awareness training to information system users, including managers, senior executives, and contractors: as part of initial training for new users, when required by information system changes, and annually thereafter. Additionally, bureaus and offices must screen individuals prior to authorizing access to the information system. Finally, bureaus and offices must establish and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage and to receive a signed acknowledgment from such individuals indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

These controls fall under the Protect Cybersecurity Function and the Identity and Access Management FISMA Metric Domain.

We noted the following:

- DO did not conduct semi-annual periodic user access reviews for DO System 2 privileged users. DO management stated that this deficiency occurred due to conflicting priorities. Lack of periodic user access reviews and validations of user access to the DO System 2 increases the risk of unauthorized access, disclosure, and modification of production data. *(See Recommendation #6.)*

- Fiscal Service lacked documentation supporting the encryption of data in transit for Fiscal Service System 2, and therefore, the encryption status of data in transit could not be verified. Furthermore, database encryption was not in place for Fiscal Service Systems 1 and 2. Fiscal Service was unable to demonstrate that the Fiscal Service System 2 was encrypted while in transit within the environment. In addition, Fiscal Service is currently executing an ongoing bureau-wide project to encrypt data at rest; therefore, several Fiscal Service systems, including Fiscal Service Systems 1 and 2, did not have encryption controls fully enforced. Failure to encrypt data at rest and data in transit increases the risk of unauthorized data exposure and disclosure to system users and malicious agents. *(See Recommendations #7 and 8.)*

- Per NIST 800-54, Rev. 4, and TD P 85-01, access to Mint systems requires a user to have a background investigation, signed Nondisclosure Agreement (NDA), signed Rules of Behavior (ROB) form, and completed Security Awareness training. New users must complete security awareness training within 5 business days of being granted system access or within the users' first 60 days by having them review and accept the ROB. For

current Mint users requesting new system access, including Mint System 1, management relies on the existing background investigation, NDAs, ROBs, and completed trainings to approve access to the system.

However, supporting documentation was not completed in accordance to the aforementioned requirements as follows:

- Two of 6 Mint System 1 users did not sign ROBs and complete security awareness training within 5 business days of being granted system access or within the users' first 60 days by having them review and accept the ROB. The ROB and security awareness training were completed after more than 3 months of their start date.
- The *Mint Information Security Policy* has not defined clear requirements for NDAs and ROBs to be signed before establishing new users' access to Mint information systems.

Further, supporting documentation was unavailable to evidence the following:

- A completed background investigation for 3 of 6 Mint System 1 users.
- A signed NDA, a signed ROB form, and completed security awareness training for 1 of 6 Mint System 1 users. Management informed us this user is exempt from these requirements because the user is not a Mint employee or contractor and does not have an Active Directory account. However, a formal risk acceptance exempting users from signing a NDA, a ROB form, and completing privacy and security trainings was not available.
- A signed NDA could not be evidenced for 1 of 6 Mint System 1 users.

Mint management stated that due to lack of oversight and clear documented policy requirements, it did not proactively verify that users had completed background investigations, signed the relevant access agreements, and completed security awareness training in adherence to the Mint Information Security Policy and TD P 85-01 prior to granting Mint System 1 user access. Bureau-wide information security polices provide guidance over controls implemented over the information system. Incomplete access management policies can lead to a misunderstanding of the information system control environment. This can lead to improper system access being provided to users, increasing the risk of unauthorized access, disclosure, and/or modification of production data and computing resources. Failure to require completed NDAs, ROBs, background investigations, and security awareness training when granting system access increases the risk of unauthorized users gaining access to the system and compromising the data integrity. *(See Recommendations #9, 10, and 11.)*

The Deputy Assistant Secretary for Information Systems and CIO should work with the responsible officials to ensure the following recommendations are implemented.

We recommend DO management:

6. Develop and implement a process to ensure that periodic user access reviews are completed for DO System 2, documented, and all unnecessary access is removed in accordance with NIST SP 800-53 and TD P 85-01.

   Management Response: DO will develop and implement a process to ensure that periodic user access reviews are completed for DO System 2, documented, and all unnecessary access is removed in accordance with Treasury and DO requirements. Target completion date: December 31, 2019.

   Auditor Comment: Management's response meets the intent of our recommendation.

We recommend the Fiscal Service management:

7. Protect the confidentiality and integrity of transmissions by encrypting Fiscal Service System 2 data in transit as required by NIST 800-53, Rev. 4.

   Management Response: Fiscal Service will ensure System 2 data in transit is encrypted to protect the confidentiality and integrity of transmissions as required by BLSR and NIST 800-53, Rev. 4, security control SC-8. Target completion date: September 30, 2020.

   Auditor Comment: Management's response meets the intent of our recommendation.

8. Enforce encryption of databases to protect the confidentiality of Fiscal Service Systems 1 and 2 as required by NIST 800-53, Rev. 4.

   Management Response: Fiscal Service will (1) research areas of non-compliance and if feasible enforce encryption of the database(s) to protect the confidentiality of System 1 data at rest as required by BLSR and NIST 800-53, Rev. 4, security control SC-28. Risk acceptance will be documented for any areas of non-compliance. Target completion date: June 30, 2020; and (2) will enforce encryption of the database to protect the confidentiality of System 2 data at rest as required by BLSR and NIST 800-53, Rev. 4, security control SC-28. This will be done in accordance with Project #2284 - Data Encryption at Rest. Target completion date: January 31, 2021.

   Auditor Comment: Management's response meets the intent of our recommendation.

We recommend the Mint management:

9. Establish a quality control process to ensure that user access to Mint System 1 and other Mint information systems follow the access management process requiring the completed background investigations, signed NDAs, signed ROBs, and completion of the security awareness training.

   Management Response: Mint plans to establish a quality control process to ensure that user access to Mint System 1 and other Mint information systems follow the access management process requiring the completed background investigations, signed NDAs, signed ROBs, and completion of the security awareness training. Target completion date: March 31, 2020.

   Auditor Comment: Management's response meets the intent of our recommendation.

10. Clearly document and formally approve exemptions to the Mint's access authorization process when a business justification exists.

    Management Response: Mint plans to clearly document and formally approve exemptions to the Mint's access authorization process when a business justification exists. Target completion date: March 31, 2020.

    Auditor Comment: Management's response meets the intent of our recommendation.

11. Update the Mint Information Security Policy to meet TD P 85-01 and NIST requirements related to access agreements and ROBs.

Management Response: Mint plans to update Mint's Information Security Policy to meet TD P 85-01 and NIST requirements related to access agreements and ROBs. Target completion date: March 31, 2020.

Auditor Comment: Management's response meets the intent of our recommendation.

Finding 3 – Privacy program was not fully established at the Mint.

NIST SP 800-53, Rev. 4, requires bureaus and offices to 1) monitor federal privacy laws and policy for changes that affect the privacy program; 2) allocate sufficient resources to implement and operate the organization-wide privacy program; 3) develop a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; 4) develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving personally identifiable information (PII); and 5) update privacy plan, policies, and procedures at least biennially. NIST SP 800-53, Rev. 4., also requires bureaus and offices to monitor and audit privacy controls and internal privacy policy based on an organization-defined frequency to ensure effective implementation. This control falls under the Protect Cybersecurity Function and the Data Protection and Privacy FISMA Metric Domain.

We noted the following:

- The Mint has taken steps to implement privacy safeguards for PII and conduct system level privacy assessments. However, based on inquiry with the Acting Chief Privacy Officer, management has not fully established a Mint bureau-wide data protection and privacy program. Specifically, we noted that management did not:

    - formally document a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; and

    - define and implement mechanisms to monitor and audit on a regular basis the effectiveness of its privacy controls and internal privacy policy at the bureau-level.

    Management is still in the process of developing a bureau-wide Privacy Program and is working with its Legal department for privacy-related policies and procedures. Failure to develop and implement a comprehensive privacy program increases the risk of disclosure of sensitive data due to the inconsistent application of privacy controls. Additionally, not having a fully documented program may lead to inconsistencies in handling privacy-related issues, including the handling of PII, in the event of personnel turnover *(See Recommendations #12 and 13.)*

The Deputy Assistant Secretary for Information Systems and CIO should work with the responsible officials to ensure the following recommendations are implemented.

We recommend that Mint management:

12. Finalize and implement its bureau-wide privacy program that includes a strategic organizational privacy plan for implementing applicable privacy control and procedures in accordance with NIST 800-53.

Management Response: Mint plans to finalize and implement its bureau-wide privacy program that includes a strategic organizational privacy plan for implementing applicable privacy control and procedures in accordance with NIST 800-53. Target completion date: May 31, 2020.

Auditor Comment: Management's response meets the intent of our recommendation.

13. Implement mechanisms to monitor and audit on a regular basis the effectiveness of its privacy controls and internal privacy policy at the bureau-level.

    Management Response: Mint plans to implement mechanisms to monitor and audit on a regular basis the effectiveness of its privacy controls and internal privacy policy at the bureau-level: May 31, 2020.

    Auditor Comment: Management's response meets the intent of our recommendation.

Finding 4 – Specialized security training requirements were not consistently implemented at the Mint.

NIST SP 800-53, Rev. 4, requires bureaus and offices to provide role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the information system or performing assigned duties, when required by information system changes, and thereafter. TD P 85-01 states that bureaus are responsible for establishing sufficient controls to ensure supervisors and managers are held accountable for their employees receiving appropriate security awareness training.

This control falls under the Protect Cybersecurity Function and Security Training FISMA Metric Domain.

We noted the following:

- The Mint requires personnel that are assigned security roles and responsibilities to complete the role-based specialized IT security training on an annual basis. However, only 81 percent of the required Mint employees completed this training. Mint does not have effective mechanisms in place to ensure the timely completion of role-based specialized IT security training. Security threats are constantly evolving, and require continuous learning and training for those individuals responsible for computer security. Without completing the necessary role-based security awareness training, the employees may not be aware of the rules and responsibilities for each employee in order to appropriately protect the information systems. As such, sensitive data could be subject to unauthorized access, modification, or loss. *(See Recommendation #14.)*

The Deputy Assistant Secretary for Information Systems and CIO work with the responsible officials to ensure the following recommendation is implemented.

We recommend that Mint management:

14. Establish sufficient controls to ensure supervisors/managers are held accountable for the completion of the role-based specialized IT security training by their employees with security roles and responsibilities.

Management Response: Mint plans to establish sufficient controls to ensure supervisors/managers are held accountable for the completion of the role-based specialized IT security training by their employees with security roles and responsibilities. Target completion date: January 31, 2020.

Auditor Comment: Management's response meets the intent of our recommendation.

MANAGEMENT RESPONSE TO THE REPORT

The following is the Deputy Assistant Secretary for Information Systems and CIO's response, dated October 18, 2019, to the FY 2019 FISMA Performance Audit Report.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 18, 2019

MEMORANDUM FOR LARISSA KLIMPEL
DIRECTOR, INFORMATION TECHNOLOGY AUDIT

FROM: Eric Olson /s/
Deputy Assistant Secretary for Information Systems and Chief Information Officer

SUBJECT: Management Response to Draft Audit Report – "Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2019 Performance Audit"

Thank you for the opportunity to comment on the draft report entitled, *Fiscal Year 2019 Evaluation of Treasury's Compliance with Federal Information Security Modernization Act [FISMA]*. We are pleased the report states our security program is consistent with FISMA requirements, the Office of Management and Budget (OMB) information security policy, and related security standards and guidance published by the National Institute of Standards and Technology (NIST).

We have carefully reviewed the draft and agree with all findings and recommendations. Please refer to the attachment for further details on our planned corrective actions. We appreciate that this year's Cybersecurity Framework maintained a common scoring model allowing the Department to conduct a year-on-year comparison of FISMA compliance and program advances. Consistent with the FY18 FISMA evaluation, we noted a moderate improvement in the overall results of this year's performance audit.

The Department remains committed to the continuous improvement of its information security program through effective continuous monitoring and evaluation of risks to our environment.

We appreciate the audit recommendations as they will help improve the effectiveness of our cybersecurity program.

Attachment

cc: David F. Eisner, Assistant Secretary for Management
Sarah Nur, Acting Associate Chief Information Officer for Cyber Security and Deputy Chief Information Security Officer

Attachment

Management Response to (KPMG) Recommendations

KPMG Finding 1: Controls over security baseline configurations, vulnerability scanning, and flaw remediation were not consistently followed at Bureau of Engraving and Printing (BEP) and Fiscal Service (FS).

KPMG Recommendation 1: We recommend BEP management: For the selected system, commit resources to update and review annually and approve the existing security baseline configurations for the BEP System 1 production database and operating system server as required by BEP Minimum Security Parameters and NIST SP 800-53, Rev.4.

> **Treasury's Response:** Management will commit resources to update and review annually the existing security baseline configurations for System 1 as required by security controls CM-2 of the BEP Minimum Baseline Security and NIST SP 800-53, Rev 4. Target completion date: January 30, 2020.
>
> **Responsible Official:** BEP, Acting Chief Information Security Officer.

KPMG Recommendation 2: We recommend BEP management: For the selected system, update the current BEP System 1 production database and operating system server security baseline configuration standards to reflect the current database and operating system versions deployed in the BEP environment.

> **Treasury's Response:** Management will commit resources to update and review annually the existing security baseline configurations for System 1 as required by security controls CM-2 of the BEP Minimum Baseline Security and NIST SP 800-53, Rev 4. Target completion date: January 30, 2020.
>
> **Responsible Official:** BEP, Acting Chief Information Security Officer.

KPMG Recommendation 3: We recommend BEP management: For the selected system, assess and remediate vulnerabilities identified during SCAP configuration baseline compliance and vulnerability scanning within the required timeframes specified in the BEP Minimum Standard Parameters:

> **Treasury's Response:** BEP Management will assess and remediate the identified vulnerabilities within the required timeframes specified. Target completion date: January 30, 2020.
>
> **Responsible Official:** BEP, Acting Chief Information Security Officer.

KPMG Recommendation 4: We recommend Fiscal Service management: For the selected system, complete the Fiscal Service System 1 configuration baseline documents and obtain formal approvals for the configuration documents.

Treasury's Response: Fiscal Service will complete the formal process to establish approved baseline configurations for System 1 components. Target completion date: March 31, 2020.

Responsible Official: FS, Chief Information Officer.

KPMG Recommendation 5: We recommend Fiscal Service management: For the selected system, identify Fiscal Service System 1 configuration baseline deviations and obtain approvals for the configuration baseline deviations from the appropriate official.

Treasury's Response: Fiscal Service will identify and document baseline deviations as part of the formal process to establish approved baseline configurations for System 1 components. Target completion date: March 31, 2020.

Responsible Official: FS, Chief Information Officer.

KPMG Finding 2: Access management, personnel screening, and data encryption controls were not fully implemented at Departmental Offices (DO), Fiscal Service (FS), and the Mint.

KPMG Recommendation 6: We recommend DO management: For the selected system, develop and implement a process to ensure that periodic user access reviews are completed for DO System 2, documented, and all unnecessary access is removed in accordance with NIST SP 800-53 and TD P 85-01.

Treasury's Response: DO will develop and implement a process to ensure that periodic user access reviews are completed for System 2, documented, and all unnecessary access is removed in accordance with Treasury and DO requirements. Target completion date: December 31, 2019.

Responsible Official: DO, Chief Information Security Officer.

KPMG Recommendation 7: We recommend Fiscal Service management: For the selected system, protect the confidentiality and integrity of transmissions by encrypting Fiscal Service System 2 data in transit as required by NIST 800-53, Rev. 4.

Treasury's Response: Fiscal Service will ensure System 2 data in transit is encrypted to protect the confidentiality and integrity of transmissions as required by BLSR and NIST 800-53, Rev. 4, security control SC-8. Target completion date: September 30, 2020.

Responsible Official: FS, Chief Information Officer.

KPMG Recommendation 8: We recommend Fiscal Service management: For the selected system, enforce encryption of databases to protect the confidentiality of Fiscal Service Systems 1 and 2 as required by NIST 800-53, Rev. 4.

Treasury's Response:

(1) Fiscal Service will research areas of non-compliance and if feasible enforce encryption of the database(s) to protect the confidentiality of System 1 data at rest as required by BLSR and NIST 800-53, Rev. 4, security control SC-28. Risk acceptance will be documented for any areas of non-compliance. Target completion date: June 30, 2020.

(2) Fiscal Service will enforce encryption of the database to protect the confidentiality of System 2 data at rest as required by BLSR and NIST 800-53, Rev. 4, security control SC-28. This will be done in accordance with Project #2284 - Data Encryption at Rest. Target completion date: January 31, 2021.

Responsible Official: FS, Chief Information Officer.

KPMG Recommendation 9: We recommend Mint management: For the selected system, establish a quality control process to ensure that user access to Mint System 1 and other Mint information systems follow the access management process requiring the completed background investigations, signed NDAs, signed ROBs, and completion of the security awareness training.

Treasury's Response: Mint plans to establish a quality control process to ensure that user access to Mint System 1 and other Mint information systems follow the access management process requiring the completed background investigations, signed NDAs, signed ROBs, and completion of the security awareness training. Target completion date: March 31, 2020.

Responsible Official: Mint, Deputy Chief Information Officer.

KPMG Recommendation 10: We recommend Mint management: Clearly document and formally approve exemptions to the Mint's access authorization process when a business justification exists.

Treasury's Response: Mint plans to clearly document and formally approve exemptions to the Mint's access authorization process when a business justification exists. Target completion date: March 31, 2020.

Responsible Official: Mint, Deputy Chief Information Officer.

KPMG Recommendation 11: We recommend Mint management: Update the Mint Information Security Policy to meet TD P 85-01 and NIST requirements related to access agreements and ROBs.

Treasury's Response: Mint plans to update Mint's Information Security Policy to meet TD P 85-01 and NIST requirements related to access agreements and ROBs. Target completion date: March 31, 2020.

Responsible Official: Mint, Deputy Chief Information Officer.

KPMG Finding 3: Privacy program was not fully established at the Mint.

KPMG Recommendation 12: We recommend Mint management: Finalize and implement its bureau-wide privacy program that includes a strategic organizational privacy plan for implementing applicable privacy control and procedures in accordance with NIST 800-53.

> **Treasury's Response**: Mint plans to finalize and implement its bureau-wide privacy program that includes a strategic organizational privacy plan for implementing applicable privacy control and procedures in accordance with NIST 800-53. Target completion date: May 31, 2020.
>
> Responsible Official: Mint, Deputy Chief Information Officer.

KPMG Recommendation 13: We recommend Mint management: Implement mechanisms to monitor and audit on a regular basis the effectiveness of its privacy controls and internal privacy policy at the bureau-level.

> **Treasury's Response**: Mint plans to implement mechanisms to monitor and audit on a regular basis the effectiveness of its privacy controls and internal privacy policy at the bureau-level: May 31, 2020.
>
> Responsible Official: Mint, Deputy Chief Information Officer.

KPMG Finding 4: Specialized security training requirements were not consistently implemented at the Mint.

KPMG Recommendation 14: We recommend Mint management: Establish sufficient controls to ensure supervisors/managers are held accountable for the completion of the role-based specialized IT security training by their employees with security roles and responsibilities.

> **Treasury's Response:** Mint plans to establish sufficient controls to ensure supervisors/managers are held accountable for the completion of the role-based specialized IT security training by their employees with security roles and responsibilities. Target completion date: January 31, 2020.
>
> **Responsible Official:** Mint, Deputy Chief Information Officer.

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this performance audit was to assess the effectiveness of the Department of the Treasury's (Treasury or Department) information security program and practices for its unclassified systems (with the exception of the Internal Revenue Service (IRS) systems) for the period July 1, 2018 through June 30, 2019.[9] The scope of our work did not include the Internal Revenue Service (IRS), as that bureau was evaluated by the Treasury Inspector General for Tax Administration (TIGTA). The TIGTA report is appended to this report and the findings are included in Appendix III.

To address our audit objective, we assessed the effectiveness of the Treasury information security program and practices for a selection of 6 bureaus (excluding the IRS) and 10 information systems (refer to Appendix IV, *Approach to Selection of Subset of Systems* for the methodology for selecting the 6 in-scope bureaus and 10 information systems). As part of our audit, we responded to the Department of Homeland Security (*DHS) FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (*FY 2019 IG FISMA Reporting Metrics*),* Version 1.3, dated April 9, 2019, and assessed the maturity levels on behalf of the Treasury Office of Inspector General. Finally, we followed up on the status of prior-year *Federal Information Security Modernization Act of 2014* (FISMA) findings.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS).[10] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To accomplish our audit objective, we evaluated security controls in accordance with applicable legislation, the FY 2019 IG FISMA Reporting Metrics, and the National Institute of Standards and Technology (NIST) standards and guidelines as outlined in the *Criteria* section. We reviewed Treasury's information security program for a program-level perspective and then examined how each selected bureau and office complied with the implementation of these policies and procedures.

We performed test procedures at the Treasury level and for a selection of 6 bureaus and 10 information systems. The following was our approach for accomplishing the FISMA audit and determining the maturity levels for each of the 5 Cybersecurity Functions and 8 FISMA Metric Domains from the *Fiscal Year (FY) 2019 Inspector General (IG) FISMA Reporting Metrics:*

1. We requested that Treasury management communicate its self-assessed maturity levels, where applicable, to confirm our understanding of the FISMA-related policies and procedures, guidance, structures, and processes established by the Department and in-scope bureaus. This helped us to understand the specific artifacts to evaluate as part of the FISMA audit.

2. We performed test procedures for maturity level 3 (Consistently Implemented) at the Department, in-scope bureaus, and in-scope systems (where applicable) for the maturity level 3 questions within the 8 FISMA Metric Domains. The test procedures evaluated the design and operating effectiveness of the controls. If we determined that maturity level 3 controls were ineffective, we assessed, based on test results and evidence obtained, the

[9] *Supra* note 2.
[10] *Supra* note 3.

maturity at level 1 (Ad Hoc) or 2 (Defined) for the questions that failed testing.

3. For maturity level 3 controls determined to be effective, we performed level 4 (Managed and Measurable) test procedures for the Department, in-scope bureaus, and in-scope systems (where applicable) for the maturity level 4 questions within the 8 FISMA Metric Domains. The test procedures evaluated the design and operating effectiveness of the controls.

4. For maturity level 4 controls determined to be effective, we performed level 5 (Optimized) test procedures for the Department, in-scope bureaus, and in-scope system (where applicable) for the maturity level 5 questions within the 8 FISMA Metric Domains. The test procedures evaluated the design of the controls.

We performed our fieldwork from April 23, 2019 to September 6, 2019, at Treasury's headquarters and offices in Washington, D.C., and bureau locations and data centers in Washington, D.C.; and Hyattsville, Maryland. During our audit, we met with Treasury management to discuss our preliminary findings.

Criteria

We focused our FISMA audit approach on federal information security guidance developed by NIST and Office of Management and Budget (OMB). NIST Special Publications (SP) provide guidelines that are considered essential to the development and implementation of agencies' security programs. The following is a listing of the criteria used in the performance of the FY 2019 FISMA performance audit:

- The Federal Information Security Modernization Act of 2014 (Public Law 113-283, §2, 128Stat. 3073, 3075-3078 [2014])

- NIST Federal Information Processing Standard (FIPS) and/or SPs[11]

    - FIPS Publication 199*, Standards for Security Categorization of Federal Information and Information Systems*

    - FIPS Publication 200*, Minimum Security Requirements for Federal Information and Information Systems*

    - NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*

    - NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*

    - NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*

    - NIST SP 800-39, *Managing Information Security*

[11] Per OMB FISMA reporting instructions, while agencies are required to follow NIST standards and guidance in accordance with OMB policy, there is flexibility within NIST's guidance documents (specifically in the 800 series) in how agencies apply the guidance. However, NIST FIPS are mandatory. Unless specified by additional implementing policy by OMB, guidance documents published by NIST generally allow agencies latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable and compliant with the guidance.

  - NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
  - NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
  - NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*
  - NIST SP 800-70 Revision 3, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*
  - NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response
  - NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
  - NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*

- OMB Policy Directives
  - OMB Circular A-130, *Management of Federal Information Resources*
  - OMB Memorandum 05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*
  - OMB Memorandum 16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for Federal Civilian Government*
  - OMB Memorandum 17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Requirements*

- Department of Homeland Security
  - FY 2019 IG FISMA Reporting Metrics
  - Federal Continuity Directive 1 (FCD-1), *Federal Executive Branch National Continuity Program and Requirements*

- Treasury Policy Directives
  - Treasury Directive Publication 15-71, *Department of Treasury Security Manual*
  - Treasury Directive Publication 85-01, Treasury Information Technology (IT) Security Program
  - Other Treasury Information and Information Technology Security Policies and Procedures
  - Relevant bureau security policies and procedures

APPENDIX II – STATUS OF PRIOR-YEAR FINDINGS

In Fiscal Years (FYs) 2018, 2017, 2015, and 2011 we conducted a Federal Information Security Management Act of 2014 (FISMA) Performance Audit in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. As part of this year's FISMA Performance Audit, we followed up on the status of the prior year findings. For the following prior-year performance audit findings, we evaluated the information systems to determine whether the recommendations have been implemented and whether the findings were closed by management. We inquired of Treasury personnel and inspected evidence to determine the status of the findings. If there was evidence that the recommendations had been sufficiently implemented, we validated the closed findings. If there was evidence that the recommendations had been only partially implemented, or not implemented at all, we determined the finding to be open.

Based on the results of our follow-up test work, we determined that the following prior-year findings are still open:

FY 2018 FISMA Performance Audit

- Finding #1 – Mint: Security Assessment and Authorization (SA&A) processes were not consistently completed.
  - Recommendation #1: Complete the SA&A packages for Systems 1 and 2 in accordance with the U.S. Mint Information Security Directive and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision (Rev.) 1
- Finding #1 – Treasury Inspector General for Tax Authority (TIGTA): SA&A processes were not consistently completed.
  - Recommendation #2: Develop a plan that incorporates and takes into account interruptions in the TIGTA System funding.
- Finding #6 – TIGTA: Configuration security baselines were not always established, and vulnerability scanning was not consistently performed.
  - Recommendation #9: Establish a current enterprise baseline of software and related configurations for the TIGTA System 1.
  - Recommendation #10: Perform vulnerability scanning over the TIGTA System 1 every 30 days in accordance with Treasury Directive Publication (TD P) 85-01.
- Finding #7 – Mint: Account management policies were not consistently followed for removing user access.
  - Recommendation #17: Ensure that Mint System 1 accounts that are inactive over 120 days are automatically disabled within the system in accordance with TD P 85-01 and NIST SP 800-53, Rev.4.
- Finding #7 – TIGTA: Account management policies were not consistently followed for authorizing, reviewing, recertifying, and removing user access.
  - Recommendation #22: Develop and disseminate to TIGTA personnel a TIGTA System 1 access control policy that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- Finding # 8 – TIGTA: Contingency planning controls were not consistently implemented.
  - Recommendation #23: Perform and document the Business Impact Analysis (BIA) for TIGTA System 1 environment every two years as required by FCD-1 and TD P 85-01.
  - Recommendation #24: Develop and disseminate TIGTA personnel a TIGTA System 1 Information System Contingency Plan (ISCP) that addresses purpose, scope, roles, responsibilities, management commitment, coordination, and compliance to facilitate the implementation of the contingency planning policy and associated contingency planning

controls. TIGTA should conduct disaster recovery and business continuity testing for the TIGTA System 1 on the frequency stipulated by the BIA.

FY 2017 FISMA Performance Audit

- Finding #1 – Mint: Information security policies, procedures, and security plans were outdated or incomplete.
  - Recommendation #2: Review and approve the Mint-wide information security policies and procedures on an annual basis.[12]
- Finding #6 – Mint: Account management activities were not compliant with System Security Policies.
  - Recommendation #23: Develop and implement a process to ensure that periodic user access reviews are completed for the selected system.
  - Recommendation #24: Ensure all active selected system accounts are consistently reviewed in accordance with NIST SP 800-53, Rev. 4.
  - Recommendation #25: Establish a process to ensure that all users are consistently completing a Rules of Behavior and Access Agreement form within a timely manner, and a process to revoke or disable accounts when a Rules of Behavior and an Access Agreement has not been completed.

FY 2015 FISMA Performance Audit

- Finding #1 – Mint: Logical account management activities were not compliant with policies.
  - Recommendation #1: Configure selected system to automatically disable user accounts after 120 days of last password change as stated within the SSP.
  - Recommendation #2: For the selected system, ensure access forms are completed, properly reviewed by the help desk prior to granting access, and centrally retained by the help desk.
- Finding #5 – Mint: Contract with third-party cloud service provider did not address the Federal Risk and Authorization Management Program (FedRAMP) requirements.
  - Recommendation #5: For the selected system, revisit the existing third-party CSP's contract and ensure the appropriate FedRAMP security clauses and requirements related to FISMA and NIST guidance are incorporated.
  - Recommendation #6: For the selected system, ensure that third-party CSP provides FISMA-related artifacts to demonstrate FISMA compliance to the Mint security compliance team.
  - Recommendation #7: For the selected system, remind the Mint contracting officer to ensure FedRAMP contract-specific clauses regarding compliance with FISMA and NIST are in place.

FY 2011 FISMA Performance Audit

- Finding #1 – TIGTA: Logical account management activities were not fully documented or consistently performed.
  - Recommendation #1: Based on TIGTA's planned corrective actions, we are not making a recommendation.

[12] Mint finalized the bureau-wide information security policy and procedures after the FISMA performance audit period of July 1, 2019 through June 30, 2019.

APPENDIX III – DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS'S FISMA 2019 QUESTIONS FOR INSPECTORS GENERAL

The information included in Appendix III represents Department of the Treasury's (Treasury) consolidated responses to questions from the Department of Homeland Security's (DHS) FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (FY 2019 IG FISMA Reporting Metrics).

We prepared comments on Treasury's responses to DHS questions based on an assessment of 10 information systems across 6 Treasury components. During the Federal Information Security Modernization Act of 2014 (FISMA) performance audit, we requested that Treasury management communicate its self-assessed maturity levels. We designed and executed test procedures to evaluate the effectiveness of management's security control program and practices over the five cybersecurity functions: identify, protect, detect, respond, and recover and the eight FISMA metric domains: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring (ISCM), incident response, and contingency planning, using the available options from CyberScope.[13] If we identified issues related to the metric, we assessed the metric at Ad Hoc (Level 1), Defined (Level 2), or Consistently Implemented (Level 3) and provided our explanations in the "Comment" section within this section about the findings or rationale for why Managed and Measurable (Level 4) was not met. We did not include any comments for Managed and Measurable (Level 4), or Optimized (Level 5) when it was the highest maturity level determined by our assessment. This Appendix includes the maturity levels that we assessed for the metrics. Per DHS's FY 2019 IG FISMA Reporting Metrics guidance, a security program is considered effective if the majority of the FY 2019 IG FISMA Reporting Metrics are at Level 4: Managed and Measurable.

In addition, the Treasury Inspector general for Tax Administration (TIGTA) performed an evaluation over the Internal Revenue Service (IRS) information systems and provided its evaluation to the Treasury Office of Inspector General (OIG) and KPMG for consolidation. TIGTA's observations are included in the section below, where applicable. We noted where the inclusion of TIGTA's assessment contributed to a maturity level of 1, 2, or 3 for a given metric. The information provided by TIGTA has not been subjected to KPMG audit procedures and, accordingly, we did not modify TIGTA's responses.

Function 0: Overall

Function 0 is the overall summary for the FISMA Performance Audit for Treasury. Functions 1–5 follow the 5 Cybersecurity Functions.

0.1 Please provide an overall IG self-assessment rating (Effective/Not Effective)

Not Effective

[13] *Supra* note 1.

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

KPMG Comments: Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, Treasury has established and maintained its information security program and practices for the five Cybersecurity Functions and eight FISMA Metric Domains. However, the program and practices were not fully effective as reflected in the deficiencies that we identified in Configuration Management, Identity and Access Management, Data Privacy and Protection, and Security Training. In addition, we did not assess any of the FISMA Metric Domains as Managed and Measurable (Level 4). We assessed Treasury's Information Security program for systems as Consistently Implemented (Level 3).

Function 1: Identify – Risk Management

1 To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800- 53, Rev. 4: CA-3, PM-5, and CM-8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2019 Chief Information Officer (CIO) FISMA Metrics: 1.1 and 1.4, OMB A-130)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization maintains a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third party systems), and system interconnections.

KPMG Comments: To achieve a Managed and Measurable level of Risk Management (RM) practices, the Treasury management should ensure that the information systems included in its inventory are subject to the monitoring processes defined within the organization's ISCM strategy.

FY 2017 Finding #1 for Mint, "Mint management did not update and approve the bureau-wide information security policies and procedures in accordance with Treasury Directive Publication (TD P) 85-01 and NIST SP 800-53, Rev. 4," remained open. Mint finalized its bureau-wide information security policies and procedures after the 2019 FISMA performance audit period of July 1, 2018 through June 30, 2019.

2 To what extent does the organization use 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 (NIST SP 800-53 Rev. 4: CA-7 and CM-8; NIST SP 800-137; NIST Interagency or Internal Reports (NISTIR) 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2019 CIO FISMA Metrics: 1.2 and 3.9.2; CSF: ID.AM-1)?

Maturity Level: **Managed and Measurable (Level 4)** – The organization ensures that the hardware assets connected to the network are covered by an organization-wide hardware asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy.

KPMG Comments: In the *Treasury Inspector General for Tax Administration – Fiscal Year Evaluation of the Internal Revenue Service's Cybersecurity Program Against the Federal Information Security Modernization Act* (Reference Number: 2019-20-082), dated September 24, 2019 (TIGTA - FY 2019 FISMA Evaluation of IRS report), TIGTA reported that the IRS has not identified and documented all of its current system hardware components. TIGTA[14] 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[15] 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 (NIST SP 800-53 Rev. 4: CA7, CM-8, and CM-10; NIST SP 800-137; NISTIR 8011; FEA Framework, v2; FY 2019 CIO FISMA Metrics: 3.10.1; CSF: ID.AM-2)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up- to-date inventory of software assets and licenses utilized in the organization's environment and uses this taxonomy to inform which assets can/cannot be introduced into the network.

KPMG Comments: To achieve a Managed and Measurable level of RM practices, the Treasury management should ensure that the software assets on the network (and their associated licenses) are covered by an organization-wide software asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy.

FY 2017 Finding #1 for Mint, "Mint management did not update and approve the bureau-wide information security policies and procedures in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4," remained open. Mint finalized its bureau-wide information security policies and procedures after 2019 FISMA performance audit period of July 1, 2018 through June 30, 2019.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported the IRS is still in the process of implementing systems for compiling a reliable software inventory. TIGTA[16] reported instances of software and associated licenses not being effectively managed and controlled.

[14] TIGTA, Ref. No. 2019-20-061, *Firewall Administration Needs Improvement* (Sept. 2019).
[15] TIGTA, Ref. No. 2018-20-041, *Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability* (July 2018).
[16] 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).

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 (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2019 CIO FISMA Metrics: 1.1; OMB M-19-03)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization's defined importance/priority levels for its information systems considers risks from the supporting business functions and mission impacts, including for high value assets, and is used to guide risk management decisions.

KPMG Comments: To achieve a Managed and Measurable level of RM practices, the Treasury management should ensure risk-based allocation of resources for the protection of high value assets through collaboration and data-driven prioritization.

FY 2017 Finding #1 for Mint, "Mint management did not update and approve the bureau-wide information security policies and procedures in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4," remained open. Mint finalized its bureau-wide information security policies and procedures after 2019 FISMA performance audit period of July 1, 2018 through June 30, 2019.

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 (NIST SP 800- 39; NIST SP 800-53 Rev. 4: PM-8, PM-9; CSF: ID RM-1– ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; NIST SP 800-37 (Rev. 2); NIST SP 800-161: Appendix E; CSF: ID.SC-1 – 2; SECURE Technology Act: s. 1326)?

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.

KPMG Comments: Not applicable

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 (NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA9, SA-12, and PM-9; NIST SP 800-161; CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. System security engineering principles are followed and include

assessing the impacts to the organizations information security architecture prior to introducing information system changes into the organization's environment.

KPMG Comments: To achieve a Managed and Measurable level of RM practices, the Treasury management should ensure its 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 (ICT) supply chain and the organization's information systems.

Additionally, FY 2017 Finding #1 for Mint, "Mint management did not update and approve the bureau-wide information security policies and procedures in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4," remained open. Mint finalized its bureau-wide information security policies and procedures after 2019 FISMA performance audit period of July 1, 2018 through June 30, 2019.

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 (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; OMB A-123; CFO Council ERM Playbook; NIST SP 800-37 (Rev. 2); OMB M19-03)?

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

KPMG Comments: To achieve a Managed and Measurable level of RM practices, the Treasury management should allocate its resources (people, processes, and technology) in a risk-based manner for stakeholders to effectively implement risk management activities. Further, the Treasury should ensure stakeholders are held accountable for carrying out their roles and responsibilities effectively.

Additionally, the Treasury should utilize an integrated risk management governance structure for implementing and overseeing an enterprise risk management (ERM) 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 (NIST SP 800-53 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2); OMB M-19-03, CSF v1.1, ID.RA-6)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently utilizes POA&Ms to effectively mitigate security weaknesses.

KPMG Comments: To achieve a Managed and Measurable level of RM practices, the Treasury management should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its POA&M activities and uses that

information to make appropriate adjustments, as needed, to ensure that its risk posture is maintained.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reviewed 52 weaknesses that the IRS identified during the annual testing of controls of the seven selected systems. Of those 52 weaknesses, TIGTA 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, TIGTA 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. TIGTA 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 (NIST SP 800-39; NIST SP 800-53 REV. 4: PL-2 and RA-1; NIST SP 800-30; CSF: Section 4.0; NIST SP 800-37 (Rev. 2))?

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

KPMG Comments: To achieve a Managed and Measurable level of RM practices, the Treasury management should consistently monitor the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level.

FY 2017 Finding #1 for Mint, "Mint management did not update and approve the bureau-wide information security policies and procedures in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4," remained open. Mint finalized its bureau-wide information security policies and procedures after 2019 FISMA performance audit period of July 1, 2018 through June 30, 2019.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 (CFO Council ERM Playbook; OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; SECURE Technology Act: s. 1326)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization ensures that information about risks is communicated in a timely and consistent manner to all internal and external stakeholders with a need-to-know. Furthermore, the organization actively shares information with partners to ensure that accurate, current information is being distributed and consumed.

KPMG Comments: To achieve a Managed and Measurable level of RM practices, the Treasury management should employ robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization. The Treasury should ensure the dashboards present 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, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (NIST SP 800-53 REV. 4: SA-4; NIST SP 800- 152; NIST SP 800-37 Rev. 2; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4).

Maturity Level: **Consistently Implemented (Level 3)** – The organization ensures that specific contracting language and SLAs are consistently included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services. Further, the organization obtains sufficient assurance, through audits, test results, or other forms of evaluation, that the security controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance.

KPMG Comments: To achieve a Managed and Measurable level of RM practices, the Treasury management should use qualitative and quantitative performance metrics (e.g., those defined within SLAs) 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 (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?

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.

KPMG Comments: To achieve a Managed and Measurable level of RM practices, the Treasury management should use automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems and data.

Performance Improvement Opportunity (PIO): DO, Mint, and TTB did not have an automated solution that provides centralized, enterprise wide view of risks.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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.

13.1 Please provide the assessed maturity level for the agency's Identify - Risk Management function.

Maturity Level: **Consistently Implemented (Level 3)**

KPMG Comments: We determined that Treasury's security program and practices for RM did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.

13.2 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?

KPMG Comments: According to DHS criteria, we assessed the RM overall maturity levels as Consistently Implemented, which is ineffective. Please refer to 13.1 for explanation.

PIO: BEP, Fiscal Service, and TTB did not develop an action plan that outlined its processes to address the supply chain risk management strategy and related policy and procedural requirements of the SECURE Technology Act. DO did not fully implement its action plan for supply chain risk management in accordance with the SECURE Technology Act.

In the July 2019 report, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges* (GAO-19-384), the Government Accountability Office (GAO) provided the following actions that the Secretary of the Treasury that the Treasury should take to improve Treasury's risk management program:

- Develop a cybersecurity risk management strategy that includes the key elements identified in this report.
- Establish a process for conducting an organization-wide cybersecurity risk assessment.
- Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions.

Function 2A: Protect – Configuration Management

14 To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: CM-1; NIST SP 800 - 128: Section 2.4)?

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

KPMG Comments: To achieve a Managed and Measurable level of Configuration Management (CM) practices, the Treasury management should ensure its resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, ensure stakeholders are held accountable for carrying out their roles and responsibilities effectively.

PIO: Although Fiscal Service conducted workforce assessments to identify gaps in its resource/workforce, Fiscal Service was unable to provide evidence of addressing the identified gaps in its workforce assessment to enhance and improve its Configuration Management program.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53 REV. 4: CM-9)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization has consistently implemented an organization wide configuration management plan and has integrated its plan with its risk management and continuous monitoring programs. Further, the organization utilizes lessons learned in implementation to make improvements to its plan.

KPMG Comments: To achieve a Managed and Measurable level of CM practices, the Treasury management should monitor, analyze, and report to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plan, use this information to take corrective actions when necessary, and ensure that data supporting the metrics is 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) (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: 2.2.1)

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its policies and procedures for managing the configurations of its information systems. Further, the organization utilizes lessons learned in implementation to make improvements to its policies and procedures.

KPMG Comments: To achieve a Managed and Measurable level of CM practices, the Treasury management should monitor, analyze, and report on the qualitative and quantitative performance measures used to gauge the effectiveness of its configuration management policies and procedures and ensure that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported that 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 (NIST SP 800-53 REV. 4: CM-2 and CM-8; FY 2019CIO FISMA Metrics: 1.1, 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently records, implements, and maintains under configuration control, baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures.

KPMG Comments: In the Findings section of this report, we reported that BEP management did not consistently review, update, and approve configuration baselines for the BEP System 1 production database and operating system server in a timely manner.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported that 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 TIGTA 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[17] and the GAO[18] 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? (NIST SP 800-53 REV. 4: CM-6, CM-7, and SI-2; FY 2019CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on least functionality. Further, the organization consistently utilizes SCAP-validated software assessing (scanning) capabilities against all systems on the network (see inventory from questions #1 - #3) to assess and manage both code-based and configuration-based vulnerabilities.

KPMG Comments: In the Findings section of this report, we reported that Fiscal Service did not formally document and approve security configuration baseline documentation or configuration baseline deviations for Fiscal Service System 1. Although management conducted security compliance scans using bureau-wide baselines, management did not specifically tailor the baselines used in the scans to Fiscal Service System 1. For BEP, we reported that BEP management could not provide evidence of its remediation for 5 high vulnerabilities identified during Security Content Automation Protocol (SCAP) configuration baseline compliance scans and 2 high vulnerabilities identified during vulnerability scans for BEP System 1.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 TIGTA 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.

---

[17] 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).

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

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20,Control 4.5; FY 2019CIO FISMA Metrics: 2.13; CSF: ID.RA-1; DHS Binding Operational Directive (BOD)15-01; DHS BOD 18-02)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its flaw remediation policies, procedures, and processes and ensures that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner. In addition, the organization patches critical vulnerabilities within 30 days.

KPMG Comments: To achieve a Managed and Measurable level of CM practices, the Treasury management should centrally manage its flaw remediation process and utilize automated patch management and software update tools for operating systems, where such tools are available and safe.

For DO System 1, DO management issued a self-identified weakness: "DO is developing requirements for an enhanced monitoring program, with expected delivery in FY 2020."

For findings related to this metric for BEP and Fiscal Service, refer to comments for question 18.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 TIGTA 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[19] and the GAO[20] reported that the IRS did not remediate high-risk vulnerabilities or install security patches on systems in a timely manner.

[19] 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).

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

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-08-05)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization has consistently implemented its TIC approved connections and critical capabilities that it manages internally. The organization has consistently implemented defined TIC 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.

KPMG Comments: Consistently Implemented (Level 3) is the highest level of maturity 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 CCB, as appropriate (NIST SP 800-53 REV. 4: CM-2 and CM-3; CSF: PR.IP-3)?

Maturity Level: **Consistently Implemented (Level 3)** – 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.

KPMG Comments: To achieve a Managed and Measurable level of CM practices, the Treasury management should monitor, analyze, and report qualitative and quantitative performance measures on the effectiveness of its change control activities and ensure that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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

[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).

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?

Maturity Level: **Consistently Implemented (Level 3)**

KPMG Comments: According to DHS criteria, we assessed the CM overall maturity level as Consistently Implemented, which is ineffective according to DHS guidance. Please refer to 45.1 for explanation.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 2B: Protect – Identity and Access Management

23 To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

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

KPMG Comments: To achieve a Managed and Measurable level of Identity and Access Management (IA) practices, the Treasury management should ensure resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement identity, credential, and access management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

PIO: Although Mint has performed an analysis of the resources needed to support ICAM activities, Mint lacked a comprehensive strategy to address identified resource gaps.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 (FICAM)?

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

KPMG Comments: To achieve a Managed and Measurable level of IA practices, the Treasury management should transition to its desired or "to-be" ICAM architecture and integrate its ICAM strategy and activities with its enterprise architecture and the FICAM segment architecture.

PIO: Although Mint has a policy for the implementation of PIV Cards and plans for strong authentication, Mint lacked a comprehensive ICAM strategy that include the streamlining of the collection and sharing of digital identity data, process improvement opportunities, and modernizing physical and logical access control system infrastructure.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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) (NIST SP 800-53 REV. 4: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

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.

KPMG Comments: To achieve a Managed and Measurable level of IA practices, the Treasury management should use automated mechanisms (e.g. machine-based, or user based enforcement), where appropriate, to manage the effective implementation of its policies and procedures. Examples of automated mechanisms include network segmentation based on the label/classification of information stored on the servers; automatic removal/disabling of temporary/emergency/inactive accounts, use of automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews.

PIO: Mint lacked a comprehensive ICAM strategy that addresses purpose, scope, roles, responsibilities, and compliance.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 (NIST SP 800-53 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11)?

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

KPMG Comments: In the Findings section of this report, we reported that Mint was unable to provide evidence that for Mint System 1 some selected users, completed background investigations, signed non-disclosure agreements (NDAs), signed rules of behavior (ROB) forms, and completed security awareness training within the time frame required by TD P 85-01. Additionally, the Mint Information Security Policy did not clearly define the requirements for NDAs and ROBs to be signed before granting information system access.

FY 2017 Finding #1 for Mint, "Mint management did not update and approve the bureau-wide information security policies and procedures in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4," remained open. Mint finalized its bureau-wide information security policies and procedures after 2019 FISMA performance audit period of July 1, 2018 through June 30, 2019.

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 (NIST SP 800- 53 REV. 4: AC-8, PL-4, and PS6)?

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.

KPMG Comments: Not applicable

28 To what extent has the organization implemented strong authentication mechanisms (Personal Identification Verification [PIV] or a Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.4 and 2.7; CSF: PR.AC-1 and 6; and Cybersecurity Sprint)?

Maturity Level: **Managed and Measurable (Level 4)** – All non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems.

KPMG Comments: For DO System 1, DO management issued a self-identified weakness: "DO System 1 does not require multi-factor (specifically PIV) authentication."

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 (PIV or a Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01; and Cybersecurity Sprint)?

Maturity Level: **Managed and Measurable (Level 4)** – All privileged users, including those who can make changes to DNS records, utilize strong authentication mechanisms to authenticate to applicable organizational systems.

KPMG Comments: For DO System 1, DO management issued a self-identified weakness: "DO System 1 does not require multi-factor (specifically PIV) authentication."

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 (FY 2019 CIO FISMA Metrics: 2.3 and 2.5; NIST SP 800-53 REV. 4: AC-1, AC-2 (2), and AC-17; CSIP; DHS Emergency Directive (ED) 19- 01; CSF: PR.AC-4).

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.

KPMG Comments: In the Findings section of this report, we reported that DO did not conduct semi-annual periodic user access reviews for DO System 2 privileged users.

FY 2017 Finding #1 for Mint, "Mint management did not update and approve the bureau-wide information security policies and procedures in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4," remained open. Mint finalized its bureau-wide information security policies and procedures after 2019 FISMA performance audit period of July 1, 2018 through June 30, 2019.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 (NIST SP 800-53 REV. 4: AC-17 and SI-4; CSF: PR.AC-3; and FY 2019 CIO FISMA Metrics: 2.10)?

Maturity Level: **Managed and Measurable (Level 4)** – The organization ensures that end user devices have been appropriately configured prior to allowing remote access and restricts the ability of individuals to transfer data accessed remotely to non-authorized devices.

KPMG Comments: In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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?

KPMG Comments: According to DHS criteria, we assessed the IA overall maturity level as Consistently Implemented, which is ineffective according to DHS guidance. Please refer to 45.1.

PIO: Fiscal Service's network account creation standard operating procedures did not completely reflect the account creation and user account enablement process that is in place.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported the IRS Identity and Access Management Program is not effective because it did not meet the Managed and Measurable maturity level.

[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).

Function 2C: Protect – Data Protection and Privacy

33 To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; NIST SP 800-37 (Rev. 2); OMB M-18- 02; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its privacy program by:

- Dedicating appropriate resources to the program.
- Maintaining an inventory of the collection and use of Personally Identifiable Information (PII).
- Conducting and maintaining privacy impact assessments and system of records notices for all applicable systems.
- Reviewing and removing unnecessary PII collections on a regular basis (i.e., Social Security Numbers (SSNs)).

KPMG Comments: In the Finding section of this report, we reported that although Mint has taken steps to implement privacy safeguards for PII and conduct system level privacy assessments, Mint management has not fully established a Mint bureau-wide data protection and privacy program.

PIO: Fiscal Service was in the process of developing and implementing a strategy to integrate the recommendations from the Cyber Clean Assessment Report into its Privacy Program during the FY 2019 FISMA audit period of July 1, 2018 through June 30, 2019. The strategy to implement those recommendations was drafted in May 2019, and Fiscal Service plans to execute its strategy in FY 2020.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported the IRS did not provide sufficient evidence to show that it reviews and removes unnecessary PII collections on a regular basis. In addition, TIGTA[25] reported that the Privacy, Government Liaison, and Disclosure Office does not actively review PII collections on a regular basis to remove unnecessary PII.

34 To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (NIST SP 800-53 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2019 CIO FISMA Metrics: 2.8; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)?

- Encryption of data at rest
- Encryption of data in transit
- Limitation of transfer to removable media
- Sanitization of digital media prior to disposal or reuse

Maturity Level: **Consistently Implemented (Level 3)** – The organization's policies and procedures have been consistently

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

implemented for the specified areas, including: (i) use of FIPS-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data.

KPMG Comments: In the Findings section of this report, we reported that Fiscal Service's supporting documentation evidencing the encryption of data in transit was unavailable for Fiscal Service System 2; thus, the encryption status of data in transit could not be verified. Furthermore, database encryption was not enforced for Fiscal Service Systems 1 and 2. Fiscal Service was unable to identify personnel who could demonstrate that the Fiscal Service System 2 was encrypted while in transmit within the mainframe environment. In addition, Fiscal Service is currently completing an ongoing bureau-wide project to encrypt data at rest; therefore, several Fiscal Service systems, including Fiscal Service Systems 1 and 2, do not have encryption controls fully enforced.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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? (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2019 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

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 PII. Also, suspected malicious traffic is quarantined or blocked.

KPMG Comments: To achieve a Managed and Measurable level of Data Protection and Privacy (DP) practices, the Treasury management should analyze qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. The Treasury also should conduct exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses. Further, the Treasury should monitor its DNS infrastructure for potential tampering, in accordance with its ISCM strategy.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported the IRS did not provide sufficient support that it conducts

[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).

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? (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2018 Senior Agency Official for Privacy (SAOP) FISMA metrics; OMB M-17-12; and OMB M-17- 25)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its Data Breach Response plan. Additionally, the breach response team participates in table-top exercises and uses lessons learned to make improvements to the plan as appropriate. Further, the organization is able to identify the specific individuals affected by a breach, send notice to the affected individuals, and provide those individuals with credit monitoring and repair services, as necessary.

KPMG Comments: To achieve a Managed and Measurable level of DP practices, the Treasury management should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate. The Treasury should ensure 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 (NIST SP 800-53 REV. 4: AR-5)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, 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 PII or activities involving PII receive role-based privacy training at least annually. Additionally, the organization ensures that individuals certify acceptance of responsibilities for privacy requirements at least annually.

KPMG Comments: In the Finding section of this report, we reported that only 81 percent of the required Mint personnel that are assigned security roles and responsibilities completed the role-based specialized IT security training on an annual basis. Additionally, Mint does not have effective mechanisms in place to ensure the timely completion of role-based Specialized IT Security Training.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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?

KPMG Comments: According to DHS criteria, we assessed the DP overall maturity level as Consistently Implemented, which is ineffective according to DHS guidance. Please refer to 45.1.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported the IRS data protection and privacy program is not effective because it did not meet the Managed and Measurable maturity level.

Function 2D: Protect – Security Training

39 To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST SP 800- 53 REV. 4: AT-1; and NIST SP 800-50).

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

KPMG Comments: To achieve a Managed and Measurable level of Security Training (ST) practices, the Treasury management should ensure resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

PIO: Although Mint's security awareness program was defined, Mint's security awareness and training program is not adequately resourced or adequately communicated across the organization to consistently implement its security awareness and training program.

In the TIGTA - FY 2019 FISMA Evaluation of IRS, TIGTA reported 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 (NIST SP 800-53 REV. 4: AT-2 and AT-3; NIST SP 800- 50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS/SANS Top 20: 17.1)?

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.

KPMG Comments: To achieve a Managed and Measurable level of ST practices, the Treasury management should address its identified knowledge, skills, and abilities gaps through training or hiring of additional staff/contractors.

PIO: Although the Mint information Security Policy and the Cyber Security Training Policy document the user training requirements, the requirements for updating these policies based on workforce needs and changes in the risk environment were not defined. Fiscal Service's specialized and security awareness training program was not updated based on an assessment of workforce needs.

In the TIGTA - FY 2019 FISMA Evaluation of IRS, TIGTA reported 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, the 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, phishing simulation tools), frequency of training, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT- 1).

Maturity Level: **Consistently Implemented (Level 3)** – The organization has consistently implemented its organization-wide security awareness and training strategy and plan.

KPMG Comments: To achieve a Managed and Measurable level of ST practices, the Treasury management should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The organization should ensure that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

FY 2017 Finding #1 for Mint, "Mint management did not update and approve the bureau-wide information security policies and procedures in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4," remained open. Mint finalized its bureau-wide information security policies and procedures after the FISMA performance audit period of July 1, 2019 through June 30, 2019.

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) (NIST SP 800-53 REV. 4: AT-1 through AT-4; and NIST SP 800-50).

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 or training, and/or disciplinary action, as appropriate.

KPMG Comments: PIO: Fiscal Service security awareness training policies and procedures did not define qualitative and quantitative performance measures.

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 (NIST SP 800-53 REV. 4: AT-2; FY 2019 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).

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 or training, and/or disciplinary action, as appropriate.

KPMG Comments: Not applicable

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) (NIST SP 800- 53 REV. 4: AT-3 and AT-4; FY 2019 CIO FISMA Metrics: 2.15)?

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 or training, and/or disciplinary action, as appropriate.

KPMG Comments: Not applicable

45.1 Please provide the assessed maturity level for the agency's Protect Function.

Maturity Level: **Consistently Implemented (Level 3)**

KPMG Comments: We determined that Treasury's security program and practices for CM, IA, and DP did not meet the

Managed and Measurable maturity (Level 4). We assessed the majority of these metrics at the Consistently Implemented maturity level.

45.2 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?

KPMG Comments: According to DHS criteria, we assessed the ST overall maturity level as Managed and Measurable, which is effective.

PIO: BEP did not request for feedback on the bureau's security awareness content and could not provide evidence of changes to the security awareness content based on feedback. However, BEP began the process to implement requests for feedback on its security awareness content in the fourth quarter of FY 2019 and plans to execute changes to the security awareness content in FY 2020 based on the feedback. Fiscal Service Security Awareness Training strategies and plans did not define qualitative and quantitative performance measures for specialized security training.

Function 3: Detect – ISCM

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 (NIST SP 800-37 (Rev. 2); NIST SP 800-137: Sections 3.1 and 3.6)?

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.

KPMG Comments: To achieve a Managed and Measurable level of ISCM practices, the Treasury management should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its ISCM strategy and make updates, as appropriate. The Treasury should ensure that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported while the IRS has developed and communicated its ISCM strategy and procedures across its enterprise, it has not provided TIGTA with sufficient evidence to meet the Managed and Measurable 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 (NIST SP 800-53 REV. 4: CA-7, NISTIR 8011) (Note: The overall maturity level should take into consideration the maturity of question 49)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization's ISCM policies and procedures have been consistently implemented for the specified areas. The organization also consistently captures lessons learned to make improvements to the ISCM policies and procedures.

KPMG Comments: To achieve a Managed and Measurable level of ISCM practices, the Treasury management should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its ISCM policies and procedures and make updates, as appropriate. The Treasury should ensure that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; and FY 2019 CIO FISMA Metrics)?

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

KPMG Comments: To achieve a Managed and Measurable level of ISCM practices, the Treasury management should allocate its resources (people, processes, and technology) in a risk-based manner for stakeholders to effectively implement ISCM activities. Further, the Treasury should ensure stakeholders are held accountable for carrying out their roles and responsibilities effectively.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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[28] 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 (NIST SP 800- 137: Section 2.2; NIST SP 800- 53 REV. 4: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2); NISTIR 8011; OMB M-14-03; OMB M-19-03)?

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

KPMG Comments: To achieve a Managed and Measurable level of ISCM practices, the Treasury management should utilize results of security control assessments and monitoring to maintain ongoing authorizations of information systems

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 (NIST SP 800-137)?

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

KPMG Comments: To achieve a Managed and Measurable level of ISCM practices, the Treasury management should ensure it is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported the IRS has an ISCM program plan in place to

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

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

51.1 Please provide the assessed maturity level for the agency's Detect Function.

Maturity Level: **Consistently Implemented (Level 3)**

KPMG Comments: We determined that Treasury's security program and practices for ISCM did not meet the Managed and Measurable maturity (Level 4). We assessed the majority of these metrics at the Consistently Implemented maturity level.

51.2 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?

KPMG Comments: According to DHS criteria, we assessed the ISCM overall maturity level as Consistently Implemented, which is ineffective. Please refer to 51.1 for further explanation.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported the IRS ISCM program is not effective because it did not meet the Managed and Measurable maturity level.

Function 4: Respond – Incident Response

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 (NIST SP 800-53 REV. 4: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800- 184; OMB M-17-25; OMB M- 17-09; FY 2018 CIO FISMA Metrics: 4.2; CSF: RS.RP-1; Presidential Policy Direction (PPD) 41)? (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.

KPMG Comments: To achieve a Managed and Measurable level of Incident Response (IR) practices, the Treasury management should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies, as appropriate. The Treasury should ensure that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2019 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

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

KPMG Comments: To achieve a Managed and Measurable level of IR practices, the Treasury management should ensure its resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement incident response activities. Further, the Treasury should ensure stakeholders are held accountable for carrying out their roles and responsibilities effectively.

54 How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-18-02; CSF: DE.AE-1, PR.DS-6, RS.AN-4, and PR.DS- 8; and US-CERT Incident Response Guidelines)

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently utilizes its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements, and analyzes precursors and indicators generated by, for example, the following technologies: intrusion detection/prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity checking software.

KPMG Comments: To achieve a Managed and Measurable level of IR practices, the Treasury management should utilize 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 Treasury should maintain a comprehensive baseline of network operations and expected data flows for users and systems.

55 How mature are the organization's processes for incident handling (NIST SP 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its containment strategies, incident eradication processes, processes to remediate vulnerabilities that may have been exploited on the target system(s), and

recovers system operations.

KPMG Comments: To achieve a Managed and Measurable level of IR practices, the Treasury management should manage and measure the impact of successful incidents and ensure it is able to quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.

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 (FISMA; OMB M-18-02; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 4; DHS Cyber Incident Reporting Unified Message)

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

KPMG Comments: To achieve a Managed and Measurable level of IR practices, the Treasury management should ensure incident response metrics are used to measure and manage the timely reporting of incident information to departmental officials and external stakeholders.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported the IRS did not provide sufficient evidence to support the Managed and Measurable maturity level.

57 To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support (NIST SP 800- 86; NIST SP 800-53 REV. 4: IR- 4; OMB M-18-02; Presidential Policy Direction [PPD]-41).

Maturity Level: **Managed and Measurable (Level 4)** – The organization utilizes Einstein 3 Accelerated to detect and proactively block cyber-attacks or prevent potential compromises.

KPMG Comments: Not applicable

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 (SIEM) 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 (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44)

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

KPMG Comments: To achieve a Managed and Measurable level of IR practices, the Treasury management should use technologies for monitoring and analyzing qualitative and quantitative performance across the entire Department and ensure it is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities.

59.1 Please provide the assessed maturity level for the agency's Respond - Incident Response function.

Maturity Level: **Consistently Implemented (Level 3)**

KPMG Comments: We determined that Treasury's security program and practices for IR did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.

59.2 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 about and based on all testing performed, is the incident response program effective?

KPMG Comments: We have no additional information that was not already covered in questions 52 to 58 above. According to DHS criteria, we assessed the IR overall maturity level as Consistently Implemented, which is ineffective. Please refer to 59.1 for further explanation.

Function 5: Recover – Contingency Planning

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 (NIST SP 800-53 REV. 4: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

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

KPMG Comments: To achieve a Managed and Measurable level of Contingency Planning (CP) practices, the Treasury management should ensure resources (people, processes, and technology) are allocated in a risk-based manner for

stakeholders to effectively implement system contingency planning activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

PIO: Although Mint documented and distributed the information system contingency planning roles and responsibilities, individuals assigned to contingency planning roles and responsibilities are not consistently performing their assigned contingency planning roles.

In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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) (NIST SP 800-34; NIST SP 800-161; CSF: ID.BE-5, PR.IP-9, and ID.SC-5)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its defined information system contingency planning policies, procedures, and strategies. In addition, the organization consistently implements technical contingency planning considerations for specific types of systems, including but not limited to methods such as server clustering and disk mirroring. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of information system contingency planning policies, procedures, strategy, and processes to update the program.

KPMG Comments: To achieve a Managed and Measurable level of CP practices, the Treasury management should ensure it understands and manages its ICT supply chain risks related to contingency planning activities. As appropriate, the Treasury should: integrate ICT supply chain concerns into its contingency planning policies and procedures, define and implement a contingency plan for its ICT supply chain infrastructure, apply appropriate ICT supply chain controls to alternate storage and processing sites, consider alternate telecommunication service providers for its ICT 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 (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17- 09; FY 2019 CIO FISMA Metrics: 5.1; CSF:ID.RA-4)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization incorporates the results of organizational and system level BIAs into strategy and plan development efforts consistently. System level Business Impact Analysis (BIAs) are integrated with the organizational level BIA and include: characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system

resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high value assets.

KPMG Comments: Consistently Implemented (Level 3) is the highest level of maturity for this metric.

63 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800- 53 REV. 4: CP-2; NIST SP 800- 34; FY 2019 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

Maturity Level: **Consistently Implemented (Level 3)** – Information system contingency plans are consistently developed and implemented for systems, as appropriate, and include organizational and system level considerations for the following phases: activation and notification, recovery, and reconstitution. In addition, system level contingency planning development/maintenance activities are integrated with other continuity areas including organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan (as appropriate), and occupant emergency plans.

KPMG Comments: To achieve a Managed and Measurable level of CP practices, the Treasury management should 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 (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2019 CIO FISMA Metrics: 5.1; CSF: ID.SC-5 and CSF: PR.IP-10)?

Maturity Level: **Consistently Implemented (Level 3)** – Processes for information system contingency plan testing and exercises are consistently implemented. ISCP testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/Continuity of Operation Plan (COOP)/Business Continuity Plan (BCP).

KPMG Comments: To achieve a Managed and Measurable level of CP practices, the Treasury management should coordinate information system contingency plan testing with organizational elements responsible for related plans.

FY 2017 Finding #1 for Mint, "Mint management did not update and approve the bureau-wide information security policies and procedures in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4," remained open. Mint finalized its bureau-wide information security policies and procedures after the FISMA performance audit period of July 1, 2018 through June 30, 2019.

65 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53 REV. 4: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3;

FCD-1; NIST CSF: PR.IP-4; FY 2019 CIO FISMA Metrics: 5.1.1; and National Archives and Records Administration [NARA] guidance on information systems security records)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and Redundant Array of Independent Disks (RAID), as appropriate. Alternate processing and storage sites are chosen based upon risk assessments which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized, and are not subject to the same physical and/or cybersecurity risks as the primary sites. In addition, the organization ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site. Furthermore, backups of information at the user- and system-levels are consistently performed and the confidentiality, integrity, and availability of this information is maintained.

KPMG Comments: In the TIGTA - FY 2019 FISMA Evaluation of IRS report, TIGTA reported 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 (CSF: RC.CO-3; NIST SP 800-53 REV. 4: CP-2 and IR-4)?

Maturity Level: **Consistently Implemented (Level 3)** – Information on the planning and performance of recovery activities is consistently communicated to relevant stakeholders and executive management teams, who utilize the information to make risk based decisions.

KPMG Comments: To achieve a Managed and Measurable level of CP practices, the Treasury management should ensure metrics on the effectiveness of recovery activities are communicated to relevant stakeholders and the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.

PIO: BEP and TTB did not complete the FY 2019 Eagle Horizon Exercise After-Action Report and Improvement Plan process during the FY 2019 FISMA audit period.

67.1 Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.

Maturity Level: **Consistently Implemented (Level 3)**

KPMG Comments: We determined that Treasury's security program and practices for CP did not meet the Managed and

Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.

67.2 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?

KPMG Comments: We have no additional information that was not already covered in questions 60 to 66 above. According to DHS criteria, we assessed the CP overall maturity level as Consistently Implemented, which is ineffective. Please refer to 67.1 for further explanation

Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	10
Managed and Measurable	2
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	8
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	4
Managed and Measurable	3
Optimized	1
Function Rating: Consistently Implemented (Level 3)	

Function 2C: Protect – Data Protection and Privacy

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

Function 2D: Protect – Security Training

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

Function 3: Detect - ISCM

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

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	6
Managed and Measurable	1
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	7
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's security program and practices RM did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 2A: Protect – Configuration Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's security program and practices for CM did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 2B: Protect – Identity and Access Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's security program and practices for IA did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 2C: Protect – Data Protection and Privacy	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's security program and practices for DP did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 2D: Protect – Security Training	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	We determined that Treasury's security program and practices for ST met the Managed and Measurable maturity level 4.
Function 3: Detect - ISCM	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's security program and practices for ISCM did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's security program and practices for IR did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's security program and practices for CP did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Overall	Not Effective	Not Effective	Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, Treasury has established and maintained its information security program and practices for the five Cybersecurity Functions and eight FISMA Metric Domains. However, the program and practices were not fully effective as reflected in the deficiencies that we identified in CM, IA, DP, and ST. In addition, we did not assess any of the FISMA Metric Domains as Managed and Measurable (Level 4). We assessed Treasury's Information Security program for systems as Consistently Implemented (Level 3).

APPENDIX IV – APPROACH TO SELECTION OF SUBSET OF SYSTEMS

In executing the Fiscal Year (FY) 2019 Federal Information Security Modernization Act of 2014 (FISMA) Unclassified performance audit, we assessed relevant control areas and control techniques from National Institute of Standards and Technology (NIST) for the Department of Treasury's (Treasury or Department) in-scope systems at the Bureau of Engraving and Printing (BEP), Departmental Offices (DO), Bureau of the Fiscal Service, (Fiscal Service), United States Mint (Mint), Office of the Comptroller of the Currency (OCC), and the Alcohol and Tobacco Tax and Trade Bureau (TTB).

In order to select our sample, working with Treasury Office of Inspector General (OIG), we judgmentally selected 10 systems that were operated and/or managed by 6 bureaus.

Approach

With the assistance of DO management, we obtained a listing of Treasury's FISMA inventory of systems. All Treasury bureaus and offices were required to register their IT systems with the Department. KPMG LLP (KPMG) considered the following factors during the selection process:

- Treasury High Value Asset[29] listing;
- total number of financial and operational systems per bureau; excluded were systems in the implementation, development, and disposal phases;
- whether a particular system was tested in the FYs 2016, 2017, and 2018 FISMA performance audits; and
- whether a particular system consists of personally identifiable information (PII)

Once we determined the subset of systems to select, we then employed a random sampling approach to determine the in-scope operational information systems to support the FY 2019 FISMA Performance Audit for Treasury's unclassified systems.

Table 3 summarizes our considerations for selecting the in-scope systems for the 2019 performance audit.

Table 3: *Considerations for selecting systems for the FY 2019 FISMA performance audit.*

#	Bureau	Total # of Operational Info. Systems	Number of Information Systems Considered After Analysis	Number of Information Systems Selected
1	BEP	12	9	1
2	DO[30]	40	33	2
3	Fiscal Service	60	54	2[31]
4	Mint	20	17	1
5	OCC	40	38	2
6	TTB	26	24	2
	Totals	**198**	**175**	**10**

[29] High Value Assets are those assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people.

[30] DO went through a restructuring where several systems were broken off and realigned internally based on their function. In order for Treasury FISMA Inventory Management System (TFIMS) to recognize this level of granularity, two new internal divisions were entered into TFIMS as bureaus, but still continue to reside within DO.

[31] One of these systems was randomly selected from the High Value Asset listing.

Using a random number generator, KPMG randomly selected 10 of 175 operational systems. **Table 4** below denotes the selected application and systems for the 2019 performance audit.

Table 4: *Selected application and systems for the 2019 performance audit.*

Bureau	System	FIPS 199	System Type	Financial System	High Value Asset	PII
BEP	BEP System 1	Moderate	Minor Application	No	No	Yes
DO	DO System 1	Moderate	Minor Application	No	No	No
DO	DO System 2	High	Major Application	No	No	Yes
Fiscal Service	Fiscal Service System 1	High	General Support System (GSS)	No	Yes	Yes
Fiscal Service	Fiscal Service System 2	Moderate	Major Application	Yes	No	Yes
Mint	Mint System 1	Moderate	Major Application	No	No	Yes
OCC	OCC System 1	Moderate	Major Application	No	No	No
OCC	OCC System 2	Moderate	GSS	No	No	Yes
TTB	TTB System 1	Moderate	Minor Application	No	No	No
TTB	TTB System 2	Moderate	Minor Application	No	No	No

APPENDIX V – GLOSSARY OF TERMS

Acronym	Definition
ACIOCS	Associate Chief Information Officer for Cyber Security
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
ATO	Authority to Operate
BCP	Business Continuity Planning
BEP	Bureau of Engraving and Printing
BIA	Business Impact Analysis
BLSR	Baseline Security Requirements
BOD	Building Operational Directors
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Plan
CSIRC	Computer Security Incident Response Center
CSP	Cloud Service Provider
CSS	Cyber Security Sub-Council
Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity
DHS	Department of Homeland Security
DNS	Domain Name System
DO	Departmental Offices
EAC	Enterprise Application CyberSecurity
ED	Emergency
EIC	Enterprise Infrastructure CyberSecurity
FCD-1	Federal Continuity Directive 1
FedRAMP	Federal Risk and Authorization Management Program
FinCEN	Financial Crimes Enforcement Network
FIPS	Federal Information Processing Standards
Fiscal Service	Bureau of the Fiscal Service
FISMA	Federal Information Security Modernization Act of 2002
FY	Fiscal Year
FY 2019 IG FISMA Reporting Metrics	Fiscal Year 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics
HSPD	Homeland Security Presidential Directive
IA	Identity and Access Management
IG	Inspector General
IR	Incident Response
IRS	Internal Revenue Service

Acronym	Definition
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
ISSO	Information Systems Security Officer
ISCP	Information System Contingency Plan
IT	Information Technology
KPMG	KPMG LLP
Mint	United States Mint
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Reports
OCC	Office of the Comptroller of the Currency
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIO	Performance Improvement Opportunity
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestone
RA	Risk Assessment
Rev.	Revision
RM	Risk Management
ROB	Rules of Behavior
SA&A	Security Assessment and Authorization
SDLC	System Development and Lifecycle
SI	System and Information Integrity
SIGTARP	Special Inspector General for the Troubled Asset Relief Program
SECURE	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure
SO	System Owner
SOAP	Senior Agency Official for Privacy
SOP	Standard Operating Procedure
SP	Special Publication
SSN	Social Security Number
SSP	System Security Plan
ST	Security Training
TARP	Troubled Asset Relief Program
TCSIRC	Treasury Computer Security Incident Response Capability
TD P	Treasury Directive Publication
TIGTA	Treasury Inspector General for Tax Administration
Treasury	Department of the Treasury
TTB	Alcohol and Tobacco Tax and Trade Bureau

ATTACHMENT 2

Treasury Inspector General for Tax Administration –
Federal Information Security Modernization Act Report for Fiscal Year 2019
September 24, 2019

This Page Intentionally Left Blank

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

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

Abbreviations

Abbreviation	Description
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 Identity and Access Management Data Protection and Privacy Security Training	 Defined (Level 2) Consistently Implemented (Level 3) Consistently Implemented (Level 3) Managed and Measurable (Level 4)	No
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).

This Page Intentionally Left Blank

REPORT WASTE, FRAUD, AND ABUSE

Treasury OIG Hotline: 1-800-359-3898
Hotline@oig.treas.gov

Gulf Coast Restoration Hotline: 1-855-584.GULF (4853)
gulfcoastrestorationhotline@oig.treas.gov

Access Treasury OIG reports and other information online:
www.treasury.gov/about/organizational-structure/ig