Audit Report

OIG-19-007

INFORMATION TECHNOLOGY: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2018 Performance Audit

October 31, 2018

Office of Inspector General

Department of the Treasury

THIS PAGE INTENTIONALLY LEFT BLANK

OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 31, 2018

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 2018 Performance Audit*

We are pleased to transmit the following reports:

- *Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2018 Performance Audit*, dated October 31, 2018, (Attachment 1); and

- *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018*, dated September 21, 2018 (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 as KPMG identified 8 deficiencies within 3 of the 5 Cybersecurity Functions and within 4 of the 8 FISMA program areas. Accordingly, KPMG made 24 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 yet implemented, 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 2018 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 2018 Performance Audit
October 31, 2018

THIS PAGE INTENTIONALLY LEFT BLANK

Department of the Treasury
Federal Information Security Modernization Act
Fiscal Year 2018 Performance Audit

October 31, 2018

KPMG LLP
1676 International Drive, Suite 1200
McLean, VA 22102

Department of the Treasury
Federal Information Security Modernization Act Fiscal Year 2018
Performance Audit

Table of Contents

FISMA Performance Audit Report

Appendices

KPMG LLP
1676 International Drive
McLean, VA 22102

The Honorable Eric Thorson
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 2018 Performance Audit

Dear Mr. Thorson:

This report presents the results of our independent performance audit of the Department of the Treasury's (Treasury) information security program and practices for its unclassified systems. The Federal Information Security Modernization Act of 2014 (FISMA) requires Federal agencies, including the 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 to collect FISMA metrics. Appendix III, *Department of the Treasury's Consolidated Response to DHS's FISMA 2018 Questions for Inspectors General,* dated May 24, 2018, 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. 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, 2017 through June 20, 2018. As part of our audit, we responded to the DHS Fiscal Year DHS *FISMA 2018 Questions for Inspectors General*, dated May 24, 2018, and assessed the maturity levels on behalf of the Treasury Office of Inspector General. The scope of our work did not include the Internal Revenue Service, as that bureau was evaluated by the Treasury Inspector General for Tax Administration (TIGTA). The TIGTA report is appended to this report and its findings are included in Appendix III, *Department of the Treasury's Consolidated Response to DHS's FISMA 2018 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[1] and 8 FISMA Metric Domains.[2] However, the program was not effective according to DHS criteria and as reflected in the 8 deficiencies within 3 of the 5 Cybersecurity Functions and within 4 of the 8 FISMA program areas that we identified as follows:

Cybersecurity Function: Identify

1. Security Assessment and Authorization (SA&A) processes were not consistently completed at the United States Mint (Mint) and the U.S. TIGTA. (Risk Management)
2. System Security Plans were not always updated in accordance NIST Special Publication (SP) 800-53, Revision (Rev.) 4, Treasury Directive Publication (TD P) 85-01, and bureau and office information security policies at Bureau of Engraving and Printing (BEP) and the Office of the Comptroller of the Currency (OCC). (Risk Management)
3. Monitoring of information security controls for systems hosted by third parties was not consistently defined, documented, and implemented at Departmental Offices (DO). (Risk Management)
4. Plans of Action and Milestones (POA&Ms) were not consistently created and tracked in accordance with TD P 85-01 at the Mint. (Risk Management)
5. Information system hardware and software inventory controls were not fully defined and consistently reviewed at the Mint. (Risk Management)

Cybersecurity Function: Protect

6. Configuration security baselines were not always established, and vulnerability scanning was not consistently performed at TIGTA. (Configuration Management)
7. Account management policies were not consistently followed for authorizing, reviewing, recertifying, and removing user access at DO, Bureau of the Fiscal Service (Fiscal Service), Mint, and TIGTA. (Identity and Access Management)

Cybersecurity Function: Recover

8. Contingency planning controls were not consistently implemented at TIGTA. (Contingency Planning)

We made 24 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).

Some bureaus and offices reported self-identified weaknesses over their implementation of NIST Standard Publication (SP) 800-53, Revision 4 (Rev. 4) security controls. For this performance audit, we only evaluated the self-identified weaknesses for security controls referenced in the FY 2018 IG FISMA Reporting Metrics questionnaire. We inspected each self-identified weakness and noted that the Bureau's created 14 POA&Ms with corrective action plans for these self-identified weaknesses. Therefore, we did not provide any additional recommendations for these self-identified weaknesses (see Self-identified Weaknesses).

---

[1] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency developed the FY 2018 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. The eight IG FISMA Metric Domains are aligned with the five functions of identify, protect, detect, respond, and recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

[2] As described in the DHS's *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0.1,* 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.

These findings and recommendations did not include the results from TIGTA's evaluation of the IRS's security program and practices.[3]

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 31, 2018

[3] *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018

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 the NIST related to information security practices.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of FISMA and related OMB policies and NIST procedures, standards, and guidelines. 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. DHS is responsible for the operational aspects of Federal cyber security, such as establishing government-wide 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 OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG.

FY 2018 IG FISMA Reporting Metrics

For fiscal year (FY) 2018, the OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) organized the FY 2018 IG FISMA Reporting Metrics around five information security functions outlined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. In addition, the FY 2018 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 to the FISMA Metric Domains.

Table 1: *Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FY 2018 IG FISMA Metric Domains*

Cybersecurity Framework Security Functions	FY 2018 IG 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

In FY 2018, CIGIE added the Data Protection and Privacy FISMA Metric Domain, which included 5 additional questions. 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, where the most frequent level across the questions will serve as the domain rating. A security program is considered to be effective it is at Level 4, Managed and Measureable.

Table 2: *Inspector General Assessment Maturity Levels*

Maturity Level	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
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 (Bureaus)

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** – Designs and manufactures United States paper currency, securities, and other official certificates and awards.
3 **Bureau of the 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** – 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 Finance 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. Effective July 1, 2018, changes occurred to the operational security organizational alignment for Departmental Offices Bureau IT Systems and the Department of the Treasury Shared Service IT Systems managed by Enterprise Business Solutions (EBS) and Enterprise Infrastructure Operations Services (EIOS), which are responsible for shared service applications and infrastructure respectively.

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** – 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** – 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** – 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** – 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 2018 FISMA Unclassified performance audit, we selected the following bureaus and offices for testing: BEP, DO, Fiscal Service, Mint, OCC, and TIGTA. The sampling methodology is provided in Appendix IV, *Approach to Selection of Subset of Systems.*

We followed up on the status of prior-year findings for the in-scope bureaus and for BEP, DO, Mint, FinCEN, Fiscal Service, TTB, and TIGTA. As in prior years, TIGTA evaluated IRS' information security program and practices. The TIGTA report is appended to this report and the findings of that report are included in Appendix III, *Department of the Treasury's Consolidated Response to DHS's FISMA 2018 Questions for Inspectors General*.

Department of the Treasury Information Security Management Program

Treasury Office of the Chief Information Officer

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 Office of the Chief Information Officer (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:

1. **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.
2. **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.
3. **Cyber Security Reviews** – Conducts technical and program reviews to help strengthen the overall cyber security posture of the Treasury and meet their oversight responsibilities.
4. **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 the Treasury.
5. **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.
6. **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.
7. **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.
8. **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 the Treasury, including those operated by another Federal agency or contractor on behalf of the Treasury. In addition, as OMB periodically releases updates/clarifications of FISMA or as NIST releases updates to publications, the ACIOCS and the OCIO's Cyber Security Program have responsibility to interpret and release updated policy for the Treasury. The ACIOCS and OCIO's Cyber Security Program are 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 established 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 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's information security program and practices for its unclassified systems were established and have been maintained for the 5 Cybersecurity functions and 8 FISMA Metric Domains. The FISMA program areas are outlined in the FY 2018 IG FISMA Reporting Metrics and were prepared by the DHS's Office of Cybersecurity and Communications Federal Network Resilience; however, while the security program has been implemented across the Treasury for its non-IRS bureaus, the program was not effective according to DHS criteria and as reflected in 4 deficiencies in 3 of the 5 Cybersecurity Functions and 4 out of the 8 FISMA program areas that needed improvement. [4]

We have made 24 recommendations that, if effectively addressed by management, should strengthen the respective bureaus', offices', and Treasury's information security programs. The *Findings* section of this report presents the detailed findings and associated recommendations. We noted 14 self-identified control weaknesses by three bureaus, which are in the *Self-Identified Weakness* section of the report. We will follow up on the status of all corrective actions as part of the FY 2019 independent evaluation.

Additionally, we evaluated the prior-year findings from the FY 2017, 2016, 2015, and 2011 FISMA performance audits, as well as the FY 2014 and 2013 FISMA evaluations and noted that management had closed a total of 20 of 31 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).

[4] 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 – SA&A processes were not consistently completed at Mint and TIGTA.

Based on the NIST SP 800-37, Rev. 1, *Guide for Applying Risk Management Framework to Federal Information Systems,* organizations should complete the Security Authorization and Accreditation (SA&A) process to evaluate, test, and examine the security controls that have been pre-determined based on the organization's risk profile and environment, and to accept the residual risks associated with the continued operation of the system and granting approval to operate for a specific time period. The SSP, Security Assessment Report (SAR), POA&M and Authority to Operate (ATO) are components of the SA&A process. TD P 85-01 requires the organization to assign a senior level executive or manager as the authorizing official for the information system; ensure the authorizing official authorizes the information system for processing before commencing operations; update the security authorization when a significant change occurs or every three years; and when a child system is being authorized under the same authorization letter as its parent system, the name of each child system shall be included in the accreditation letter (or an addendum) for Authorizing Official approval.

This control falls under the Identify Cybersecurity area and the Risk Management FISMA Metric Domain.

We noted the following:

- Mint did not complete SA&A packages for Mint System 1 and Mint System 2. The following SA&A package components were not completed: SSPs and SARs up until FY 2017, Mint management authorized Mint Systems 1 and 2 under its network SA&A package and authorization letter as the parent system. However, during FY 2018, management stated that due to lack of resources and competing priorities, it determined that Mint Systems 1 and 2 would undergo their own SA&A packages and would be separated out of the Mint network SA&A package because management no longer classified Mint System 1 and 2 as child systems. Information SA&A packages provide guidance over controls implemented over the information system. Their lack can lead to improper control implementation, thus causing a vulnerability to risks. Without proper accreditation for Mint Systems 1 and 2, management may not be aware of, or accept, the security risks posed by the use of these systems and, therefore, cannot actively support and monitor the effectiveness of their security policies. *(See recommendation #1.)*

- For the TIGTA System, management only issued an interim ATO that did not fully address the following security SA&A items:

    - The TIGTA SSP was not finalized and approved. Additionally, the SSP did not address the system architecture and 144 of 159 NIST SP 800-53, Rev. 4, security controls for a FIPS 199 moderate system were either not implemented or were only partially implemented.
    - POA&Ms were not created for NIST SP 800-53, Rev. 4, controls that were either not implemented or were only partially implemented.
    - A SAR was not completed for the TIGTA System.

    Due to lack of funding and resources and a need to replace an older system, TIGTA stated that it is slowly deploying the TIGTA System in phases and plans to implement information

security controls and practices after funding becomes available. A complete and fully approved SSP should provide documentation for the security controls that are in place within the system's environment. However, incomplete documentation in the SSP increases the risk of misunderstanding in the information system control environment which may lead to a false sense of security. In addition, the deficiencies referred to above increase the risk of improper execution of security control responsibilities and the risk of being vulnerable to existing threats. (See recommendations #2 and 3.)

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

We recommend Mint management:

1. Complete the SA&A packages for the Mint Systems 1 and 2 in accordance with U.S. Mint Information Security Directive (ISD) and NIST SP 800-37, Rev.1.

   Management Response: Mint will complete security assessment for Mint System 1 and 2 under Mint's General Support System. Target completion date: May 31, 2019.

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

We recommend the TIGTA management:

2. Develop a plan that incorporates and takes into account interruptions in the TIGTA System funding.

   Management Response: TIGTA has implemented a rollout plan to bring the system into a mature state in coordination with the program's scheduled deployment plan. The plan involves:
   - Completion of SA&A process;
   - Establishing configuration security baselines and conducting regular vulnerability scanning;
   - Account management policies development and implementation;
   - Development and implementation of contingency plan and performing CP test.

   TIGTA has developed a roll-out plan to bring the system to a more mature secure state in coordination with the deployment phases. Target completion date: June 30, 2019.

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

3. Obtain and issue full ATO to include the following:
   a. Ensure that TIGTA System current SSP is finalized and updated to include the system architecture and all security controls based on system categorization are implemented according with TD P 85-01 and NIST SP 800-53, Rev. 4, guidance.
   b. Develop POA&Ms for the 144 out of 159 TIGTA System NIST SP 800-53, Rev. 4, security controls that were not implemented or were partially implemented.
   c. Complete the SA&A package for the TIGTA System in accordance with NIST SP 800-37, Rev.1.

Management Response: TIGTA has implemented a rollout plan to bring the system into a mature state in coordination with the program's scheduled deployment plan. The plan involves:

- Completion of SA&A process;
- Establishing configuration security baselines and conducting regular vulnerability scanning;
- Account management policies development and implementation;
- Development and implementation of contingency plan and performing CP test.

TIGTA has developed a roll-out plan to bring the system to a more mature secure state in coordination with the deployment phases. Target completion date: June 30, 2019.

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

Finding 2 – SSPs were not always updated in accordance NIST 800-53, Rev. 4, TD P 85-01, and bureau and office information security policies at BEP and OCC.

NIST SP 800-53, Rev.4, TD P 85-01, and bureau and office information security policies require bureaus and offices to develop security plans for the information system that are consistent with the organization's enterprise structure and that are updated to address changes to the information system/environment of operation.

This control falls under the Identify Cybersecurity area and the Risk Management FISMA Metric Domain.

We noted the following:

- BEP management did not fully define the required security controls and control enhancements for the BEP System in the SSP in accordance with BEP Minimum Standard Parameters and NIST SP 800-53, Rev. 4. Specifically, BEP management did not document 8 of 159 controls and the corresponding control enhancements required for a system categorization of moderate. BEP management stated that due to the lack of management oversight and competing priorities, BEP did not commit the resources to ensure that it implemented the required NIST SP 800-53, Rev. 4., controls. (*See recommendation #4.*)

- OCC did not fully document the required security controls and control enhancements in the OCC SSP in accordance with the OCC Master Security Control Catalog (MSCC) and NIST SP 800-53, Rev. 4. Specifically OCC management did not document controls based on the Federal Information Processing Standards (FIPS) 199 moderate categorization. Specifically, we noted the following:

  - 2 out of 159 controls were not documented as implemented, and
  - 5 out of 159 controls were not documented as partially implemented.

  OCC stated that errors occurred in the OCC System SSP template generated by the legacy governance, risk, and compliance solution, and editorial review did not identify and address these errors in documenting the implementation approach for the listed controls and control enhancements. *(See recommendation #5)*

SSPs provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. Inaccurate documentation in the SSP can lead to a misunderstanding of the information system control environment, and improper control implementation, therefore creating vulnerabilities to threats.

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:

4. Validate that it has documented the required security controls for the BEP System 1 and the controls' implementation status in the BEP System 1 SSP as required by the BEP Minimum Standards Parameters and the NIST SP 800-53, Rev. 4.

   Management Response: BEP will review the current system SSP and document and assess any missing security control implementations based on the system categorization as required by Treasury's Minimum Standards Parameters and NIST SP 800-53 Rev. 4. Target completion date: May 1, 2019

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

We recommend that OCC management:

5. Implement an ongoing oversight process to ensure that required security controls and control enhancements are documented in the OCC System SSP as required by OCC MSCC and NIST SP 800-53, Rev. 4.

   Management Response: OCC has fully remediated this finding by documenting the implementation approach for the selected security controls and control enhancements in accordance with OCC's internal documented standards, FIPS 200, NIST SP 800-53, Rev. 4., and NIST SP 800-53, Rev. 1. Completion date: September 20, 2018.

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

Finding 3 – Monitoring of information security controls for systems hosted by third parties was not consistently defined, documented, and implemented at DO.

The TD P 85-01 and Departmental Offices Information Technology Security Policy (DO P-910) require bureaus to develop a continuous monitoring strategy and implement a continuous monitoring program that includes establishing security metrics to be monitored both at the organization and for data and system hosted or managed by third parties, the frequency for monitoring, ongoing security assessments, ongoing security status monitoring of security metrics, correlation and analysis of security-related information generated by the assessments and monitoring, response actions to address results of security related information, and reporting the security status of the organization and the information systems.

This control falls under the Identify Cybersecurity area and the Risk Management FISMA Metric Domain.

We noted the following:

- DO management did not define, document, and implement the monitoring and reviewing controls for the security authorization package and risks tracked by the cloud service provider (CSP) as they relate to the status of security controls for DO System 2 in accordance with the DO P-910. Specifically, we noted the following:

  - 4 out of 159 security controls were not defined and implemented for DO System 2 within the SSP and DO management did not monitor and review the risks associated with these controls; and
  - 4 weaknesses were identified as part of the DO System 2 SAR, and DO management did not monitor and review the risks associated with these weaknesses.

  DO management stated that it was not aware that it had to define a process that documents the review and monitoring of risks that are identified and tracked by the cloud service provider for DO System 2. Without an established monitoring and review process of the security authorization package and the risks, DO may not be aware of existing or potential risks that are introduced in the DO System 2 environment from the cloud service provider. Additionally, without a monitoring and review process, DO may not have a way to determine that the cloud service provider is addressing vulnerabilities in a timely and appropriate fashion. The potential of unauthorized disclosure, modification, or destruction of data is increased and has the potential to adversely affect the confidentiality, integrity, and availability of the DO System 2 data. *(See recommendation #6.)*

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

We recommend that DO management:

6. Define and document the process of monitoring and reviewing the security authorization package and risks and controls identified for the DO System 2 by the service provider, as required by DO P 910,TD P 85-01, and NIST SP 800-53, Rev. 4.

   Management Response: Enterprise Applications Cybersecurity (EBS) plans to institute a procedure to ensure Cloud Service Provider (CSP) continuous monitoring artifacts are reviewed on a scheduled, recurring basis. Target completion date: January 31, 2019.

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

Finding 4 – POA&Ms were not consistently created and tracked in accordance with TD P 85-01 at Mint.

TD P 85-01 also requires the organization to develop POA&Ms for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of security controls and to reduce or eliminate known vulnerabilities in the systems. The organization should update the existing POA&M at least quarterly based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. In addition TD P 85-01, requires the organization to implement a process for ensuring that POA&Ms for the security program and associated organizational information systems are developed and maintained; document the remedial

information security actions to respond adequately to the risk to the organizational operations and assets, individuals, other organizations, and the Nation; and report in accordance with OMB FISMA reporting requirements. Furthermore, the organization should review the POA&Ms for consistency with the organizational risk management strategy and organization-wide priorities for the risk response.

This control falls under the Identify Cybersecurity area and the Risk Management FISMA Metric Domain.

We noted the following:

- Mint management did not create POA&Ms for self-identified weaknesses for Mint System 1 and 2. Due to lack of resources and competing priorities, management stated that it did not create and update POA&Ms to track the status of self-identified weaknesses. Lack of POA&M items for weaknesses identified from security assessments could lead to security weaknesses and vulnerabilities not being remediated in a timely manner, thereby increasing the risk of unauthorized access, use, and/or modification of Mint System 1 and 2 resources. *(See recommendation #7.)*

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:

7. Create POA&Ms for any self-identified security weaknesses and vulnerabilities for Mint Systems 1 and 2.

   Management Response: Mint will create POA&Ms for identified security weaknesses and vulnerabilities for Mint Systems 1 and 2. Target completion date: May 31, 2019.

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

Finding 5 – Information system hardware and software inventory controls were not fully defined and consistently reviewed at Mint.

Security control CM-8, Information System Component Inventory, from TD P 85-01 and NIST SP 800-53, Rev. 4, requires bureaus and offices to include information deemed necessary to achieve effective information system component accountability and to review and update the information system component inventory. This control falls under the Identify Cybersecurity area and the Risk Management FISMA Metric Domain.

We noted the following:

- Mint management did not define any of the required information for maintaining, reviewing, and updating a hardware and software inventory within the Information Security Division (ISD) Security Control Implementation and Status (SCIS) policy in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4, security control requirement CM-8. Additionally, Mint did not review the software and hardware inventory for Mint System 1 and 2. As stated by management the SSP for the Mint network documenting information for maintaining,

reviewing, and updating a hardware and software inventory was completed; however, the SSP was not appended in the ATO package for the network, the parent system for both Mint System 1 and 2. Lack of definitions for establishing and maintaining accurate hardware and software inventories for the Mint does not allow management the ability to manage and monitor an effective information system component accountability. This increases the risk of high impact vulnerabilities occurring within the Mint environment. *(Recommendation #8)*

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

We recommend that Mint management:

8. Update the ISD SCIS, specifically CM-8, security controls to define the information necessary for maintaining an accurate hardware and software inventory in accordance with the TD P 85-01 and NIST SP 800-53, Rev. 4, control requirement CM-8.

   Management Response: Mint will update the system security plan ATO to define information system's authoritative source. Target completion date: May 31, 2019.

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

Finding 6 – Configuration security baselines were not always established, and vulnerability scanning was not consistently performed at TIGTA.

Both NIST SP 800-53, Rev. 4, and TD P 85-01 require bureaus and offices to develop, document and maintain current baseline configurations for the information systems. The bureaus and offices are required to use or develop security configurations for all operational information technology and communications systems. Additionally, both NIST SP 800-53, Rev. 4, and TD P 85-01 require bureaus and offices to scan for vulnerabilities in the information system and hosted application every 30 days and when new vulnerabilities potentially affecting the system/applications are identified and reported. This control falls under the Protect Cybersecurity domain and the Configuration Management FISMA Metric Domain.

We noted the following:

- TIGTA has not established configured security baselines for the TIGTA System. Furthermore, although TIGTA performs vulnerability scanning for its systems, TIGTA did not perform vulnerability scanning over the TIGTA System. TIGTA stated that due to lack of funding and resources, and a need to replace an older system, it is slowly deploying the TIGTA System in phases and will implement information security controls and practices after funding becomes available. By not having established configured security baselines for the TIGTA System, the TIGTA system network is exposed to significant risks to data confidentiality, availability, and integrity. By not scanning for vulnerabilities in the information system, creating POA&Ms, and establishing configured security baselines, the system's computing resources and production data could be subjected to unauthorized access, disclosure, and/or modification. (*See recommendations #9 and 10.)*

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

We recommend that TIGTA management:

9. Establish a current enterprise baseline of software and related configurations for the TIGTA System.

   Management Response: TIGTA has implemented a rollout plan to bring the system into a mature state in coordination with the program's scheduled deployment plan. The plan involves:
   - Completion of SA&A process;
   - Establishing configuration security baselines and conducting regular vulnerability scanning;
   - Account management policies development and implementation;
   - Development and implementation of contingency plan and performing CP test.

   TIGTA has developed a roll-out plan to bring the system to a more mature secure state in coordination with the deployment phases. Target completion date: June 30, 2019.

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

10. Perform vulnerability scanning over the TIGTA System 1 every 30 days in accordance with TD-P 85-01

    Management Response: TIGTA has implemented a rollout plan to bring the system into a mature state in coordination with the program's scheduled deployment plan. The plan involves:
    - Completion of SA&A process;
    - Establishing configuration security baselines and conducting regular vulnerability scanning;
    - Account management policies development and implementation;
    - Development and implementation of contingency plan and performing CP test.

    TIGTA has developed a roll-out plan to bring the system to a more mature secure state in coordination with the deployment phases. Target completion date: June 30, 2019.

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

Finding 7 – Account management policies were not consistently followed for authorizing, reviewing, recertifying, and removing user access at DO, Fiscal Service, Mint, and TIGTA.

NIST SP 800-53, Rev. 4, and TD P 85-01 require bureaus and offices to 1) create, enable, modify, disable, and remove information system accounts and to monitor the user of information system accounts; 2) notify account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes; and 3) review accounts for compliance with bureau- and office-defined account management requirements. NIST SP 800-53, Rev. 4, and TD P 85-01 also require bureaus and offices to explicitly define access to organization-defined security functions and security-relevant information. Moreover, both NIST SP 800-53, Rev. 4, and TD P 85-01 require bureaus and offices to 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 the information system and its 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. This control falls under the Protect Cybersecurity domain and the Identity and Access Management FISMA Metric Domain.

We noted the following:

- For DO System 1, no supporting documentation was available to demonstrate that management conducted a semi-annual user access review for privileged users or the annual review for non-privileged users in accordance with the DO-910, TD P 85-01, and NIST SP 800-53, Rev. 4, guidance. Due to competing priorities, DO management informed us that it was unable to conduct periodic user access reviews semi-annually for privileged users and annually for non-privileged users. Not performing periodic user access reviews and validation of user access for DO System 1 increases the risk of unauthorized access, disclosure, and modification of production data. (*See recommendation #11.)*

- For DO System 1, DO management granted access to an individual prior to the individual signing a Rules of Behavior acknowledgement form. DO management stated that this occurred due to lack of management oversight. Failure to ensure an individual signs the Rules of Behavior acknowledgement form prior to being granted system access, creates a situation where the CISO cannot ensure that DO System 1 users have been properly made aware of the system or application rules, their responsibilities, and their expected behavior. *(See recommendation #12.)*

- Fiscal Service System 2 had 3 out of 20 enabled users that were inactive for more than 120 days and were not disabled automatically within the system, which does not adhere to the Fiscal Service Baseline Security Requirements (BLSR), TD P 85-01, and NIST SP 800-53, Rev. 4. Management informed us that due to lack of management oversight, it did not ensure that Fiscal Service System 2 inactive accounts were automatically disabled. Failure to disable user accounts after 120 days of inactivity increases the risk of the account being compromised by unauthorized access which may result in the loss, alteration, or removal of data. *(See recommendation #13.)*

- Fiscal Service System 3 had 1 of 2 new operating system (OS) and database (DB) users who did not complete the security awareness trainings within the required timeframe. Management stated that due to lack of management oversight, it did not make sure that the user completed the two required trainings within 60 days of being granted access to the system. Educated personnel in an organization are essential to ensuring the security of an organization. Without trained personnel, many security controls in the organization may not be as effective. The potential for unauthorized access is increased when employees are not aware of the risks of sharing passwords, leaving their logged on terminal unattended, and other security procedures. In addition, by not formally assigning responsibility of security to each employee through training courses the employer bears responsibility of employee security breaches with little recourse. *(See recommendation #14.)*

- Mint management did not conduct semi-annual user access reviews for privileged users for Mint Systems 1 and 2 and did not conduct annual user access reviews for non-privileged users for Mint System 2 in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4.

Mint Management stated that due to an oversight by the program office, periodic user access reviews semi-annually for privileged users and annually for non-privileged users were not conducted in accordance with the Treasury Information Technology Security Program TD P 85-01 and NIST SP 800-53, Rev. 4, guidance. Not performing periodic user access reviews and validation of user access for Mint System 1 and 2 increases the risk of unauthorized access, disclosure, and modification of production data. *(See recommendations #15 and 16.)*

- Mint System 1 had 231 user accounts that were inactive for more than 120 days and were not disabled automatically within the system, which does not adhere to the TD P 85-01 and NIST SP 800-53, Rev. 4. Mint management stated that due to oversight by the program office, no inactive user accounts were disabled according to TD P 85-01 and NIST SP 800-53, Rev. 4. Failure to automatically disable inactive user accounts for systems increases the risk of unauthorized user access and lack of accountability of user activities in the system. *(See recommendation #17.)*

- Mint management did not remove Mint System 1 access for nine terminated users after the user's respective separation date in accordance with the TD P 85-01 and NIST SP 800-53, Rev. 4. In addition, Mint has an open finding (see FY 2017 Mint Finding #1 in Appendix II) for not having defined procedures or conditions for creating, enabling, modifying, disabling, and removing system accounts. Specifically we noted the following:

  - 5 out of the 9 user accounts were not deactivated for over 7 months past termination;
  - 2 out of the 9 user accounts were not deactivated for 6 months past termination;
  - 1 out of the 9 user accounts were not deactivated for 5 months past termination; and
  - 1 out of the 9 user accounts were not deactivated for 2 months past termination.

  Mint management stated that due to oversight by the program office, semi-annual and annual user access reviews were not conducted in accordance with the TD P 85-01 and NIST SP 800-53, Rev. 4 guidance. Additionally, the program office did not notify the U.S. Mint service desk of the user's departure from the U.S. Mint, requesting user access be removed. Therefore, Mint management did not properly notify the service desk of the user's departure from the U.S. Mint. Failing to properly remove terminated users could allow for an increased risk of being compromised by unauthorized individuals. Further, unauthorized user account access may result in the loss of data, data corruption, and/or other privileged access. *(See recommendations #18 and 19.)*

- Access was granted for one out of two Mint System 1 users prior to management completing the background screening process, which does not adhere to TD P 85-01 and NIST SP 800-53, Rev. 4. Mint management stated the program office responsible for adjudicating the background investigation screening process for a Mint user was not properly completed prior to granting access to the system. Therefore, Mint management did not properly notify the service desk of the user's departure from the U.S. Mint. Failing to properly remove terminated users could allow for an increased risk of being compromised by unauthorized individuals. Further, unauthorized user account access may result in the loss of data, data corruption, and/or other privileged access. *(See recommendations #20 and 21.)*

- TIGTA has not established account management policies for the TIGTA System. Due to lack of funding and resources, and a need to replace an older system, TIGTA stated that it is slowly deploying the TIGTA System in phases and will implement information security

controls and practices after funding becomes available. Without effective controls defined and in place to ensure that access to the system is restricted to authorized individuals that require TIGTA System access for job responsibilities, the risk is increased that unauthorized persons could access sensitive resources. *(See recommendation #22.)*

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 DO management:

11. Enforce that DO System 1 semi-annual privileged user and annual non-privileged user access reviews are consistently completed to ensure that accounts are removed when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes, as required by DP-910, TD P 85-01, and NIST SP 800-53, Rev. 4.

    Management Response: EBS will plan to institute an account management process to perform user account reviews for both regular (annually) and privileged users (semi-annually) in accordance with the DP-910, TD P 85-01, and NIST SP 800-53, Rev. 4. Target completion date: January 31, 2019.

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

12. Ensure that new users sign the Rules of Behavior acknowledgement form prior to being granted access to DO System 1.

    Management Response: EBS plans to institute a process to ensure the Rules of Behavior documents are acknowledged and signed prior to granting user access to a Treasury information system. Target completion date: March 31, 2019.

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

We recommend that Fiscal Service management:

13. Create a process to automatically disable accounts within the system that are inactive for over 120 days.

    Management Response: Fiscal Service has updated procedures to identify and disable accounts that meet the inactivity threshold. Fiscal Service will validate that the procedures and controls implemented at our Fiscal Agent are effective and operating as intended. Target Completion is June 30, 2019.

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

14. Ensure that all new hires receive initial security awareness and privacy training within 60 days of being granted access to a system and accepting the rules of behavior.

    Management Response: Fiscal Service has recognized and corrected the issue to ensure new hires receive initial security awareness and privacy training within the required timeframe. Fiscal Service will validate that the procedures and controls

implemented at our Fiscal Agent are effective and operating as intended. Target Completion is June 30, 2019.

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

We recommend that Mint management:

15. Perform Mint System 1 semi-annual privileged user access review and ensure it is consistently completed as required by NIST SP 800-53, Rev. 4, and any unnecessary account access is removed.

    Management Response: Mint's Program Office will review existing policies and procedures and update account management review processes to complete scheduled user access reviews. Target completion date: May 31, 2019.

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

16. Perform Mint System 2 semi-annual privileged user and annual unprivileged user access reviews and ensure they are consistently completed as required by NIST SP 800-53, Rev. 4, and remove any unnecessary account access.

    Management Response: Mint's Program Office will review existing policies and procedures and update account management review processes to complete scheduled user access reviews. Target completion date: May 31, 2019.

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

    Management Response: Mint's Program office will review and update existing policies and procedures for account management processes for disabling accounts inactive over 120 days. Target completion date: May 31, 2019.

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

18. Implement a remediation plan to commit resources to update all Mint-wide information security policies and procedures on the frequency required by TD P 85-01 and NIST SP 800-53, Rev. 4.

    Management Response: Mint's Program Office will review existing policies and procedures and update account management review processes to complete scheduled user access reviews. Target completion date: May 31, 2019.

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

19. Establish a process to ensure that Mint System 2 access for terminated users is removed in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4.

Management Response: Mint's Program Office will review existing policies and procedures and update account management review processes to complete scheduled user access reviews. Target completion date: May 31, 2019.

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

20. Implement a remediation plan for FY 2017 Mint Finding #1 to commit resources to update all Mint-wide information security policies and procedures on the frequency required by TD P 85-01 and NIST SP 800-53, Rev. 4.

    Management Response: Mint's Program Office will conduct annual review of all information security policies and procedures for review and approval by United States Mint management for Mint-wide access and distribution. Target completion date: May 31, 2019.

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

21. Establish a process to ensure that Mint System 1 access for terminated users is removed in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4.

    Management Response: Mint's Program Office will review existing policies and procedures and update account management review processes to complete scheduled user access reviews. Target completion date: May 31, 2019.

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

We recommend that TIGTA management:

22. Develop and disseminate to TIGTA personnel a TIGTA System access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

    Management Response: TIGTA has implemented a rollout plan to bring the system into a mature state in coordination with the program's scheduled deployment plan. The plan involves:

    - Completion of SA&A process;
    - Establishing configuration security baselines and conducting regular vulnerability scanning;
    - Account management policies development and implementation;
    - Development and implementation of contingency plan and performing CP test.

    TIGTA has developed a roll-out plan to bring the system to a more mature secure state in coordination with the deployment phases. Target completion date: June 30, 2019.

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

Finding 8 – Contingency planning controls were not consistently implemented at TIGTA.

DHS Federal Emergency Management Agency (FEMA), Federal Continuity Directive 1 (FCD-1) requires bureaus and offices to conduct and document a risk assessment of all mission essential functions (MEFs) by completing a Business Impact Analysis (BIA) for all threats and hazards, and all capabilities associated with continuance of essential functions. Moreover, TD P 85-01 and NIST SP 800-34, Rev.1, *Contingency Planning Guide for Federal Information Systems,* provides directions to bureaus and offices to complete BIAs to determine and plan for the resumption of essential mission and business functions. The bureaus and offices should provide the capability to restore information system components within the time period per the BIAs. Finally, TD P 85-01 and NIST SP 800-53, Rev. 4, require bureaus and offices to develop, document, and disseminate: 1) a contingency planning policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance; and 2) procedures to facilitate the implementation of the contingency planning policy and associated contingency planning control. Furthermore, bureaus and offices should provide capabilities to restore system capabilities within a time period specified by the BIA and the contingency planning policy. This control falls under the Recover Cybersecurity domain and the Contingency Planning FISMA Metric Domain.

We noted the following:

- TIGTA management has not conducted a BIA for the TIGTA system and has not established an Information System Contingency Plan (ISCP). Additionally, TIGTA informed us that it had not completed disaster recovery and business continuity testing for the TIGTA system. Due to lack of funding and resources, and a need to replace an older system, TIGTA is slowly deploying the TIGTA System in phases and will implement information security controls and practices after funding becomes available. Operating without a BIA increases the risk that recovery strategies and priorities, including maximum tolerable downtime (MTD), recovery point objective (RPO), and recovery time objective (RTO), do not align with management expectations. In the event of a service disruption, not having a documented ISCP that can be used as a reference for restoring operations effectively and efficiently could result in unnecessary and costly delays during the restoration process. *(See recommendations #23 and 24.)*

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 TIGTA management:

23. Perform and document the Business Impact Analysis for the TIGTA System environment every two years as required by FCD-1 and TD P 85-01.

    Management Response: TIGTA has implemented a rollout plan to bring the system into a mature state in coordination with the program's scheduled deployment plan. The plan involves:
    - Completion of SA&A process;
    - Establishing configuration security baselines and conducting regular vulnerability scanning;

- Account management policies development and implementation;
- Development and implementation of contingency plan and performing CP test.

TIGTA has developed a roll-out plan to bring the system to a more mature secure state in coordination with the deployment phases. Target completion date: June 30, 2019.

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

24. Develop and disseminate to TIGTA personnel a TIGTA System 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 on the frequency stipulated by BIA.

    Management Response: TIGTA has implemented a rollout plan to bring the system into a mature state in coordination with the program's scheduled deployment plan. The plan involves:

    - Completion of SA&A process;
    - Establishing configuration security baselines and conducting regular vulnerability scanning;
    - Account management policies development and implementation;
    - Development and implementation of contingency plan and performing CP test.

    TIGTA has developed a roll-out plan to bring the system to a more mature secure state in coordination with the deployment phases. Target completion date: June 30, 2019.

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

SELF-IDENTIFIED WEAKNESSES

During the FY 2018 Treasury FISMA performance audit, we noted NIST SP 800-53, Rev. 4, security control requirements that were referenced in the FY 2018 IG FISMA Reporting Metrics Reporting Metrics questionnaire. Since management already identified these weaknesses, we did not issue findings and recommendations. These self-identified weaknesses were associated with POA&Ms.

FY18 FISMA Self-Identified Weaknesses – Department of the Treasury

Bureau	System	NIST SP 800 53 Control	FY 2018 IG FISMA Reporting Metric	Weakness
OCC	Not Applicable	SA-01, SA-04	11	POAM ID #22112: OCC has not established a formal process for ensuring that the necessary security requirements are included in acquisition documents.
TIGTA	Not Applicable	AC-2, AC-2 (1), AC-2 (4), AU-6, AU-6 (1), AU-6 (3)	30	POAM ID #10779: Monitoring Use of Accounts and Reviewing Compliance with Account Management Requirements through a Centralized, Automated Mechanism.
	System #1	AC-2 (5), (9), (10), (12)	30	POAM ID #16771: Policy, Shared accounts in-use, and System accounts monitoring.
		CA-3	1	POAM ID #16777: Interconnection Security Agreement for internal connections to TIC.
		CA-7	2, 3, 47, 49	POAM ID #16778: Continuous Monitoring Plan.
		CM-6	18	POAM ID #16809: There is no documentation to identify any deviations from established configuration settings and what tools are being used.
		CM-7 (1),(2),(5)	17, 18	POAM ID #16810: Process for automated scanning to review the system for restricted services, ports, functions, and protocols needs to be improved.
		CP-3	64	POAM ID #16813: Contingency Training
		CP-4	64	POAM ID #16814: Contingency Plan Test
		PS-6	27	POAM ID #16822: Access agreements have not been updated within the last year.
		SI-3, SI-3(7)	4	POAM ID #16827: The assessor did not observe the specific configurations that would indicate that the agents installed on the individual assets within the system are set to pull updates regularly, specific actions are taken in response to the discovery of malicious code, and non-signature-based detection features are enabled.

Bureau	System	NIST SP 800 53 Control	FY 2018 IG FISMA Reporting Metric	Weakness
	System #2	CA-3	1	POAM ID #21695: An ISA is not currently in place.
		AU-6	58	POAM ID #21697: There is not a current procedure for ISSO review of audit logs and reports.
		AU-2, AU-3	58	POAM ID #21698: No defined specific audit log requirements for the SIEM capability.

MANAGEMENT RESPONSE TO THE REPORT

The following is the Deputy Assistant Secretary for Information Systems and Chief Information Officer's response, dated October 30, 2018, to the Fiscal Year (FY) 2018 Federal Information Security Modernization Act of 2014 (FISMA) Performance Audit Report.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 30, 2018

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 2018 Performance Audit"

Thank you for the opportunity to comment on the draft report entitled, *Fiscal Year 2018 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 your noting that for those Bureaus' with self-identified weaknesses, each Plan of Action and Milestones (POA&M) had adequate corrective action plans established, and therefore, your auditors did not provide any additional recommendations. Finally, 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 FY17 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 have made notable progress over the past year and have accomplished a number of achievements, to include:

- Upgrading existing Splunk architecture with enhanced logging capabilities provides greater detection and response of unknown threats and anomalous behavior across the

enterprise. Improved functionality supplies the Department with greater capability to apply rapid queries in response to a quickly changing threat environment.

- Successfully completed 7 GSOC to Treasury Bureau SOC Roadshows identifying short and long term tasks to help increase overall SOC to SOC effectiveness. GSOC's roadshows have fostered increased awareness of sharing methods and techniques for threat hunting, engineering, architecture, and solutions with plans to develop highly targeted working groups aimed at tackling future challenges identified throughout the Treasury community.

- Finalized upload of Treasury CDM Data to the DHS Federal Dashboard meeting a critical milestone for Phase I deployment of the Continuous Diagnostic Mitigation (CDM) program. Additionally, automated collection and storage of Asset and Vulnerability data enables the GSOC to pre-posture against threats by combining GSOC's threat intelligence with known vulnerabilities to mitigate potential risks to Treasury.

- Coordinated with the Treasury Enterprise Federation Service (TEFS) and external agencies to deploy 6 enterprise-wide integrations of Single Sign On applications supporting strong authentication.

- Further expedited Personal Identity Verification (PIV) card issuance across Treasury networks to achieve a 97% implementation rate across the enterprise for local PIV card printing. This new functionality decreased PIV card issuance wait time by 30% for all cardholders using Treasury systems.

- Completed coordination and participation in Risk Vulnerability Assessment (RVA) and Security Architecture Review (SAR) activities with the Department of Homeland Security (DHS) per Binding Operational Directive 18-02.

- Successful deployment of Apache Nifi Express for data processing resulted in 60% increased capture of complete email events. This advancement enables the GSOC to respond to threat actors in near real time.

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
Jack Donnelly, Associate Chief Information Officer for Cyber Security and Chief Information Security Officer

Attachment

Management Response to (KPMG) Recommendations

KPMG Finding 1: SA&A processes were not consistently completed at the United States Mint (Mint) and the Treasury Inspector General for Tax Administration (TIGTA).

KPMG Recommendation 1: We recommend Mint management: For the selected system, complete the SA&A packages for systems 1 and 2 in accordance with U.S. Mint Information Security Directive (ISD) and NIST SP 800-37, Rev.1.

Treasury's Response: Complete security assessment for both child systems under US Mint Wide Area Network General Support System. Target completion date: May 31, 2019.

Responsible Official: Mint, Chief Information Security Officer

KPMG Recommendation 2: We recommend TIGTA management: For the selected system, develop a plan that incorporates and considers interruptions in the TIGTA System funding.

Treasury's Response: TIGTA has implemented a rollout plan to bring the system into a mature state in coordination within the program's scheduled deployment plan. The plan involves:

- Completion of SA&A process;
- Establishing configuration security baselines and conducting regular vulnerability scanning;
- Account management policies development and implementation;
- Development and implementation of contingency plan and performing CP test.

TIGTA has developed a roll-out plan to bring the system to a more mature secure state in coordination with the deployment phases. Target completion date: June 30, 2019.

Responsible Official: TIGTA, Chief Information Security Officer.

KPMG Recommendation 3: We recommend TIGTA management: For the selected system, obtain and issue full ATO to include the following:

a. Ensure that TIGTA System current SSP is finalized and updated to include the system architecture and all security controls based on system categorization are implemented according with TD P 85-01 and NIST SP 800-53, Rev. 4, guidance.
b. Develop POA&Ms for NIST SP 800-53, Rev. 4, security controls that were not implemented or were partially implemented.
c. Complete the SA&A package for the system in accordance with NIST SP 800-37, Rev.1.

Treasury's Response: TIGTA has implemented a rollout plan to bring the system into a mature state in coordination within the program's scheduled deployment plan. The plan involves:

- Completion of SA&A process;
- Establishing configuration security baselines and conducting regular vulnerability scanning;
- Account management policies development and implementation;
- Development and implementation of contingency plan and performing CP test.

TIGTA has developed a roll-out plan to bring the system to a more mature secure state in coordination with the deployment phases. Target completion date: June 30, 2019.

Responsible Official: TIGTA, Chief Information Security Officer.

KPMG Finding 2: SSPs were not always updated in accordance with NIST 800-53, Rev. 4, TD P 85-01, and bureau and office information security policies at Bureau of Engraving and Printing (BEP) and the Office of the Comptroller of the Currency (OCC).

KPMG Recommendation 4: We recommend BEP management: For the selected system, validate that it has documented the required security controls for the selected system and the controls' implementation status in the selected system SSP as required by Treasury's Minimum Standards Parameters and the NIST SP 800-53, Rev. 4.

Treasury's Response: BEP will review the current system SSP and document and assess any missing security control implementations based on the system categorization as required by Treasury's Minimum Standards Parameters and NIST SP 800-53 Rev. 4. Target completion date: May 1, 2019.

Responsible Official: BEP, Chief Information Security Officer

KPMG Recommendation 5: We recommend OCC management: For the selected system, implement an ongoing oversight process to ensure that required security controls and control enhancements are documented in the OCC System SSP as required by OCC MSCC and NIST SP 800-53, Rev. 4.

Treasury's Response: OCC has fully remediated this finding by documenting the implementation approach for the selected security controls and control enhancements in accordance with OCC's internal documented standards, Federal Information Processing Standards (FIPS) 200, NIST Special (SP) 800-53, Revision (Rev.) 4, and NIST SP 800-37 (Rev. 1). Completion date: September 20th, 2018.

Responsible Official: OCC, Chief Information Security & Privacy Officer

KPMG Finding 3: Monitoring of information security controls for systems hosted by third parties was not consistently defined, documented, and implemented at Departmental Offices (DO).

KPMG Recommendation 6: We recommend DO management: For the selected system, define and document the process of monitoring and reviewing the security authorization package and risks and controls identified for the DO System 2 by the service provider, as required by DO P 910, TD P 85-01, and NIST SP 800-53, Rev. 4.

> **Treasury's Response:** Enterprise Applications Cybersecurity (EBS) plans to institute a procedure to ensure Cloud Service Provider (CSP) continuous monitoring artifacts are reviewed on a scheduled, recurring basis. Target completion date: January 31, 2019.
>
> **Responsible Official:** EBS, Director

KPMG Finding 4: POA&Ms were not consistently created and tracked in accordance with TD P 85-01 at Mint.

KPMG Recommendation 7: We recommend Mint management: For the selected system, create POA&Ms for any self-identified security weaknesses and vulnerabilities for Mint systems 1 and 2.

> **Treasury's Response:** Create POA&Ms for identifies security weaknesses and vulnerabilities for affected systems. Target completion date: May 31, 2019.
>
> **Responsible Official:** Mint, Chief Information Security Officer

KPMG Finding 5: Information system hardware and software inventory controls were not fully defined and consistently reviewed at Mint.

KPMG Recommendation 8: We recommend Mint management: For the selected system, update the system security plan ATO package, specifically CM-8, security controls to define the information necessary for maintaining an accurate hardware and software inventory in accordance with the TD P 85-01 and NIST SP 800-53, Rev. 4, control requirement CM-8.

> **Treasury's Response:** Update the system security plan ATO package to define information systems authoritative source. Target completion date: May 31, 2019.
>
> **Responsible Official:** Mint, Chief Information Security Officer

KPMG Finding 6: Configuration security baselines were not always established, and vulnerability scanning was not consistently performed at TIGTA.

KPMG Recommendation 9: We recommend TIGTA management: For the selected system, establish a current enterprise baseline of software and related configurations for the TIGTA System.

Treasury's Response: TIGTA has implemented a rollout plan to bring the system into a mature state in coordination within the program's scheduled deployment plan. The plan involves:

- Completion of SA&A process;
- Establishing configuration security baselines and conducting regular vulnerability scanning;
- Account management policies development and implementation;
- Development and implementation of contingency plan and performing CP test.

TIGTA's roll-out plan will bring the system into a more mature state in coordination with planned deployment phases. Target completion date: June 30, 2019.

Responsible Official: TIGTA**,** Chief Information Security Officer

KPMG Recommendation 10: We recommend TIGTA management: For the selected system, perform vulnerability scanning over the TIGTA System 1 every 30 days in accordance with TD- P 85-01.

Treasury's Response: TIGTA has implemented a rollout plan to bring the system into a mature state in coordination within the program's scheduled deployment plan. The plan involves:

- Completion of SA&A process;
- Establishing configuration security baselines and conducting regular vulnerability scanning;
- Account management policies development and implementation;
- Development and implementation of contingency plan and performing CP test.

TIGTA's roll-out plan will bring the system into a more mature state in coordination with planned deployment phases. Target completion date: June 30, 2019.

Responsible Official: TIGTA, Chief Information Security Officer

KPMG Finding 7: Account management policies were not consistently followed for authorizing, reviewing, recertifying, and removing user access at DO, Fiscal Service, Mint, and TIGTA.

KPMG Recommendation 11: We recommend DO management: For selected system #1, enforce that semi-annual privileged user and annual non-privileged user access reviews are consistently completed to ensure that accounts are removed when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes, as required by DO P-910, TD P 85-01, and NIST SP 800-53, Rev. 4.

Treasury's Response: EBS plans to institute an account management process to perform user account reviews for both regular (annually) and privileged users (semi-annually) in accordance with the DO Information Technology Security Policy Handbook

(DO P-910), Treasury Directive Publication (TD P) 85-01, and NIST SP 800-53, Revision (Rev.) 4 guidance. Target completion date: January 31, 2019.

Responsible Official: EBS, Director

KPMG Recommendation 12: We recommend DO management: For the selected system, ensure that new users sign the Rules of Behavior acknowledgement form prior to being granted access to the selected system.

Treasury's Response: EBS plans to institute a process to ensure the Rules of Behavior documents are acknowledged and signed prior to granting user access to a Treasury information system. Target completion date: March 31, 2019.

Responsible Official: EBS, Director

KPMG Recommendation 13: We recommend Fiscal Service (FS) management: For the selected system, create a process to automatically disable accounts within the system that are inactive for over 120 days.

Treasury's Response: Fiscal Service has updated procedures to identify and disable accounts that meet the inactivity threshold. Fiscal Service will validate that the procedures and controls implemented at our Fiscal Agent are effective and operating as intended. Target Completion is June 30, 2019.

Responsible Official: FS, Chief Information Security Officer

KPMG Recommendation 14: We recommend FS management: For the selected system, ensure that all new hires receive initial security awareness and privacy training within 60 days of being granted access to a system and accepting the rules of behavior.

Treasury's Response: Fiscal Service has recognized and corrected the issue to ensure new hires receive initial security awareness and privacy training within the required timeframe. Fiscal Service will validate that the procedures and controls implemented at our Fiscal Agent are effective and operating as intended. Target Completion is June 30, 2019.

Responsible Official: FS**,** Chief Information Security Officer

KPMG Recommendation 15: We recommend Mint management: For selected system #1, perform semi-annual privileged user access review and ensure it is consistently completed as required by NIST SP 800-53, Rev. 4, and any unnecessary account access is removed.

Treasury's Response: Program office will review existing policies and procedures and update account management review processes to complete scheduled user access reviews. Target completion date: May 31, 2019.

Responsible Official: Mint, Chief Information Security Officer

KPMG Recommendation 16: We recommend Mint management: For selected system #2, perform semi-annual privileged user and annual unprivileged user access reviews and ensure they are consistently completed as required by NIST SP 800-53, Rev. 4, and remove any unnecessary account access.

Treasury's Response: Program office will review existing policies and procedures and update account management review processes to complete scheduled user access reviews. Target completion date: May 31, 2019.

Responsible Official: Mint, Chief Information Security Officer

KPMG Recommendation 17: We recommend Mint management: For the selected system, 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.

Treasury's Response: Program office will review and update existing policies and procedures for account management processes for disabling accounts inactive over 120 days. Target completion date: May 31, 2019.

Responsible Official: Mint, Chief Information Security Officer

KPMG Recommendation 18: We recommend Mint management: For the selected system, implement a remediation plan to commit resources to update all Mint-wide information security policies and procedures on the frequency required by TD P 85-01 and NIST SP 800-53, Rev. 4.

Treasury's Response: Program office will review existing policies and procedures and update account management review processes to complete scheduled user access reviews. Target completion date: May 31, 2019.

Responsible Official: Mint, Chief Information Security Officer

KPMG Recommendation 19: We recommend Mint management: For the selected system, establish a process to ensure that system access for terminated users is removed in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4.

Treasury's Response: Program office will review existing policies and procedures and update account management review processes to complete scheduled user access reviews. Target completion date: May 31, 2019.

Responsible Official: Mint, Chief Information Security Officer

KPMG Recommendation 20: We recommend Mint management: For the selected system, implement a remediation plan for FY 2017 Mint Finding #1 to commit resources to update all Mint-wide information security policies and procedures on the frequency required by TD P 85- 01 and NIST SP 800-53, Rev. 4.

> **Treasury's Response:** Program office will conduct annual review of all information security policies and procedures for review and approval by United States Mint management for Mint-wide access and distribution. Target completion date: May 31, 2019.
>
> **Responsible Official:** Mint, Chief Information Security Officer

KPMG Recommendation 21: We recommend Mint management: For the selected system, establish a process to ensure that Mint System 1 access for terminated users is removed in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4.

> **Treasury's Response:** Program office will review existing policies and procedures and update account management review processes to complete scheduled user access reviews. Target completion date: May 31, 2019.
>
> **Responsible Official:** Mint, Chief Information Security Officer

KPMG Recommendation 22: We recommend TIGTA management: For the selected system, develop and disseminate to TIGTA personnel a system access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

> **Treasury's Response:** TIGTA has implemented a rollout plan to bring the system into a mature state in coordination within the program's scheduled deployment plan. The plan involves:
>
> - Completion of SA&A process;
> - Establishing configuration security baselines and conducting regular vulnerability scanning;
> - Account management policies development and implementation;
> - Development and implementation of contingency plan and performing CP test.
>
> TIGTA's roll-out plan will bring the system into a more mature state in coordination with planned deployment phases. Target completion date: June 30, 2019.
>
> **Responsible Official:** TIGTA, Chief Information Security Officer

KPMG Finding 8: Contingency planning controls were not consistently implemented at TIGTA.

KPMG Recommendation 23: We recommend TIGTA management: For the selected system, perform and document the Business Impact Analysis (BIA) for the system environment every two years as required by FCD-1 and TD P 85-01.

Treasury's Response: TIGTA has implemented a rollout plan to bring the system into a mature state in coordination within the program's scheduled deployment plan. The plan involves:

- Completion of SA&A process;
- Establishing configuration security baselines and conducting regular vulnerability scanning;
- Account management policies development and implementation;
- Development and implementation of contingency plan and performing CP test.

TIGTA's roll-out plan will bring the system into a more mature state in coordination with planned deployment phases. Target completion date: June 30, 2019.

Responsible Official: TIGTA, Chief Information Security Officer

KPMG Recommendation 24: We recommend TIGTA management: For the selected system, develop and disseminate to TIGTA personnel a system plan 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 system on the frequency stipulated by BIA.

Treasury's Response: TIGTA has implemented a rollout plan to bring the system into a mature state in coordination within the program's scheduled deployment plan. The plan involves:

- Completion of SA&A process;
- Establishing configuration security baselines and conducting regular vulnerability scanning;
- Account management policies development and implementation;
- Development and implementation of contingency plan and performing CP test.

TIGTA's roll-out plan will bring the system into a more mature state in coordination with planned deployment phases. Target completion date: June 30, 2019.

Responsible Official: TIGTA, Chief Information Security Officer

Appendices

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY

The objective for this performance audit was to assess the effectiveness of the Department of the Treasury's (Treasury) information security program and practices for its unclassified systems (with exception to the Internal Revenue Service (IRS) systems) for the period July 1, 2017 through June 20, 2018. The scope of our work did not include the 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 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) FISMA 2018 Questions for Inspectors General,* dated May 24, 2018, 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. 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 DHS *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0.1,* dated May 24, 2018; 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. See Appendix IV, *Approach to Selection of Subset of Systems* for the Selection Methodology. The following was our approach for accomplishing the FISMA audit and being able to determine the maturity levels for each of the 5 Cybersecurity Functions and 8 FISMA Metric Domains from the Fiscal Year (FY) 2018 FISMA Reporting Metrics for the Inspector General (IG):

1. 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 maturity at level 1 (Ad Hoc) or 2 (Defined) for the questions that failed testing.
2. For maturity level 3 controls determined to be effective, we performed level 4 (Managed and Measurable) test procedures for the Department, in-scope Bureau, and in-scope system (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.

3. For maturity level 4 controls determined to be effective, we performed level 5 (Optimized) test procedures for the Department, in-scope Bureau, 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. For the 2018 FISMA performance audit of Treasury's unclassified systems, we did not assess any controls at the Level 5, Optimized. Thus, no testing was necessary to evaluate Treasury's controls at that level.

We performed our fieldwork from June 1, 2017 to July 30, 2018, at Treasury's headquarters and offices in Washington, D.C., and bureau locations and data centers in Washington, D.C.; and Hyattsville, Maryland. For one bureau information system managed and hosted at the Federal Reserve Bank of New York, we performed fieldwork at the data center in East Rutherford, New Jersey. 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 2018 FISMA performance audit:

- The Federal Information Security Modernization Act of 2014
- NIST Federal Information Processing Standard (FIPS) and/or SPs[5]
    - 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 Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*
    - NIST Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*
    - NIST Special Publication 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*
    - NIST Special Publication 800-39, *Managing Information Security*
    - NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*

[5] 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 Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST Special Publication 800-61 Revision 2, *Computer Security Incident Handling Guide*
- NIST Special Publication 800-70 Revision 3, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*
- NIST Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response
- NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST Special Publication 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 16-03, *Fiscal Year 2016-2016 Guidance on Federal Information Security and Privacy Management Requirements*
  - OMB Memorandum 17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Requirements*
- Department of Homeland Security
  - Inspector General Federal Information Security Modernization Act of 2014 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) 2017, 2016, 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. In FYs 2014 and FY 2013, we conducted a FISMA Evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation. 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 Department of the Treasury (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.

Prior Year Findings – 2017

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2017 Finding # 1– Bureau of Engraving and Printing (BEP) Information security policies, procedures, and security plans were either outdated or incomplete	For the BEP system, BEP management did not upload required documentation (e.g., Accreditation Letter and Security Test & Evaluation) to the Treasury FISMA Inventory Management System (TFIMS) as required by Treasury Directive Publication (TD P) 85-01.	We recommend that BEP management: 1. Implement a process or mechanism to ensure all required documentation (e.g., System Security Plan (SSP), Contingency Plan, Risk Assessments, etc.) is uploaded into TFIMS on the frequency stipulated in TD P 85-10.	**Closed** We inspected all documentation supporting the current Security Assessment and Authorization (SA&A) package for the BEP system located in TFIMS and noted all uploaded documentation was present and current.
Prior Year FY 2017 Finding # 1 – US Mint (Mint) Information security policies, procedures, and security plans were either outdated or incomplete	Mint management did not update and approve bureau-wide information security policies and procedures in accordance with TD P 85-01 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev.) 4 guidance. Specifically, the following bureau-wide policies were to be updated at least annually.	We recommend that Mint management: 2. Review and approve the Mint-wide information security policies and procedures on an annual basis.	**Open** We inquired of Mint and were informed that this finding is in the process of being remediated.

Finding #	Prior-Year Condition	Recommendation(s)	Status
		3. Implement a remediation plan to commit resources to update all Mint-wide information security policies and procedures on the frequency required by TD P 85-01 and NIST SP 800-53, PM-1 are updated.	
Prior Year FY 2017 Finding # 2 – Bureau of the Fiscal Service (FS) Asset management processes were not fully implemented at the Bureau of the Fiscal Service	The Fiscal Service (FS) Software Asset Management (SAM) process is not implemented and does not have any automated enterprise SAM tool to manage the documented process in the FS SAM Bureau-wide IT Standard. The SAM Bureau-wide IT Standard documents the process of maintaining an updated inventory of software inventory and associated licenses, but highlights the lack of an enterprise SAM tool to effectively implement the SAM process.	We recommend that FS management: 4. Ensure the timely deployment of the enterprise-wide SAM tool to implement and improve the documented SAM process.	**Open** We inquired of FS and were informed that this finding is in the process of being remediated with a target completion date of June 30, 2019.
Prior Year FY 2017 Finding # 3 – Alcohol & Tobacco Tax and Trade Bureau (TTB) System inventory reviews were inconsistent	The Alcohol & Tobacco Tax & Trade Bureau (TTB) Security Program Policy and SSP requires management to conduct quarterly reviews of system inventories for all general support systems, major applications, and minor applications. However, we noted that management is only reviewing the system inventories on an annual basis.	We recommend that TTB management: 5. Develop and implement plans to review system inventories by the established bureau policies.	**Closed** We obtained and inspected both the System Program Policy and SSP and noted both policies have been updated to require annual system inventory review to be completed.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2017 Finding # 4 – BEP Configuration compliance and vulnerability scanning were not consistently performed	BEP did not conduct recurring Security Content Automation Protocol (SCAP) compliance scans in accordance with TD P 85-01 requirements.	We recommend that BEP management: 6. Update BEP information security policies and procedures to: • Require scanning of the BEP network for SCAP compliance on a regular basis as required by TD P 85-01 guidelines. • Remediate configuration deviations noted during SCAP scanning within a timely manner.	**Closed** We obtained and inspected updated BEP information security policies and procedures to require scanning of the BEP network for SCAP compliant and remediated configuration deviation noted during SCAP scanning.
Prior Year FY 2017 Finding # 4 – Fiscal Service Configuration compliance and vulnerability scanning were not consistently performed	The Fiscal Service Baseline Security Requirements (BLSR) requires system and applications to perform scans at least every two weeks. However, from May 18, 2017 through June 21, 2017, the Nessus Tenable vulnerability and configuration scans were not being performed for the Fiscal Service system. Furthermore, Fiscal Service management did not identify these missing scans as part of its review process.	We recommend that FS management: 7. Complete vulnerability scans over the Fiscal Service system according to the frequency stablished by the BLSR. 8. Develop a process to ensure that the Fiscal Service system's vulnerability scans are successfully completed and reviewed.	**Closed** We inspected the Security Center Validation and Verification Standard Operating Procedure (SOP) and noted that it requires the Cyber Security Branch (CSB) to review scan logs on a weekly basis to ensure Security Center scans have successfully completed ensuring all partial and failed scans are investigated and corrected.

Finding #	Prior-Year Condition	Recommendation(s)	Status
			Next, we inspected the "Active Scan" configuration settings in Fiscal Service's vulnerability scanning tool and noted scans are automatically set to run on a weekly basis in compliance with the BLSR. Additionally, we noted that after the weekly scans have been run, a THREAT engineer will review the status log for each scan and report any scans that partially completed via email to their Team Leads for further instruction. Further, we inspected a response to the action report from a team lead and noted the email provided the THREAT engineer with instructions for correcting the scan issues noted.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2017 Finding # 4 – Departmental Offices (DO) Configuration compliance and vulnerability scanning were not consistently performed	Although DO has documented risk assessment and system and information integrity security controls to address vulnerabilities in the DO IT Security Policy Handbook, we noted that DO did not document actionable timeframes in its existing information security policies for which vulnerabilities shall be remediated. For example, the System and Information Integrity (SI-2) Flaw Remediation and Risk Assessment (RA-5) does not adequately define the time period for which security - related software is to be implemented. Moreover, through inspection of the DO system's March, April, and May vulnerability scan results, we identified the following populations of the DO system's vulnerabilities: For one DO system, seven for March and nine for April; and 37 for March and 39 April for another DO system. Furthermore, we identified that DO management had a process in place to remediate vendor identified critical and high vulnerabilities, and we observed that these processes were in place. However, management did not remediate all the critical and high vulnerabilities within its environment in a consistent manner. Specifically, we noted the following: • 2 of 2 of the judgmentally selected critical and high vulnerabilities were identified during March also existed during the April and May vulnerabilities scans, and no policy or program was in place to prioritize the timeframe to remediate these weaknesses for one system. • 3 of 5 of the selected critical and high vulnerabilities were identified during March also existed during the April and May vulnerabilities scans, and no policy or program was in place to prioritize the timeframe to remediate these weaknesses for another DO system.	We recommend that DO management: 9. Update the DO IT Security Policy Handbook, Version 3.3, specifically the RA-5 and SI-2 security controls to establish actionable timeframes for remediating vulnerabilities using a risk based approach or develop a Continuous Monitoring Program to determine and set agreed upon timeframes to remediate organizational defined vulnerabilities.	**Open** We inquired of DO and were informed that this finding is in the process of being remediated with a target completion date of December 30, 2018.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2017 Finding #4 TTB Configuration compliance and vulnerability scanning were not consistently performed	Multiple instances of end-of-life software packages were installed on the TTB network. Specifically, seven installations of outdated software were present on the July 2017 vulnerability scan, and these software packages were deemed end-of-life by Microsoft in April of 2014.	We recommend that TTB management: 10. Establish a current enterprise baseline of software and related configurations. 11. Establish a process to review and revise enterprise software baselines to maintain TTB's risk posture. As a result of the enterprise software baseline review, update systems to be compliant with enterprise baselines. 12. Test patches in adherence to the updates to the IT Security Handbook and supporting patch management policies and procedures.	**Closed** We obtained and inspected the TTB Authorized Software List (ASWL) SOP and noted the document describes the process and procedure for maintenance of the TTB OCIO ASWL. We noted the list of enterprise approved software will be reviewed on a monthly basis to identify all instances of unsupported and unapproved software and any identified instances of unsupported or unapproved software will be removed. Further, we inspected evidence of the Un-supported Software Scan, dated September 27, 2017, and noted that there were no active instances of un-supported software in use therefore the number of vulnerabilities caused by unauthorized software dropped to zero.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2017 Finding # 5 – BEP Missing or inconsistent patch management practices existed	During the FISMA performance period of June 1, 2016, through July 31, 2017, BEP did not install critical patches to the Local Area Network/Wide Area Network (LAN/WAN) network in a timely manner or have an associated Plan of Actions and Milestones (POA&M) to resolve the outstanding patches. Per inspection of the October 7, 2016, vulnerability scan, 39 critical and 68 high vulnerabilities have exceeded the 30- day timeframe to be installed or have an associated POA&M.	We recommend that BEP management: 13. Implement a process to ensure that patches are installed within the BEP Minimum Standard Parameters time frames or create POA&Ms to resolve any outstanding patches. 14. Develop procedures to implement patches in a timely manner for hardware with uptime requirements. 15. Develop procedures to ensure temporary virtual machines are patched.	**Closed** We obtained and inspected the Patch Management Process and Procedures (PMPP) and noted it addresses the implementation process for the patching PO&AMs in timely manner.
Prior Year FY 2017 Finding # 5 – DO Missing or inconsistent patch management practices existed	Although DO has documented its patch management process in its IT Security Policy Handbook, we identified that DO management does not consistently test all operating system patches prior to installation. In addition, the IT Security Policy Handbook does not specify the level of approval required prior to installation of patches. More specifically, as of June 26, 2017, we noted that there were 361 operating system patches implemented on the 5 of 31 judgmentally selected servers within the DO environment, and we observed that the process is in place to test and approve patches. However, sufficient evidence was not available to support the effective management of all 15 judgmentally selected patches for the operating systems supporting two FY17 in-scope systems. Specifically, we noted: • Testing evidence was not available for 13 of 15 selected operating system patches. • Management approval was not available for 14 of 15	We recommend that DO management: 16. Update the IT Security Policy Handbook and supporting patch management policies and procedures to enforce a patch management process for the operating systems supporting the two FY17 systems , and other moderate or high risk information systems to test, document, and approve patches prior to installation. 17. Perform and document a cost benefit analysis to determine if	**Open** We inquired of DO and were informed that this finding is in the process of being remediated with a target completion date of December 30, 2018.

Finding #	Prior-Year Condition	Recommendation(s)	Status
	selected operating system patches.	a complete test environment is warranted for all DO systems to include tracking of all patch management decisions. 18. Test patches in adherence to the updates to IT Security Handbook and supporting patch management policies and procedures.	
Prior Year FY 2017 Finding # 5 – TTB Missing or inconsistent patch management practices existed	Although TTB has documented its patch management process in its Configuration Management Handbook, TTB management did not consistently approve operating system security patches prior to installation. Specifically, management retroactively approved two of five operating system patches during the FISMA testing period.	We recommend that TTB management: 19. Ensure individuals who install patches are properly trained to follow the required configuration and patch management processes. 20. Approve security patches prior installing them on the operating system.	**Closed** We obtained and inspected the Patch Management SOP and noted that it has been updated and is required to be used by system admins, database admins, and managers. Further, we inspected the Request for Change (RFC) submission and Tracking tickets for a sample of months and noted both RFCs were approved by the Associate Chief Information Officer (ACIO) prior to installation.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2017 Finding # 5 – TTB Missing or inconsistent patch management practices existed	TTB did not patch six high vulnerabilities from April 2017 and one critical vulnerability from February 2017 in accordance within the timeframes established in the TTB Patch Management SOP. We noted that on the June 2017 vulnerability scan report, these 7 vulnerabilities had been open for more than 30 days. A POA&M was created for only 1 out of 7 of these vulnerabilities.	We recommend that TTB management: 21. Update the patching process to ensure that all vulnerabilities, regardless of patch publication, are remediated or have a POA&M opened in accordance with timelines. 22. Establish review processes to ensure that all, regardless of patch publication, vulnerabilities are following the bureau process.	**Closed** We obtained and inspected the Patch Management SOP and noted it has been updated and is required to be used by system admins, database admins, and managers. TTB has reviewed and updated its patch management reporting process to ensure all of its vulnerabilities are properly identified, accounted for, and tracked. Any identified vulnerabilities will either be remediated or a POA&M will be created with an associated timeline for completion, and are required to be entered into TFIMS. Further, we inspected a report containing all known old vulnerabilities and noted it captured the 'Plugin Publication Date' for each of the vulnerabilities listed.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2017 Finding # 6 –Mint Account management activities were not compliant with System Security Policies	The process for the Mint system's periodic user access review was not conducted annually for all system users in accordance with the selected in scope FY17 system's SSP and NIST SP 800-53, Rev. 4 guidance.	We recommend that Mint management: 23. Develop process to ensure that periodic user access reviews are completed for the selected system. 24. Ensure all active system accounts are consistently reviewed in accordance with NIST SP 800-53, Rev. 4.	**Open** We inquired of Mint and were informed that the SOP has been updated, but is still in the process of being approved and signed off by management.
Prior Year FY 2017 Finding # 6 –Mint Account management activities were not compliant with System Security Policies	During the FISMA audit period of July 1, 2016 through July 1, 2017, we found that 1 of 45 new network users did not complete their Rules of Behavior and Access Agreement forms in accordance with TD P 85-01 and NIST SP 800-53, Rev. 4.	We recommend that Mint management: 25. Establish a process to ensure that all users are consistently completing a Rules of Behavior and Access Agreement forms 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.	**Closed** We obtained and inspected the US Mint Information Security Policy and noted the policy had been updated to include a process to ensure that all users sign all appropriate access agreements prior to being granted system access, and resign access agreements when an update has been made or annually.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2017 Finding 6 – Financial Crimes Enforcement Network (FinCEN) Account management activities were not compliant with System Security Policies	During the FISMA audit period of July 1, 2016 through July 1, 2017, the process for the selected system periodic access review was not performed in accordance with the FY17 in scope system's SSP and TD P 85-01.	We recommend that FinCEN management: 26. Perform a periodic review of all active system's user and privileged accounts are reviewed in accordance with the FY17 in scope system's SSP and NIST SP 800-53, Rev. 4.	**Closed** We obtained and inspected evidence of Management's verification of the system's account review and determined it was performed in accordance with the system's SSP and TD P 85-01.
Prior Year FY 2017 Finding # 6 –TTB Account management activities were not compliant with System Security Policies	The TTB's selected system's SSP requires semi-annual reviews for privileged users. Specifically, we noted the following: None of the 15 selected TTB privileged users have records of completing the semi-annual reviews.	We recommend that TTB management: 27. For selected system, develop and implement its semi-annual user access review for privileged infrastructure users that support the application.	**Closed** We obtained and inspected the TTB Privileged Account Review SOP and noted the SOP describes the process by which all privileged accounts are reviewed in TTB's OCIO.
Prior Year FY 2017 Finding # 6 –BEP Account management activities were not compliant with System Security Policies	For the BEP system, BEP management did not retain the Non-disclosure agreement, Acceptable Use Agreement, Rules of Behavior, and required training documentation for one out five new users.	We recommend that BEP management: 28. For selected system, ensure that new system users complete the Non-disclosure agreements, Acceptable Use Agreements, Rules of Behavior, and required training documentation.	**Closed** For a sample of five (5) new BEP system user accounts, we inspected evidence that each selected user had signed a Non-Disclosure Agreement (NDA) prior to being granted access to the BEP system.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2017 Finding # 7 –Mint Contingency planning activities were not compliant with policies	A BIA was not conducted and documented for the Mint system as part of the process of developing an Information System Contingency Plan (ISCP) in accordance with the NIST SP 800-53, Rev.4.	We recommend that Mint management: 29. Ensure that the Cloud Service Provider (CSP) is conducting and documenting a Business Impact Analysis (BIA) for Mint system prior to the next major ISCP update. 30. For the selected, complete BIAs per TD P 85-01 and NIST SP 800-34, as part of its contingency planning process.	**Open** We inquired of Mint and were informed that the BIA has been developed, but is still in the process of being approved and signed off by management.
Prior Year FY 2017 Finding # 7 –BEP Contingency planning activities were not compliant with policies	A BIA was not conducted and documented for the BEP system as part of the process of developing an ISCP in accordance with NIST SP 800-53, Rev. 4.	We recommend that BEP management: 31. Conduct and document a BIA for the BEP system prior to the next major ISCP update. 32. Implement a process to ensure that BIAs are completed for BEP system per TD P 85-01 and NIST SP 800-53, Rev. 4.	**Closed** We inspected the BEP system's BIA and noted it was completed on September 12, 2017. Further, we noted that the BIA is scheduled to be updated annually with its next updated to be completed by November 13, 2018.

Prior Year Findings – 2016 Performance Audit

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 5 – DO Account management activities were not compliant with policies.	For the selected DO system, 71 out of 3,214 system user accounts had gone unused for more than 120 days and were not disabled as required by the SSP.	We recommend DO management: 1. For the selected system, configure the system to disable user accounts automatically after 120 days of inactivity.	**Closed** We obtained and inspected the DO listing of active DO network accounts and noted that none of the active accounts had been inactive for more than 120 days from the date of the system-generated list.
Prior Year FY 2016 Finding # 5 –Fiscal Service Account management activities were not compliant with policies.	For the selected system, the SSP and Fiscal Service BLSR required management to disable system user accounts that are inactive for more than 120 days and that management should delete user accounts after 13 months of inactivity.	We recommend that Fiscal Service management: 2. For the first system, establish a process to ensure that all system users are consistently completing a NDA within a timely manner, and a process to revoke accounts when a NDA is not completed. 3. For the selected system, in the absence of a long-term system capability solution, obtain a formal risk acceptance waiver and perform manual monthly reviews of all system user accounts and disable or delete accounts that no longer need access. 4. For the selected system, configure or acquire additional system capability to automatically disable user accounts in accordance with system and Fiscal Service defined frequency.	**Closed** We obtained and inspected the Bureau of the Fiscal Service Corrective Action Completion/Risk Acceptance Closure form and noted that management has accepted this risk. Further, we noted that due to the shared nature of the system's account, the lack of activity using one application cannot be allowed to cause the account to be inactivated without negatively impacting the user's ability to access the other applications for which they are authorized and still using. Therefore it is necessary that the applications manage the authorization disablement due to inactivity themselves.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 6 – Mint Contingency planning activities were not compliant with policies.	Mint management did not approve and sign the contingency plan during the FISMA year. Mint management did not sign the contingency plan because a signature page was not included in the contingency plan template.	We recommend that Mint management: 5. For the selected system, require that senior level officials document their approvals of the Contingency Plan by adding their signature to the Contingency Plan signature page following each annual plan update.	**Closed** We inspected the system's ISCP and noted it was last updated on January 24, 2018 and signed off by a senior level official acknowledging their review and approval.

Prior Year Findings – 2015 Performance Audit

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2015 Finding #1 – Mint Logical account management activities were not compliant with policies.	Per the selected Mint system's System Security Plan (SSP), the system is required to be configured to automatically disable any user account when 120 days have passed since the last password change. However, after KPMG performed an analysis of the twenty-one (21) users, based on the 120 day requirement outlined in the SSP, KPMG noted that one user's login was not disabled. Overall, one out of twenty-one user accounts were not appropriately disabled within the application. Additionally, the help desk did not document or retain records for 7 of the 25 new user access authorizations for the application within the selected system between July 1, 2014 and June 30, 2015.	We recommend that Mint management, for the selected system: 1. Configure selected system to automatically disable user accounts after 120 days of last password change as stated within the SSP. 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.	**Partially Implemented/Open** We inspected the password configurations for the selected system and noted account passwords are set to automatically expire after 90 days meeting the requirements defined in the selected system's SSP. However, we noted that new user access approval forms were not retained for multiple system's users.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2015 Finding #2 – Mint Did not implement all of the NIST SP 800-53, Rev. 4, security controls for some of their SSPs and ensure completeness in accordance with NIST guidance.	Mint's SSP for the selected system that is managed by a third party cloud service provider (CSP) did not address all required NIST SP 800-53, Rev. 4 controls. We noted that 38 controls and 35 control enhancements were either missing or did not contain sufficient information to satisfy the control requirements. In addition, the SSP did not adequately address the following sections as outlined in the NIST SP 800-18: 1.3 Operation Status, 1.5 System Environment, 1.5.2 Encryption/PKI, 1.5.3 Network Configuration, 1.6 System Interconnection/Information Sharing, 1.6.2 Mobile Code, and 1.6.3 Ports, Protocols, & Services. Furthermore, control implementation statuses (i.e., implemented, not implemented, planned, inherited, not inherited, partially implemented, or compensated) were not documented for all NIST SP 800-53, Rev. 4, controls. Mint management stated that this was the first year of authorization for the selected system and that the SSP was not finalized because the third party CSP had limited resources to complete all required sections sufficiently in the time that was allotted.	We recommend that Mint management: 3. For the selected system, ensure that control implementation statements and statuses for all NIST SP 800-53, Rev. 4 controls and control enhancements are fully addressed in the SSP. 4. For the selected system, ensure that the following sections: 1.3 Operation Status, 1.5 System Environment, 1.5.2 Encryption/PKI, 1.5.3 Network Configuration, 1.6 System Interconnection/Information Sharing, 1.6.2 Mobile Code, 1.6.3 Ports, Protocols, & Services are consistent with guidance provided in the criteria and are fully documented.	**Partially Implemented/Open** We obtained and inspected the SSP and noted that it did not completely address all of the control implementation statements and statuses for all NIST SP 800-53, Rev. 4, controls and control enhancements. We obtained and inspected the extension letter related to this finding and noted that the due date was extended from May 2018 to May 2019. We noted that the CSP has determined that the timeframe for completion of the FedRAMP Agency Authorization to Operate (ATO) for the selected system is 12 months and will include conducting a gap analysis of the existing system security documentation.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2015 Finding #5 – Mint Contract with third-party cloud service provider did not address FedRAMP requirements.	The TD P 85-01 requires that all cloud systems shall comply with FedRAMP guidelines. This control falls under the contractor systems FISMA program area. We noted the Mint's selected system is managed by a third-party CSP; however, the CSP only provides application vulnerability scan reports and does not provide vulnerability scanning results of their infrastructure to the Mint. In addition, the Mint required the CSP to provide the Contingency Plan (CP). Furthermore, the CSP did not provide the following FISMA- related artifacts demonstrating compliance with NIST SP 800-53, Rev. 4: Vulnerability scans for the months of January and May to ensure patches were occurring in a timely manner. Security auditing tools' configuration settings were configured for a component of the selected system to capture auditable events as specified in accordance with the SSP. User lists for two components of the selected system to capture the account creation date. User lists for two components of the selected system to capture the last log-on date. In addition, one of the in-scope component's user list to capture both the last log-on date and enabled/disabled status.	We recommend that Mint management: 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. 6. For the selected system, ensure that third-party CSP provides FISMA-related artifacts to demonstrate FISMA compliance to the Mint security compliance team. 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.	**Open** We obtained and inspected the extension letter related to this finding and noted that the due date was extended from May 2018 to May 2019. We noted that the Cloud Service Provider has determined that the timeframe for completion of the FedRAMP Agency ATO for the selected system is 12 months.

Prior Year Findings – 2014 Evaluation

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #3 – Mint Did not follow NIST guidance for SSPs.	Mint's SSP for the selected system was last updated in May 2013, and has not been reviewed annually as required by Mint guidelines. Furthermore, the SSP utilized security controls from an outdated initial public draft version of the NIST SP 800-53, Rev. 4, which was released in February 2012. The Mint had not updated the SSP to include all of the required controls and enhancements from the final NIST SP 800-53, Rev. 4, version, dated April 2013. On March 30, 2012, the designated Mint security analyst reviewed the SSP and completed updates to reflect NIST SP 800-53, Rev. 4, initial public draft controls and enhancements. Mint management was aware that the SSP needed to be updated to reflect the final Rev. 4 controls. However, there were limited resources to update the SSP due to a transition in the IT contractor support in June 2013.	We recommend that Mint management: 1. For the selected systems, review and update the SSP to include all relevant controls from the NIST SP 800-53, Rev. 4, final version. 2. For the selected systems, ensure Rev. 4 controls and enhancements are implemented on the system and tested promptly.	**Closed** We inspected the selected system's SSP and noted it includes all relevant Rev. 4 controls, and their respective implementation status. Further, we noted the systems' controls were tested by an independent assessor as part of the system's System Testing & Evaluation (ST&E) testing.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #5 – BEP Bureau IT security and configuration management policies had not been updated or reviewed to address NIST and Treasury requirements.	BEP management had not updated their IT security policies and procedures to incorporate the latest NIST SP 800-53, Rev. 4, controls. BEP management failure to stay compliant with NIST and Treasury policies was due to competing priorities with other IT initiatives. This was a self-reported finding and documented within BEP's enterprise-wide POA&M, with an estimated completion date of December 15, 2014.	Based on the planned corrective actions for BEP, we are not making a recommendation.	**Closed** BEP had finished completing its corrective action plan.

Prior Year Findings – 2013 Evaluation

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2013 Finding #1 – Treasury Inspector General for Tax Administration (TIGTA) Logical account management activities were not in place or consistently performed.	For a selected TIGTA system, TIGTA management was unable to provide a system-generated list showing last login dates and times. In addition, we were unable to obtain evidence of user authorization forms for the system. As a result, there was no evidence that user account management was in place and operating effectively. It was noted that this was a self-reported finding and was listed as a POA&M within the Trusted Agent FISMA (TAF) system with an estimated completion date of January 31, 2014.	Based on TIGTA's planned corrective actions, we are not making a recommendation.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that the finding was remediated as of April 9, 2018.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2013 Finding #4 – TIGTA Contingency planning and testing controls were not fully implemented or operating as designed.	TIGTA did not fully implement contingency planning (planning and testing) controls as required by TD P 85-01 Volume I, NIST SP 800-53, Rev. 3, and NIST SP 800-34 guidance. While these controls do not affect normal, daily operations, they are invaluable in quickly recovering the system from a disaster or service interruption. Contingency plan documentation for a selected TIGTA system was not finalized within the FISMA year. This was a self-reported finding and documented within TIGTA's POA&M report on TAF, with an estimated completion date of December 31, 2013.	Based on TIGTA's planned corrective actions, we are not making a recommendation.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that the finding was remediated as of April 9, 2018.

Prior Year Findings – 2011 Performance Audit

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2011 Finding #1 – TIGTA Logical account management activities were not fully documented or consistently performed.	TIGTA did not fully document account management activities (e.g., review frequency, inactivity limits, use of shared accounts) in their SSPs. TIGTA management was unaware of the lack of documentation until a 2010 security assessment was conducted. In response to the security assessment, TIGTA established four corrective actions in the system's POA&M with scheduled completion dates of October 2011, April 2012, July 2012, and December 2012. These security weaknesses continued to exist at the time of FY 2011 FISMA audit.	Based on TIGTA's planned corrective actions, we are not making a recommendation.	**Partially Implemented/Open** TIGTA has not finished completing its corrective action. We noted that the POA&M due date has been revised to meet new milestones on May 31, 2019.
Prior Year FY 2011 Finding #8 – TIGTA Contingency planning and testing and backup controls were not fully implemented or operating as designed.	The selected TIGTA system lacked sufficient documentation regarding the system's contingency plan and contingency plan testing. Specifically, the documentation did not include certain key software used. TIGTA management identified these weaknesses during a 2010 security assessment and established two POA&M items with scheduled completion dates of January 2012 and June 2012.	Based on TIGTA's planned corrective actions, we are not making a recommendation.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that the finding was remediated as of May 26, 2018.

For FY 2018 FISMA performance audit, we only followed up on management's prior-year self-identified weaknesses that included NIST SP 800-53, Rev. 4, security controls that were referenced in the FY 2018 IG FISMA Reporting Metrics.

FY17 FISMA Self-Identified Weaknesses – Department of the Treasury

Bureau	System	NIST SP 800 53 Control	Weakness	Status
DO	DO System #1	IA-2 IA-5 AC-2 (1) AC-2(3)	POA&M #16460 Accounts are not automatically disabled after a period of inactivity POA&M #16465 The application does not require the use of multifactor authentication	**Open** POA&M #16460 – Open POA&M #16533 – Open We noted that the POA&M due date has been revised to April 27, 2018, and these POA&Ms are notated as being late.
Fiscal Service	Enterprise Common Control for Fiscal Service System #1, 2, and 3	AC-2	POA&M #15699 User access recertification process needs improvement POA&M #15700 User access recertification process needs improvement POA&M #15701 User access recertification process needs improvement **Note:** Although management closed these POA&Ms on 4/21/17, these POA&Ms were open for the majority of the FISMA year; therefore, we noted the self-identified weaknesses as open for purposes of the FY 2018 IG FISMA Metrics.	**Closed** POA&M #15699– Closed POA&M #15700 – Closed POA&M #15701 – Closed We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that the findings were remediated on April 21, 2017.
	Enterprise Common Control for Fiscal Service System #1, 2, and 3	CM-2	POA&M #10903 The Control implementation statement does not fully address the control requirement of the configuration baselines being approved by the bureau	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that the finding was remediated on September 5, 2017.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	Enterprise Common Control for Fiscal Service System #1, 2, and 3	SI-1	POA&M #16760, #16761, #16762, #16763, #16764 Security Patches and Updates – Security-relevant updates and/or patches have not been applied to information system components within organizational timeframes	**Partially Implemented/Open** POA&M #16760– Open POA&M #16761 – Closed POA&M #16762 – Closed POA&M #16763 – Open POA&M #16764 – Open We noted that the due date for POA&M #16760 has been revised to September 30, 2018, and the POA&M is notated as being late. We obtained and examined supporting evidence in support of POA&M #16761 finding and noted that the corrective actions were implemented and that the findings were remediated on May 1, 2018. We obtained and examined supporting evidence in support of POA&M #16762 finding and noted that the corrective actions were implemented and that the findings were remediated on March 31, 2018 We noted that POA&M #16763 is currently in progress and is due to be completed on January 31, 2019. We noted that POA&M #16764 is currently in progress and is due to be completed on August 31, 2018. Note: Due to the scheduled completion date being after the FISMA audit period, follow up testing of this finding's status will occur during FY19.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	Enterprise Common Control for Fiscal Service System #1, 2, and 3	AC-2	POA&M #10922 Inactive accounts are not automatically disabled after 120 days POA&M #10904 The system does not automatically disable inactive accounts after 120 days	**Closed** POA&M #10922– Risk Accepted POA&M #10904– Closed We obtained and examined supporting evidence in support of POA&M 10922 and noted the Information System Security Officer (ISSO), System Owner (SO), Authorizing Official (AO), Chief Information Security Officer (CISO), and Chief Information Security Officer (CIO) have decided to accept this risk and take no further action. We obtained and examined supporting evidence in support of POA&M #10904 finding and noted that the corrective actions were implemented and that the findings were remediated on October 2, 2017.
	Enterprise Common Control for Fiscal Service System #1, 2, and 3	CA-3 SA-4	POA&M #10905 The Inter-Service Agreement (ISA) and Memorandum of Understanding (MOU) expired in May and June, respectively	**Closed** We obtained and examined supporting evidence in support of POA&M #10905 finding and noted that the corrective actions were implemented and that the findings were remediated on October 2, 2017.
	Enterprise Common Control for Fiscal Service System #1, 2, and 3	CA-3	POA&M #10902 All ISAs were not updated annually	**Closed** We obtained and examined supporting evidence in support of POA&M #10902 finding and noted that the corrective actions were implemented and that the findings were remediated on September 28, 2017.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	Fiscal Service System #2	CA-2	POA&M #11715 Unknown if security assessments performed on control enterprise infrastructure control	**Open** We noted that the POA&M due date has been revised to September 30, 2018, and these POA&Ms are notated as being late. Note: Due to the scheduled completion date being after the FISMA audit period, follow up testing of this finding's status will occur during FY19.
	Fiscal Service System #2	AC-6	POA&M #16055 Least functionality	**Closed** We obtained and examined supporting evidence in support of POA&M #10904 finding and noted that the corrective actions were implemented and that the findings were remediated on August 16, 2017.
TTB	TTB System #1	SI-2	POA&M #16061 May CARD vulnerabilities –VDI **Note:** Although management closed this POA&M on 6/13/17, this POA&M was open for the majority of the FISMA year; therefore, we noted the self-identified weaknesses as open.	**Closed** We obtained and examined supporting evidence in support of POA&M #10904 finding and noted that the corrective actions were implemented and that the findings were remediated on June 13, 2017.

FY16 FISMA Self-Identified Weaknesses – Department of the Treasury

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	DO System #1	CM -2	POA&M #16533: Website and Database Scans Required for new system and remediation of vulnerabilities	**Open** We obtained and examined supporting evidence in support of this finding and noted that the finding was cancelled and opened with POA&M #16533, which remained open.
	DO System #2	AC-2	POA&M #15524: Password policies not up to FISMA standard.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the finding was remediated.
	DO System #2	AU-6	POA&M #15528: Information system monitoring logs/alerts are not provided to DO.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the finding was remediated.
	DO System #2	CM-6 SI-2	POA&M #15526: Vulnerability scanning is executed monthly; application scanned when promoted from dev. To production.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the finding was remediated.
	DO System #2	CM-6	POA&M #15531: USB ports are not disabled on the servers.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the finding was remediated.
	DO System #2	PL-4 PS-6	POA&M #8401: Third-party personnel are not required to sign a DO NDA nor a Rules of Behavior (ROB).	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the finding was remediated.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	DO System #3	CM-2	POA&M #10970: The systems Baseline Configurations not adequately documented.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the finding was remediated.

FY15 FISMA Self-Identified Weaknesses – Department of the Treasury

Bureau	System	NIST SP 800 53 Control	Weakness	Status
BEP	BEP System #1	CA-6 CM-11 IA-2 MP-7 PL-2 PL-8 RA-2 RA-3 RA-5 SI-2	POA&M #4001 (enterprise-wide): The system implementation for NIST SP 800-53 Rev. 4 is incomplete.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the finding was remediated.
DO	DO System #1	SI-2	POA&M #6861: Application supports Java SE Development Kit (JDK) 5.x and 6.x. Load balancers affected by multiple vulnerabilities.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the finding was remediated.
	DO System #1	RA-5	POA&M #6736: Monthly vulnerability scan data (OS, Database and application levels) and Summary Reports are not provided to Treasury	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the finding was remediated.
	DO System #1	AU-6	POA&M #7413: Application logs are not forwarded to the centralized log server for automated review, analysis, and reporting.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the finding was remediated.
	DO System #2	CM-2	POA&M #576: CM-2: Although several secure hardening guides exist, the system only employs vendor-recommended settings. Additionally, the baseline is not documented.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the finding was remediated.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
OCC	OCC System #1	AC-2 AU-2 AU-6 AU-12	POA&M #47: Component-level audit requirements have not yet been determined and documented. Lack of auditing for the following: Audit database management event and Audit database object management event. This finding is applicable to the multiple applications within the system.	**Open/Late** POA&M #47/6336 - Closed POA&M #47/6329 –Open We noted that POA&M #47 has transferred to POA&M #6336 and POA&M #6329. POA&M #6336 was closed September 3, 2018, which is after the FISMA audit period of July 1, 2018 to June 30, 2018. POA&M #6329 is outstanding and has a revised due date of March 1, 2018. Therefore, this POA&M is late and open.

APPENDIX III – DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS's FISMA 2018 QUESTIONS FOR INSPECTORS GENERAL

The information included in Appendix III represents Department of the Treasury's (Treasury) consolidated responses to Department of Homeland Security's (DHS) FISMA 2018 questions for Inspectors General. We prepared 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, and 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.[6] If issues were identified related to the metric, we assessed the metric at Ad Hoc (Level 1), Defined (Level 2), or Consistently Implemented (Level 3) and provided explanations in the "Comment" 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), Optimized (Level 5), or Consistently Implemented (Level 3), when it was the highest maturity level determined by management's self-assessment.

Treasury Inspector general for Tax Administration (TIGTA) performed audit procedures over the IRS information systems and provided its answers to the Treasury Office of Inspector General (OIG) and KPMG for consolidation. TIGTA's answers are included within the table below, and denoted where its response lowered the maturity level from 3 to a 1 or 2. The information provided by TIGTA may have been summarized and has not been subjected to KPMG audit procedures and, accordingly, we did not modify TIGTA's responses.

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 (National Institute of Standards and Technology (NIST) SP 800-53: CA-3, PM-5, and CM-8; OMB-M-04-25; NIST 800-161; NIST Cybersecurity Framework(CSF): ID.AM-1-4; Fiscal Year (FY) 2018 CIO FISMA Metrics: 1.1, 1.4, and 1.5)?

[6] The scoring methodology is described in the DHS's *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.0.1, May 24, 2018, requires a Managed and Measurable (Level 4) rating for an effective security program and is determined by the entries in CyberScope.

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.

Comments: For Departmental Offices (DO) System 1, DO management issued self-identified weakness in Plan of Action and Milestone (POA&M) ID #16777: "Interconnection Security Agreement (ISA) for internal connections to Trusted Internet Connection (TIC)." For DO System 2, DO management issued self-identified weakness in Plan of Action and Milestone (POA&M) ID #21695: "An ISA is not currently in place."

FY 2017 Finding #3 for the Alcohol and Tobacco Tax and Trade Bureau (TTB), "System inventory reviews were inconsistent," was closed.

Performance Improvement Opportunity (PIO): Mint and Treasury Inspector General for Tax Administration (TIGTA) should consider having a policy to define maintaining an information system.

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: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2; FY 2018 CIO FISMA Metrics:1.2)?

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 hardware assets connected to the organization's network and uses this taxonomy to inform which assets can/cannot be introduced into the network.

Comments: For DO System 1, DO management issued a self-identified weakness in POA&M ID #16778: "Continuous Monitoring Plan." FY 2017 Finding #2 for Fiscal Service, "Asset management processes were not fully implemented," was open. Mint management did not define any of the required information for maintaining, reviewing, and updating a hardware and software inventory within the Information Security Division (ISD) Security Control Implementation and Status (SCIS) policy in accordance with TD P 85-01 and the NIST SP 800-53, Rev. 4, security control requirement. (Refer to Finding #5 in the Findings section for Mint.)

PIO: TIGTA should consider documenting their hardware inventory in their system security plan (SSP).

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: CA-7, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?

Maturity Level: **Consistently Implemented (Level 3)** - 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: Refer to comments in question 2 and 4.

PIO: TIGTA should consider documenting their software inventory in their system security plan (SSP).

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA[7] reported instances of hardware issues, including unverified computers and uncontrolled hardware on the Internal Revenue Service (IRS) asset management system. Mint management did not define any of the required information for maintaining, reviewing, and updating a hardware and software inventory within the Information Security Division (ISD) Security Control Implementation and Status (SCIS) policy in accordance with TD P 85-01 and the NIST SP 800-53, Rev. 4, security control requirement. (Refer to Finding #5 in the Findings section for Mint.)

4 To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; and FIPS 199; FY 2018 CIO FISMA Metrics: 1.1)?

Maturity Level: **Defined (Level 2)** – The organization has categorized and communicated the importance/priority of information systems in enabling its missions and business functions.

Comments: The Bureau of Engraving and Printing (BEP) System 1 SSP was missing 8 of 159 security controls and control enhancements. DO did not define, document, and implement the monitoring and reviewing controls for the security authorization package and risks tracked by the cloud service provider (CSP) as they relate to the status of security controls for DO System 2. The Office of the Comptroller of the Currency (OCC) System 1 SSP had 2 of 159 controls not documented as implemented and 5 of 159 controls not documented as partially implemented. TIGTA did not finalize and approve the TIGTA System 1 SSP, and within the SSP, the office did not implement or fully implement the system architecture and security controls based on the system's categorization. Mint did not complete SA&A packages for Mint System 1 and Mint System 2. (In the Findings section, refer to Finding #2 for BEP and OCC; Refer to Finding #1 for TIGTA and Mint; Refer to Finding #3 for DO.)

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

For DO System 1, DO management issued self-identified weakness POA&M ID #16827: "The assessor did not observe the specific configurations that would indicate that the agents installed on the individual assets within the system are set to pull updates regularly, specific actions are taken in response to the discovery of malicious code, and non-signature-based detection features are enabled."

Finally, refer to comments for question 11.

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that include 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: 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; FY 2018 CIO FISMA Metrics: 1.6)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its risk management policies, procedures, and strategy at the enterprise, business process, and information system levels. The organization uses its risk profile to facilitate a determination on the aggregate level and types of risk that management is willing to assume. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of risk management processes and activities to update the program.

Comments: To improve its Risk Management (RM) program, Treasury should monitor and analyze its defined qualitative and quantitative performance measures on the effectiveness of its RM strategy across disciplines and collect, analyze, and report information on the effectiveness of its RM program.

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; FEA Framework; NIST SP 800-53: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; DHS Binding Operational Directive 17-01)?

Maturity Level: **Defined (Level 2)** – The organization has defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture. In addition, the organization has defined a process to conduct a security architecture review for new/acquired hardware/software prior to introducing systems into its development environment.

Comments: Refer to comment for question 4 in Identify – 1: Risk Management. FY 2015 Finding #2 for Mint, "Did not implement all of the NIST SP 800-53, Revision (Rev.) 4, security controls for some of their SSPs and ensure completeness in accordance with NIST guidance," was partially implemented/open.

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2, OMB A-123, CFO Council ERM Playbook)?

Maturity Level: **Consistently Implemented (Level 3)** – Roles and responsibilities of stakeholders involved in risk management have been defined and communicated across the organization. Stakeholders have adequate resources (people, processes, and technology) to effectively implement risk management activities.

Comments: To improve its RM program, Treasury should utilize an integrated RM 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 POA&Ms are utilized for effectively mitigating security weaknesses (NIST SP 800-53: CA-5; OMB M-04-25)?

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

Comments: Mint management did not create POA&Ms for self-identified weaknesses for the Mint System 1 and 2. Additionally, TIGTA did not create POA&Ms for 144 of 159 security controls that were not implemented or partially implemented. For DO System 2, refer to comment in question 11. (In the Findings section, refer to Finding #1 for Mint and TIGTA and Finding #4 for Mint.)

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA reviewed 97 weaknesses that the IRS identified during the annual testing of controls of the 7 selected systems. Of the 97 weaknesses, TIGTA could not track 9 weaknesses to either existing or closed POA&Ms that supported effective remediation. In addition, TIGTA reviewed 21 POA&Ms that were closed in FY 2018 related to the 7 selected systems. Of the 21 POA&Ms that were closed, 4 POA&Ms were closed without sufficient support that the weaknesses were corrected even though the IRS had validated the closures through its closure verification process. After TIGTA brought this to the IRS's attention, it provided additional evidence for 1 POA&M closure and reopened the other 3 POA&Ms.

PIO: DO should consider tracking POA&Ms that are identified by the service provider.

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 800-37; NIST SP 800-39; NIST SP 800-53: PL-2, RA-1; NIST 800-30; CSF:ID.RA-1 – 6)

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

Comments: TIGTA did not complete the Security Assessment Report (SAR) for the TIGTA System 1. (Refer to Finding #1 in the Findings section for TIGTA) FY 2017 Finding #4, "Configuration compliance and vulnerability scanning were not consistently performed," was open for DO.

FY 2017 TTB System 1, TTB management closed POA&M #16061 "May CARD vulnerabilities –VDI."

For FY 2016 DO System 2, DO management closed POA&M #15526: "Vulnerability scanning is executed monthly; application scanned when promoted from development to production."

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA reviewed the IRS's system risk assessments of the 7 systems selected for the FY 2018 FISMA evaluation. TIGTA identified issues with security control testing. Security controls were not reliably tested according to the assessment procedures. For example, the IRS used an outdated compliance checker to test the configuration controls of systems, with no risk based decision in place for using the outdated compliance checker. In addition, the results of the security test showed that the controls passed testing; however, results of other tests indicate that pass was not a reasonable conclusion.

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))?

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

Comments: To enhance its RM program, Treasury should employ robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization.

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 (FAR) clauses, and clauses on protection, detection, and reporting of information) and Service Level Agreements (SLAs) are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (FAR Case 2007-004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, 52.239-1; President's Management Council; NIST 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2018 CIO FISMA Metrics: 1.5; Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)?

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 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.

Comments: DO did not define, document, and implement the monitoring and reviewing controls for the security authorization package and risks tracked by the CSP as they relate to the status of security controls for DO System 2. (Refer to Finding #3 in the Findings section for DO.) In addition, OCC issued self-identified weakness in POA&M ID #22112: "OCC has not established a formal process for ensuring that the necessary security requirements are included in acquisition documents."

FY 2015 Finding #5 for Mint, "Contract with third-party cloud service provider did not address FedRAMP requirements" was open.

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.

Comments: To improve its RM program, Treasury 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.

PIO: BEP, DO, Mint, TIGTA should consider consistently implement an automated enterprise solution.

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

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

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. TIGTA reported that the IRS' RM program was effective and was assessed at the Managed and Measurable 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?

Comments:

During the 2018 Mint financial statement audit, we noted that Mint did not documented the Security Assessment and Authorization (SA&A) for a financial management system in accordance with NIST 800-37 and NIST SP 800-18. In addition, the control over the recertification of the Tax Major Application (TMA) SSP, did not operate effectively as the TTB Information System Security Owner (ISSO) did not certify that the annual review of a financial management system SSP was complete by signing off on the FY 2018 SSP. According to DHS criteria, we assessed the RM program to be ineffective based on the maturity levels assessed in metric questions 1 to 12. Please refer to 13.1 for explanation.

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: CM-1; NIST SP 800-128: Section 2.4)?

Maturity Level: **Consistently Implemented (Level 3)** – Stakeholders have adequate resources (people, processes, and technology) to consistently implement information system configuration management activities.

Comments: This is the highest maturity level for this question.

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;[8] configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53: 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.

Comments: To improve its Configuration Management (CM) program, Treasury 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: 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.

Comments:

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that while the IRS as defined policies and

[8] The Federal Information Systems Audit Manual (FISCAM) defines System Development Life Cycle (SDLC) methodology as the "policies and procedures that govern software development and modification as a software product goes through each phase of its life cycle."

procedures for managing the configuration of its information systems, it has not consistently implemented 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: CM-2, CM-8; FY 2018 CIO FISMA Metrics: 1.1, 1.2; CSF: ID.DE.CM-7)?

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.

Comments: For DO System 1, DO management issued the self-identified weakness in POA&M ID #16810: Process for automated scanning to review the system for restricted services, ports, functions, and protocols needs to be improved. TIGTA has not established configuration baselines for the TIGTA System 1. (Refer to Finding #6 in the Findings section for TIGTA.)

For FY 2016 DO System 1, POA&M#16533: "Website and Database Scans Required for new system and remediation of vulnerabilities" was open.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, 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 three of the seven systems we selected for the FY 2018 FISMA evaluation did not consistently maintain baseline configurations. Further, the annual security testing reported that two of seven systems did not maintain and have an up-to-date information system component inventory. In addition, TIGTA[9] and the U.S. Government Accountability Office (GAO)[10] reported instances of baseline configurations not being consistently implemented and inaccurate system component inventories.

[9] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017); TIGTA, Ref. No. 2017-20-032, *The Internal Revenue Service Does Not Have a Cloud Strategy and Did Not Adhere to Federal Policy When Deploying a Cloud Service* (Aug. 2017); TIGTA, Ref. No. 2018-20-029, *Security Over High-Value Assets Should Be Strengthened* (May 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. 2018-20-030, *The Cybersecurity Data Warehouse Needs Improved Security Controls* (June 2018); TIGTA, Ref. No. 2018-20-041, *Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability* (July 2018); and TIGTA, Ref. No. 2018-20-066, *Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented* (Sept. 2018).

[10] GAO, GAO-18-391, *IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 2018).

18 To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53: CM-6, CM-7, and SI-2; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7)?

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.

Comments: Refer self-identified weakness in question 1. For DO System 1, DO management issued the self-identified weakness in POA&M ID #16809: "There is no documentation to identify any deviations from established configuration settings and what tools are being used."

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that while the IRS has defined common secure configurations, it has not ensured that its information systems consistently maintain secure configuration settings in compliance with IRS policy. The IRS's annual security testing of systems reported that six of the seven systems we selected for the FY 2018 FISMA evaluation did not maintain secure configuration settings in accordance with IRS policy. In addition, least functionality controls were not in place for five of the seven systems, and flaw remediation processes were not in place for three of the seven systems. Also, TIGTA[11] and the GAO[12] reported findings of systems that did not maintain secure configuration settings in accordance with agency policy. Further, the IRS's tool to assess configuration settings is not Security Content Automation Protocol–compliant. In addition, the GAO reported that the mainframe tools only test compliance with a limited subset of agency's policies.

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53: CM-3, SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20 Control 4.5; FY 2018 CIO FISMA Metrics: 2.13; and DHS Binding Operational Directive 15-01)?

[11] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017); TIGTA, Ref. No. 2018-20-029, *Security Over High-Value Assets Should Be Strengthened* (May 2018); TIGTA, Ref. No. 2018-20-039, *Private Collection Agency Security Over Taxpayer Data Needs Improvement* (July 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. 2018-20-034, *Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls* (June 2018); and 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).
[12] GAO, GAO-18-165, *IRS's Fiscal Years 2017 and 2016 Financial Statements* (Nov. 2017), and GAO, GAO-18-391, *IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 2018).

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.

Comments: Although TIGTA performs vulnerability scanning for its systems, the office did not perform vulnerability scanning of the TIGTA System 1. (Refer to Finding #6 in the Findings section for TIGTA.)

For 2017 Fiscal Service System 1, 2, and 3, POA&M #16760, #16763, #16764 "Security Patches and Updates – Security-relevant updates and/or patches have not been applied to information system components within organizational timeframes" was open. However, management did close associated #16761 and #16762.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that 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 processes were not in place for three of the seven systems we selected for the FY 2018 FISMA evaluation. Also, TIGTA[13] and the GAO[14] reported that the IRS did not remediate high-risk vulnerabilities or install security patches on systems in a timely manner.

PIO: BEP management should consider documenting the results of their monthly SCAP scans in such a way that reviewers know when each deviation was initially observed.

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

[13] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017); TIGTA, Ref. No. 2018-20-029, *Security Over High-Value Assets Should Be Strengthened* (May 2018); TIGTA, Ref. No. 2018-20-039, *Private Collection Agency Security Over Taxpayer Data Needs Improvement* (July 2018); TIGTA, Ref. No. 2018-20-036, *The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved* (July 2018); and 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).
[14] GAO, GAO-18-165, *IRS's Fiscal Years 2017 and 2016 Financial Statements* (Nov. 2017), and GAO, GAO-18-391, *IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 2018).

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 maturity level for this question.

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: CM-2, CM-3)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its change control policies, procedures, and processes, including explicit consideration of security impacts prior to change implementation.

Comments: In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that while the IRS has defined policy and procedures for managing configuration change control, these policy and procedures have not been consistently followed at the information system level. The IRS's annual security testing of systems reported that two of the seven systems selected for the FY 2018 FISMA evaluation had failed security controls related to change management practices. In addition, two of the seven systems did not have baseline configurations in place for some of their components. Also, TIGTA[15] and the GAO[16] 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?

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

Comments: During the FY 2018 Treasury consolidated financial statement audit, we noted that one Fiscal Service financial management system's configuration management plan did not include sufficient detail to describe the process to implement standard and emergency changes; moreover, Fiscal Service had not applied vendor security patches to this financial

[15] TIGTA, Ref. No. 2018-20-029, *Security Over High-Value Assets Should Be Strengthened* (May 2018), and TIGTA, Ref. No. 2018-20-030, *The Cybersecurity Data Warehouse Needs Improved Security Controls* (June 2018).
[16] GAO, GAO-18-165, *IRS's Fiscal Years 2017 and 2016 Financial Statements* (Nov. 2017), and GAO, GAO-18-391, *IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 2018).

management system's database production server. Fiscal Service also did not include the production database of another financial management system in its vulnerability scanning.

TIGTA reported that that IRS' CM program was not effective because it did not meet the Managed and Measurable maturity level; TIGTA assessed the program at the Defined maturity level.

According to DHS criteria, we assessed the RM program to be ineffective based on the maturity levels assessed in metric questions 14 to 21.

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: AC-1, IA-1, PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Maturity Level: **Consistently Implemented (Level 3)** – Stakeholders have adequate resources (people, processes, and technology) to effectively implement identity, credential, and access management activities.

Comments: This is the highest maturity level for this question.

PIO: DO and Mint should consider documenting plans to supplement vacant positions.

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.

Comments: For FY 2017 DO System 1, POA&M #16465 "The application does not require the use of multifactor authentication" was open.

PIO: OCC should consider implementing automation of tools that are in development. Mint should consider documenting an automated tracking of risk designations and screening information.

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: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; FY 2018 CIO FISMA Metrics: 2.3)?

Maturity Level: **Defined (Level 2)** - The organization has developed, documented, and disseminated its policies and procedures for ICAM. Policies and procedures have been tailored to the organization's environment and include specific requirements.

Comments: The BEP System 1 SSP was missing some access management controls and control enhancements. Fiscal Service System 2 had 3 out of 20 users were inactive for more than 120 days and were not disabled automatically. New hire training was not completed in a timely manner for Fiscal Service System 3 users. TIGTA has not established account management policies for the TIGTA System 1. (In the Findings section, refer to Finding #1 for BEP, Refer to Finding #7 for Fiscal Service.)

For Mint System 1, Mint did not consistently conduct semi-annual access reviews for privileged users and annual access reviews for non-privileged users, and Mint granted access for one out of two users prior to completing the background screening process. For Mint System 1, 231 user accounts were inactive for more than 120 days and were not disabled automatically within the system, and Mint did not remove Mint System 1 access for nine terminated users after the users' respective separation date. For Mint System 2, Mint did not conduct annual access reviews for non-privileged users. (Refer to Finding #7 in the Findings section for Mint)

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that while the IRS has developed, documented, and disseminated its policies and procedures for ICAM, it did not consistently implement them. TIGTA[17] reported that Criminal Investigation does not have an automated process for discovering and disabling inactive accounts. In addition, based on the maturity levels of metrics 26 through 31, the IRS does not meet Consistently Implemented.

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: PS-2, PS- 3; and National Insider Threat Policy; FY 2018 CIO FISMA Metrics: 2.16)?

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.

[17] TIGTA, Ref. No. 2018-20-034, *Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls* (June 2018).

Comments: As noted in question 25, TIGTA has not established account management policies for the TIGTA System 1, and Mint granted access to Mint System 1 for one out of two users prior to completing the background screening process. (In the Findings section, refer to Finding #7 for Mint and TIGTA.)

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: AC-8, PL-4, and PS-6)?

Maturity Level: **Defined (Level 2)** - The organization has defined its processes for developing, documenting, and maintaining access agreements for individuals that access its systems.

Comments: See comments in question 25. One out of the two new Fiscal Service operating system (OS) and database (DB) users did not complete the two trainings within the required timeframe.(Refer to Finding #7 in the Findings section for Fiscal Service.) For Do System 1, DO management issued self-identified weakness POA&M ID #16822: "Access agreements have not been updated within the last year."

FY 2015 Finding #1 for Mint, "Logical account management activities were not compliant with policies," was partially implemented/open.

28 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 Identity Assurance Level (IAL)3/ Authenticator Assurance Level (AAL) 3/ Federated Assurance Level (FAL) 3 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: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2018 CIO FISMA Metrics: 2.4; and Cybersecurity Sprint)?

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

Comments: Not Applicable (N/A)

29 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-62 r3 IAL 3/ AAL 3/ FAL 3 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2018 CIO FISMA Metrics: 2.5; and Cybersecurity Sprint)?

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

Comments: N/A

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 2018 CIO FISMA Metrics: 2.4 and 2.5; NIST SP 800-53: AC-1, AC-2 (2), AC-17; CSIP)?

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: See comments in question 25.

TIGTA management issued the self-identified POAM ID #10779: "TSIS: Monitoring Use of Accounts and Reviewing Compliance with Account Management Requirements through a Centralized, Automated Mechanism." For DO System 1, DO management issued POAM ID #16771: "Policy, Shared accounts in-use, and System accounts monitoring."

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: AC-17, SI-4; and FY 2018 CIO FISMA Metrics: 2.10)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization ensures that FIPS 140-2 validated cryptographic modules are implemented for its remote access connection method(s), remote access sessions time out after 30 minutes (or less), and that remote users' activities are logged and reviewed based on risk.

Comments: For FY 2017 DO System 1, POA&M #16460 "Accounts are not automatically disabled after a period of inactivity" was open.

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?

Comment: FY 2015 OCC System 1, POA&M #47: "Component-level audit requirements have not yet been determined and documented. Lack of auditing for the following: Audit database management event and Audit database object management event. This finding is applicable to the multiple applications within the system" is open.

TIGTA reported that that IRS' IA program was not effective because it did not meet the Managed and Measurable maturity level; TIGTA assessed the program at the Consistently Implemented maturity level.

According to DHS criteria, we assessed the RM program to be ineffective based on the maturity levels assessed in metric questions 23 to 31. Please refer to 13.1 for explanation.

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 900-122; OMB M-18-02; OMG A-130, Appendix I; NIST SP 800-53: 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 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., SSNs)

Comments: In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that the IRS did not provide evidence to show that it reviews and removes unnecessary PII collections on a regular basis.

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; Appendix J, SC-8, SC-28, MP-3, and MP-6; FY 2018 CIO FISMA Metrics: 2.9 and 2.10)?

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

Comments: In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that The IRS indicated that it has not fully implemented all elements of the Data Loss Prevention solution specifically related to data at rest. It will not meet the Consistently Implemented maturity level until this is accomplished. In addition, TIGTA[18] reported that the data at rest were not encrypted before or after transit in some cases, and no information was provided pertaining to sanitization of digital media. Also, the security documents reported that protection of information at rest was partially in place for two of the seven systems we selected for the FY2018 FISMA evaluation.

35 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: Appendix J, SE-2; FY 2018 SAOP FISMA Metrics: 3.8-3.12)?

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.

Comments: In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that The IRS did not meet the Consistently Implemented maturity level because it indicated that it is not checking outbound communications to detect encrypted exfiltration of information.

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: Appendix J, SE-2; FY 2018 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.

Comments: To improve its Data Privacy and Protection (DP) program, Treasury should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate.

[18] TIGTA, Ref. No. 2019-20-039, *Private Collection Agency Security Over Taxpayer Data Needs Improvement* (July 2018).

37 To what degree does the organization ensure that security awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53: 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.

Comments: To improve its DP program, Treasury should measure the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, Treasury should make updates to its program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing.

38 Provide any addition 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?

Comments: TIGTA reported that that IRS' DP program was not effective because it did not meet the Managed and Measurable maturity level; TIGTA assessed the program at the Defined maturity level.

According to DHS criteria, we assessed the DP program to be ineffective based on the maturity levels assessed in metric questions 33 to 37. Please refer to 13.1 for explanation.

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; AT-1; and NIST SP 800-50).

Maturity Level: **Consistently Implemented (Level 3)** – Roles and responsibilities for stakeholders involved in the organization's security awareness and training program have been defined and communicated across the organization. In addition, stakeholders have adequate resources (people, processes, and technology) to consistently implement security awareness and training responsibilities.

Comments: This is the highest maturity level for this question.

40 To what extent does the organization utilize of 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; 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.

Comments: In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year* 2018 (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that the IRS has not addressed all of its identified knowledge, skills, and abilities.

PIO: Fiscal Service should consider developing training based on an assessment of workforce needs.

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: AT-1; NIST SP 800-50: Section 3).

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

Comments: To improve its Security Training (ST) program, Treasury should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans.

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

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its policies and procedures for security awareness and specialized security training.

Comments: To improve its ST program, Treasury should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures.

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: AT-2; FY 2018 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; SANS Top 20: 17.4).

Maturity Level: **Consistently Implemented (Level 3)** – The organization ensures that all systems users complete the organization's security awareness training (or a comparable awareness training for contractors) prior to system access and periodically thereafter and maintains completion records. The organization obtains feedback on its security awareness and training program and uses that information to make improvements.

Comments: To improve its ST program, Treasury should measure 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.

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: AT-3 and AT-4; FY 2018 CIO FISMA Metrics: 2.15)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization ensures that individuals with significant security responsibilities are provided specialized security training prior to information system access or performing assigned duties and periodically thereafter and maintains appropriate records.

Comments: To improve its ST program, Treasury should obtain feedback on its security training content and make updates to its program, as appropriate. In addition, the Treasury should measure 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.

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

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

Comments: We determined that Treasury's security programs and practices for CM, IA, DP, and ST did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level. TIGTA reported that the IRS' CM, IA, and DP programs were not effective, but TIGTA reported that IRS' ST program was effective.

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?

Maturity Level: **Consistently Implemented (Level 3)**
Comments: TIGTA reported that that IRS' ST program was effective because it did met the Managed and Measurable maturity level.

According to DHS criteria, we assessed the Treasury' ST program to be ineffective based on the maturity levels assessed in metric questions 38 to 44. Please refer to 13.1 for explanation.

Function 3: Detect – ISCM

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

Comments: As commented in question 4 for Identify: 1 – Risk Management, TIGTA did not finalize and approve the TIGTA System 1 SSP and ensure that the NIST SP 800-53, Rev. 4, security controls were implemented.

FY 2017 Finding #1 for Mint, "Information security policies, procedures, and security plans were either outdated or incomplete," was open.

For FY 2017 Fiscal Service Systems 1, 2, and 3, POA&M #11715 "Unknown if security assessments performed on control enterprise infrastructure control" was open.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year* 2018 (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that the IRS is working to automate and develop additional performance measures for the processes and procedures that support ISCM.

PIO: BEP should consider documenting ISCM lesson learned activities to improve the ISCM program.

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: CA-7). (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.

Comments: Refer to comments in question 2. The BEP System 1 SSP did not document NIST SP 800-53, Rev. 4, controls CA-7 Continuous Monitoring. As commented in question 11, DO did not define, document, and implement the monitoring and reviewing controls and risks tracked by the cloud service provider as they relate to the status of security controls for DO System 3, which is hosted by a CSP. As commented in question 4. TIGTA did not finalize and approve the TIGTA System 1 SSP and ensure that the NIST SP 800-53, Rev. 4, security controls were implemented.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that the IRS is working to automate and develop additional performance measures for the processes and procedures that support ISCM.

PIO: TIGTA should consider capturing qualitative and quantitative performance measure reports to capture performance metrics along with defining a frequency to report for senior management review for TIGTA system.

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: CA-1; NIST SP 800-137; and FY 2018 CIO FISMA Metrics)?

Maturity Level: **Consistently Implemented (Level 3)** – Defined roles and responsibilities are consistently implemented and teams have adequate resources (people, processes, and technology) to effectively implement ISCM activities.

Comments: In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that the IRS's roles and responsibilities are documented and the Information Technology organization's Cybersecurity Office said that its workforce had increased. However, TIGTA[19] reported that the IRS's limited resources placed additional burden on asset management (which is part of the ISCM program plan). In addition, the GAO[20] reported that the IRS has a shortage of human resources with critical skills and will continue to face challenges in assessing and addressing the gaps in knowledge and skills that are critical to the success of its key information technology investments.

PIO: Mint should consider completing a workforce assessment to determine any resource gaps and needs. TIGTA should consider capturing qualitative and quantitative performance measure reports to capture performance metrics along with defining a frequency to report for senior management review for TIGTA system.

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: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?

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.

Comments: See comments for question 2 and for question 47. TIGTA did not finalize and approve the TIGTA System 1 SSP and ensure that the NIST SP 800-53, Rev. 4, security controls were implemented. For DO System 1, DO management issued POAM ID #16778: "Continuous Monitoring Plan."

[19] TIGTA, Ref. No. 2018-20-041, *Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability* (July 2018).
[20] GAO, GAO-18-298, *IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing* (June 2018).

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.

Comments: In the Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018 (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that the IRS is in the process of implementing a data analysis tool and reporting system to achieve requirements for data collection, storage, analysis, retrieval, and reporting.

PIO: TIGTA should consider capturing qualitative and quantitative performance measure reports to capture performance metrics along with defining a frequency to report for senior management review for TIGTA system.

51.1 Please provide the assessed maturity level for the agency's Detect - ISCM function.

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

Comments: We determined that Treasury 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?

Comments: TIGTA reported that that IRS' ISCM program was not effective because it did not meet the Managed and Measurable maturity level; TIGTA assessed IRS' ISCM at the Consistently Implemented maturity level.

We have not additional information that was not already covered in metric questions 46 to 50 above. According to DHS criteria, we assessed the ISCM program to be ineffective. Please refer to 51.2 for explanation.

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: IR-1; NIST 800-61 Rev. 2; NIST SP 800-184; OMB M-17-25; FY 2018 CIO FISMA Metrics: 4.1, 4.3, 4.6, and 5.3; 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.

Comments: In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018* (Reference number 2018-20-082), dated September 21, 2018, TIGTA reported that 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; IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMG M-16-24; FY 2018 CIO FISMA Metrics: Section 4; and US-CERT Federal Incident Notification Guidelines?

Maturity Level: **Consistently Implemented (Level 3)** – Defined roles and responsibilities are consistently implemented and teams have adequate resources (people, processes, and technology) to consistently implement incident response activities.

Comments: To improve its Incident Response (IR) program, Treasury should assign responsibility for monitoring and tracking the effectiveness of incident response activities. Treasury staff should consistently collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of incident response activities.

54 How mature are the organization's processes for incident detection and analysis (NIST SP 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-18-02; 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.

Comments: To improve its IR program, Treasury 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.

55 How mature are the organization's processes for incident handling (NIST SP 800-53: IR-4; NIST SP 800-61, Rev. 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.

Comments: To improve its IR program, Treasury should manage and measure the impact of successful incidents and be 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 800-53: IR-6; US-CERT Incident Notification Guidelines; PPD-41; 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.

Comments: To improve its IR program, Treasury should use incident response metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.

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 (FY 2018 CIO FISMA Metrics: 4.4; NIST SP 800-86; NIST SP 800-53: IR-4; OMB M-18-02; PPD-41).

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently utilizes on-site, technical assistance/surge capabilities offered by DHS or ensures that such capabilities are in place and can be leveraged when needed. In addition, the organization has entered into contractual relationships in support of incident response processes (e.g., for forensic support), as needed. The organization has fully deployed DHS's Einstein 1 and 2 to screen all traffic entering and leaving its network through a TIC.

Comments: To improve its IR program, Treasury should utilize Einstein 3 Accelerated to detect and proactively block cyber-attacks or prevent potential compromises.

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 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.

Comments: For DO System 2, DO management issued self-identified weaknesses in POA&M ID #21697: "There is not a current procedure for ISSO review of audit logs and reports" and POA&M ID #21698: "DO System 2 has not defined specific audit log requirements for the SIEM capability."

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

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

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 as the Consistently Implemented maturity level.

59.1 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?

Comments: TIGTA reported that IRS' IR program was effective because it met the Managed and Measurable maturity level.

We have no additional information that was not already covered in metric questions 52 to 58 above. According to DHS criteria, we assessed the IR program to be ineffective. Please refer to 59.1 for 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: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization has established appropriate teams that are ready to implement its information system contingency planning strategies. Stakeholders and teams have adequate resources (people, processes, and technology) to effectively implement system contingency planning activities.

Comments: This is the highest maturity level for this question.

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; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5).

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.

Comments: TIGTA has not conducted a Business Impact Analysis (BIA) for the TIGTA System 1. In addition, TIGTA has not established an Information Security Contingency Plan (ISCP) for TIGTA System1, and the bureau had not completed disaster recovery and business continuity testing for this system. (Refer to Finding #8 for TIGTA)

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: CP-2; NIST SP 800-34, Rev. 1, 3.2, FIPS 199, FCD-1, OMB M-17-09; FY 2018 CIO FISMA Metrics: 5.6)?

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 BIAs are integrated with the organizational level BIA and include: characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high-value assets.

Comments: See comment in question 60. FY 2017 Finding #7, "Contingency planning activities were not compliant with policies," was closed BEP and open for Mint.

63 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST 800-53: CP-2; NIST 800-34; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

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.

Comments: See comment in question 60.

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: CP-3, CP-4; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

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 Operations (COOP)/Business Continuity Planning (BCP).

Comments: See comment in question 60. For DO System 1, DO management issued self-identified weaknesses in POA&M ID #16813: Contingency Training and POA&M ID #16814: Contingency Plan Test.

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: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD1; NIST CSF: PR.IP- 4; FY 2018 CIO FISMA Metrics)?

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 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.

Comments: See comment in question 60.

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: CP-2, 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.

Comments: See comment in question 60.

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

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

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?

Comments: TIGTA reported that IRS' CP program was effective because it met the Managed and Measurable maturity level.

We have no additional information that was not already covered in metric questions 60 to 66 above. According to DHS criteria, we assessed the IR program to be ineffective. Please refer to 67.1 for explanation.

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

Function 0: Overall

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

Not Effective

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.

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 Risk Management, Configuration Management, Identity and Access Management, and Contingency Planning. In addition, we did not assess any of the FISMA Metric Domains as Managed and Measurable (Level 4). The FY 2018 IG FISMA Reporting Metrics define an effective information security program as Managed and Measurable (Level 4).

Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	10
Managed and Measurable	0
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	0
Consistently Implemented	3
Managed and Measurable	4
Optimized	2
Function Rating: Consistently Implemented (Level 3)	

Function 2C: Protect – Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	4
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	6
Managed and Measurable	0
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	7
Consistently Implemented	0
Managed and Measurable	0
Optimized	
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 for Risk Management 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 Configuration Management did not meet the Managed and Measurable

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
			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 Identity and Access Management 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 Data Privacy and Protection did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 2D: Protect – Security Training	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's security program and practices for Security Training did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 3: Detect - ISCM	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's security program and practices for Information Security Continuous Monitoring 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 Incident Response 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 Contingency Planning 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 Risk Management, Configuration Management, Identity and Access Management, and Contingency Planning. 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) 2018 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 in-scope systems for the FY 2018 Department of Treasury (Treasury or Department) 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 Treasury Inspector General for Tax Administration (TIGTA).

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 FISMA inventory of systems. All Treasury bureaus and offices were required to register their IT systems with the Department. KPMG then employed a random sampling approach to determine the subset of Treasury's operational information systems to support the FY 2018 FISMA Performance Audit for unclassified systems.

KPMG considered the following factors during the selection process:

- Department of the Treasury High Value Asset[21] listing.
- Total number of financial and operational systems per bureau, excluded systems in the implementation, development, and disposal phases.

In addition, we excluded information systems that were selected in support of the FYs 2015, 2016, and 2017 FISMA audits to avoid redundancy. Table 3 summarizes our considerations for selecting the in-scope systems for the 2018 performance audit.

Table 3: *Considerations for selecting systems for the 2018 performance audit.*

#	Bureau	Total # of Operational Info. Systems	Number of Information Systems Considered After Analysis	Number of Information Systems Selected
1	BEP	13	6	1
2	DO	48	41	2
3	Fiscal Service	76	62	3[22]
4	Mint	19	16	2
5	OCC	29	26	1
6	TIGTA	3	2	1
	Totals	**188**	**153**	**10**

[21] 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.
[22] One of these systems was randomly selected from the High Value Asset listing.

Using a random number generator, KPMG randomly selected 10 of 148 operational systems. Table 3 below denotes the selected application and systems for the 2018 performance audit.

Table 4: *Selected application and systems for the 2018 performance audit.*

Bureau	System	FIPS 199	System Type	Financial System	Disposition	High Value Asset
BEP	BEP System 1	Moderate	Major Application	No	Operational	No
DO	DO System 1	Moderate	Major Application	No	Operational	No
	DO System 2	Moderate	Other	No	Operational	No
Fiscal Service	Fiscal Service System 1	Moderate	Major Application	No	Operational	No
	Fiscal Service System 2	High	Major Application	No	Operational	No
	Fiscal Service System 3	High	Major Application	Yes	Operational	Yes
Mint	Mint System 1	Low	Minor Application	No	Operational	No
	Mint System 2	Moderate	Minor Application	No	Operational	No
OCC	OCC System 1	Moderate	General Support System	No	Operational	No
TIGTA	TIGTA System 1	Moderate	General Support System	No	Operational	No

APPENDIX V – GLOSSARY OF TERMS

Acronym	Definition
AC	Access Control
ACIOCS	Associate Chief Information Officer for Cyber Security
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
Bureaus	Department of the Treasury Bureaus/Offices
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
DO	Departmental Offices
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
HSPD	Homeland Security Presidential Directive
IA	Identity and Access Management
IG	Inspector General
IR	Incident Response
IRS	Internal Revenue Service
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
ISSO	Information Systems Security Officer
ISCP	Information System Contingency Plan
IT	Information Technology

Acronym	Definition
KPMG	KPMG LLP
Mint	United States Mint
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
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
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
SI	System and Information Integrity
SIGTARP	Special Inspector General for the Troubled Asset Relief Program
SO	System Owner
SOP	Standard Operating Procedure
SP	Special Publication
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 2018
September 21, 2018

THIS PAGE INTENTIONALLY LEFT BLANK

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018

September 21, 2018

Reference Number: 2018-20-082

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.

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION – FEDERAL INFORMATION SECURITY MODERNIZATION ACT FOR FISCAL YEAR 2018

Highlights

Final Report issued on September 21, 2018

Highlights of Reference Number: 2018-20-082 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 custodian of this taxpayer information, the IRS has an obligation in accordance with FISMA requirements to protect 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 2018.

WHAT TIGTA FOUND

For Fiscal Year 2018, 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: IDENTITY (organizational understanding to manage cybersecurity risk to assets and capabilities), PROTECT (appropriate safeguards to ensure delivery of critical infrastructure 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 attributes not yet implemented. The Department of Homeland Security's scoring methodology defines "effective" as having maturity level 4, *Managed and Measured*, 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 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 Managed*; Data Protection and Privacy, which was at maturity level 2, *Defined*; 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 Managed*. The DETECT function area rating was based on the Information Security Continuous Monitoring metrics, which TIGTA deemed at maturity level 3, *Consistently Implemented.*

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 include 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 21, 2018

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 – Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2018 (Audit # 201820001)

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 2018. 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 determine the progress made by the IRS in meeting the requirements of the FISMA mandatory review of its unclassified information technology system security program. This audit is included in our Fiscal Year 2018 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.

[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.

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

Table of Contents

Abbreviations

DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
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	Plan 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. The 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, contractor, or other sources. It assigns specific responsibilities to agency heads and Inspectors General in complying with requirements of the 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.

The 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 the 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, the 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. The 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 provides 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 Office 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 Office is tasked with preserving the confidentiality, integrity, and availability of the IRS systems and its data.

Fiscal Year 2018 Inspector General FISMA Reporting Metrics

The Fiscal Year (FY)[2] 2018 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 FY 2018 metrics represent a continuation of work that began in FY 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:

- IDENTITY – 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 infrastructure 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).

The DHS issued the *Fiscal Year (FY) 2018 Inspector General Federal Security Modernization Act of 2014 Reporting Metrics*[4] with one significant metric domain addition from the prior year. The DHS added the *Data Protection and Privacy* domain to better align with the NIST Cybersecurity Framework. 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 FY 2018 Inspector General FISMA Metric Domains

Cybersecurity Framework's Function Areas	FY 2018 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: FY 2018 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.[5]

[4] DHS, *FY 2018 Inspector General Federal Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0* (April 11, 2018).

[5] NIST Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013; updated as of Jan. 2014), defines security control effectiveness as the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies.

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: FY 2018 Inspector General FISMA Reporting Metrics.

This review was performed with information obtained from the Information Technology organization's Cybersecurity Office in the New Carrollton Federal Building during the period April through September 2018. This report covers the FY 2018 FISMA evaluation period from July 1, 2017, through June 30, 2018. 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 not yet implemented, 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 *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0*. 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 performed or completed during the FY 2018 FISMA evaluation period, July 1, 2017 to June 30, 2018, that contained results applicable to the FISMA metrics. See Appendix IV for a list of 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) Defined (Level 2) Managed and Measurable (Level 4)	No
DETECT – ISCM	Consistently Implemented (Level 3)	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 FY 2018 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, respectively, achieved a *Managed and Measurable* maturity level 4, and therefore were deemed as "effective." The details of the results of our evaluation of the maturity levels are presented on pages 8, 26, and 28, respectively.

For the remaining two Cybersecurity Framework function areas, PROTECT and DETECT, we found four of their five security program components did not meet a *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, 16, 20, 22, and 24.

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 FY 2018 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, the security program components of Configuration Management, Identity and Access Management, and Data Protection and Privacy rated at a *Defined* maturity level 2, *Consistently Implemented* maturity level 3, and *Defined* maturity level 2, respectively. As a result, these three program components were considered "not effective." Because three of the four program components were "not effective," we rated the entire area as "not effective," and the end result for this function area was a maturity level 3.

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

- Ensure that policy and procedures for maintaining baseline configurations or component inventories, secure configurations settings in compliance with IRS policy, flaw remediation and patching, and configuration change control are consistently implemented.
- Use automated processes for discovering and disabling accounts.
- Ensure that all nonprivileged and privileged users use strong authentication to access IRS information systems.

- Ensure that privileged accounts are provisioned, managed, and reviewed.
- 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.
- Implement security controls to prevent data exfiltration, including checking outbound communications to detect encrypted exfiltration of information.
- Ensure that updates are made to its privacy program as a result of training exercises.

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

Based on the FY 2018 Inspector General FISMA Reporting Metrics, we found that the function area DETECT and its security program component, ISCM, met a *Consistently Implemented* maturity level 3. 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 automate and develop additional performance measures for the processes and procedures that support ISCM.
- Address the challenge of a shortage of human resources with critical skills in order to address the gaps in knowledge and skills that are essential to the success of key information technology investments.
- Continue to implement a data analysis tool and reporting system to achieve requirements for data collection, storage, analysis, retrieval, and reporting.

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 FY 2018 Inspector General FISMA Reporting Metrics

The details of the results of our evaluation of the maturity level of each of the FY 2018 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 and OMB memoranda. For metrics we rated lower than a maturity level 4, 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 FY 2018 Inspector General FISMA Reporting Metrics.

Function Area 1: IDENTIFY – Risk Management

Maturity Level	Count
Ad-Hoc	**0**
Defined	**4**
Consistently Implemented	**2**
Managed and Measurable	**6**
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?

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

   Comments: TIGTA[7] 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 used in the organization's environment with detailed information for tracking and reporting.

[6] Taxonomy is a scheme of classifications.
[7] TIGTA, Ref. No. 2018-20-041, *Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability* (July 2018).

Comments: The IRS is still in the process of implementing systems for compiling a reliable software inventory.

4. To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions?

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

   Comments: This is the highest maturity level for this metric.

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

   Maturity Level: ***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 reportable 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 system 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 stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission-specific resources been defined and communicated across the organization?

   Maturity Level: ***Managed and Measurable*** **(Level 4)** – The organization uses 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&M) 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 97 weaknesses that the IRS identified during the annual testing of controls of the seven selected systems. Of the 97 weaknesses, we could not track nine weaknesses to either existing or closed POA&Ms that supported effective remediation. In addition, we reviewed 21 POA&Ms that were closed in FY 2018 related to the seven selected systems. Of the 21 POA&Ms that were closed, four POA&Ms were closed without sufficient support that the weaknesses were corrected even though the IRS had validated the closures through its closure verification process. After we brought this to the IRS's attention, it provided additional evidence for one POA&M closure and reopened the other three POA&Ms.

In April 2018, the IRS issued new standard operating procedures on timely reporting weaknesses for the general support system's components directly supporting the application that may affect the security posture of the application. However, we are unable to verify that the new processes are consistently implemented because enough time has not transpired to evaluate a material number of closed 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: In our review of the IRS's system risk assessments of the seven systems selected for the FY 2018 FISMA evaluation, we identified issues with security control testing. Security controls were not reliably tested according to the assessment procedures. For example, the IRS used an outdated compliance checker to test the configuration controls of systems, with no risk-based decision in place for using the outdated compliance checker. In addition, the results of the security test showed that the controls passed testing; however, results of other tests indicate that *pass* was not a reasonable conclusion.

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[8] clauses, and clauses on protection, detection, and reporting of information) and Service Level Agreements[9] are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services?

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

12. To what extent does the organization utilize technology (such as a governance, risk management, and compliance tools) 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 continues to work with the DHS to implement Continuous Diagnostic and Mitigation solutions, the IRS has progressed in leveraging technology to data mine and generate several dashboards to help ascertain a view of risk across the agency.

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?

    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*.

[8] The Federal Acquisition Regulation is the primary regulation for use by all Federal executive agencies in their acquisition of supplies and services with appropriate funds.
[9] 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.

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)** – Stakeholders have adequate resources (people, processes, and technology) to consistently implement information system configuration management activities.

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

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;[10] 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.

[10] 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.

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.

    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 three of the seven systems we selected for the FY 2018 FISMA evaluation did not consistently maintain baseline configurations. Further, the annual security testing reported that two of seven systems did not maintain and have an up-to-date information system component inventory. In addition, TIGTA[11] and the GAO[12] 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?

[11] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017); TIGTA, Ref. No. 2017-20-032, *The Internal Revenue Service Does Not Have a Cloud Strategy and Did Not Adhere to Federal Policy When Deploying a Cloud Service* (Aug. 2017); TIGTA, Ref. No. 2018-20-029, *Security Over High-Value Assets Should Be Strengthened* (May 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. 2018-20-030, *The Cybersecurity Data Warehouse Needs Improved Security Controls* (June 2018); TIGTA, Ref. No. 2018-20-041, *Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability* (July 2018); and TIGTA, Ref. No. 2018-20-066, *Controls Continue to Need Improvement to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented and Documented* (Sept. 2018).

[12] GAO, GAO-18-391, *IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 2018).

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

Comments: While the IRS has defined common secure configurations, it has not ensured that its information systems consistently maintain secure configuration settings in compliance with IRS policy. The IRS's annual security testing of systems reported that six of the seven systems we selected for the FY 2018 FISMA evaluation did not maintain secure configuration settings in accordance with IRS policy. In addition, least functionality controls were not in place for five of the seven systems, and flaw remediation processes were not in place for three of the seven systems.

Also, TIGTA[13] and the GAO[14] reported findings of systems that did not maintain secure configuration settings in accordance with agency policy. Further, the IRS's tool to assess configuration settings is not Security Content Automation Protocol–compliant.[15] In addition, the GAO reported that the mainframe tools only test compliance with a limited subset of 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 organizationally defined timelines; and incorporating flaw remediation into the organization's configuration management processes.

[13] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017); TIGTA, Ref. No. 2018-20-029, *Security Over High-Value Assets Should Be Strengthened* (May 2018); TIGTA, Ref. No. 2018-20-039, *Private Collection Agency Security Over Taxpayer Data Needs Improvement* (July 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. 2018-20-034, *Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls* (June 2018); and 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).

[14] GAO, GAO-18-165, *IRS's Fiscal Years 2017 and 2016 Financial Statements* (Nov. 2017), and GAO, GAO-18-391, *IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 2018).

[15] 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.

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 processes were not in place for three of the seven systems we selected for the FY 2018 FISMA evaluation. Also, TIGTA[16] and the GAO[17] reported that the IRS did not remediate high-risk vulnerabilities or install security patches on systems in a timely manner.

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

    Maturity Level: ***Consistently Implemented*** **(Level 3)** – The organization has consistently implemented its Trusted Internet Connection–approved connections and critical capabilities that it manages internally. The organization had 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,[18] 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 activities related to configuration change control.

[16] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017); TIGTA, Ref. No. 2018-20-029, *Security Over High-Value Assets Should Be Strengthened* (May 2018); TIGTA, Ref. No. 2018-20-039, *Private Collection Agency Security Over Taxpayer Data Needs Improvement* (July 2018); TIGTA, Ref. No. 2018-20-036, *The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved* (July 2018); and 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).

[17] GAO, GAO-18-165, *IRS's Fiscal Years 2017 and 2016 Financial Statements* (Nov. 2017), and GAO, GAO-18-391, *IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 2018).

[18] A group of qualified people with responsibilities for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system.

Comments: While the IRS has defined policy and procedures for managing configuration change control, these policy and procedures have not been consistently followed at the information system level. The IRS's annual security testing of systems reported that two of the seven systems selected for the FY 2018 FISMA evaluation had failed security controls related to change management practices. In addition, two of the seven systems did not have baseline configurations in place for some of their components. Also, TIGTA[19] and the GAO[20] 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?

    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*.

    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	**3**
Consistently Implemented	**4**
Managed and Measurable	**1**
Optimized	**1**
Function Rating: *Consistently Implemented* (Level 3)	

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?

[19] TIGTA, Ref. No. 2018-20-029, *Security Over High-Value Assets Should Be Strengthened* (May 2018), and TIGTA, Ref. No. 2018-20-030, *The Cybersecurity Data Warehouse Needs Improved Security Controls* (June 2018).
[20] GAO, GAO-18-165, *IRS's Fiscal Years 2017 and 2016 Financial Statements* (Nov. 2017), and GAO, GAO-18-391, *IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 2018).

Maturity Level: ***Consistently Implemented*** **(Level 3)** – Stakeholders have adequate resources (people, processes, and technology) to effectively implement ICAM activities.

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

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 working with the bureaus to address challenges and is preparing to roll out Phase 2. 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: ***Defined*** **(Level 2)** – The organization has developed, documented, and disseminated its policies and procedures for ICAM. Policies and procedures have been tailored to the organization's environment and include specific requirements.

    Comments: While the IRS has developed, documented, and disseminated its policies and procedures for ICAM, it did not consistently implement them. TIGTA[21] reported that Criminal Investigation does not have an automated process for discovering and disabling inactive accounts. In addition, based on the maturity levels of metrics 26 through 31, the IRS does not meet *Consistently Implemented*.

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 partners.

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 nonprivileged 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 nonprivileged users are maintained, as necessary.

[21] TIGTA, Ref. No. 2018-20-034, *Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls* (June 2018).

28. To what extent has the organization implemented strong authentication mechanisms (two-factor Personal Identity Verification credential or other NIST Special Publication 800-63-3[22] Identity Assurance Level 3/Authenticator Assurance Level 3/ Federation Assurance Level 3 credential) for nonprivileged 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 nonprivileged 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 nonprivileged users are required to use Personal Identity Verification cards to access the network, it reported that only nine of 131 internal systems are configured to require Personal Identity Verification cards.

29. To what extent has the organization implemented strong authentication mechanisms (two-factor Personal Identity Verification credential or other NIST Special Publication 800-63-3 Identity Assurance Level 3/Authenticator Assurance Level 3/ Federation Assurance Level 3 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 nine of 131 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 user's accounts.

[22] NIST, Special Publication 800-63-3, *Digital Identity Guidelines* (June 2017).

Comments: GAO[23] reported that authorization control deficiencies still existed in the IRS's computing environment. In addition, TIGTA[24] reported that the IRS could not readily identify all individuals who had privileged access to its high-value asset components.

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 timeouts, 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 timeouts, and how it monitors and controls remote access sessions.

    Comments: The IRS has not implemented encryption complaint with Federal Information Processing Standard Publication 140-2[25] on all of its remote access connections. The IRS's annual security testing of systems reported that three of seven systems we selected for the FY2018 FISMA evaluation were not compliant with encryption requirements.

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?

    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*.

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

[23] GAO, GAO-18-391, *IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 2018).
[24] TIGTA, Ref. No. 2018-20-029, *Security Over High-Value Assets Should Be Strengthened* (May 2018).
[25] NIST, Federal Information Processing Standard Publication 140-2, *Security Requirements for Cryptographic Modules* (May 2001).

Function Area 2c: PROTECT – Data Protection and Privacy

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

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 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 evidence to show that it reviews and removes unnecessary Personally Identifiable Information collections on a regular basis.

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, 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 specified areas. Further, the policies and procedures have been tailored to the organization's environment and include specific considerations based on data classification and sensitivity.

    Comments: The IRS indicated that it has not fully implemented all elements of the Data Loss Prevention solution specifically related to data at rest. It will not meet the *Consistently Implemented* maturity level until this is accomplished. In addition, TIGTA[26] reported that the

[26] TIGTA, Ref. No. 2019-20-039, *Private Collection Agency Security Over Taxpayer Data Needs Improvement* (July 2018).

data at rest were not encrypted before or after transit in some cases, and no information was provided pertaining to sanitization of digital media. Also, the security documents reported that protection of information at rest was partially in place for two of the seven systems we selected for the FY2018 FISMA evaluation.

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

    Maturity Level: ***Defined*** **(Level 2)** – The organization has defined and communicated its policies and procedures for data exfiltration and enhanced network defenses.

    Comment: The IRS did not meet the *Consistently Implemented* maturity level because it indicated that it is not checking outbound communications to detect encrypted exfiltration of information.

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

    Maturity Level: ***Managed and Measurable*** **(Level 4)** – The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

37. To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974[27] and E-Government Act of 2002;[28] 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 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 evidence to show that it makes updates to its privacy program as a result of the training exercises.

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.

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

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?

Maturity Level: ***Defined*** **(Level 2)** – Based on the performing results for metrics 33 through 37, this function was evaluated at a maturity level 2, *Defined*.

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)	

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)** – Roles and responsibilities for stakeholders involved in the organization's security awareness and training program have been defined and communicated across the organization. In addition, stakeholders have adequate resources (people, processes, and technology) to consistently implement security awareness and training responsibilities.

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

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 function 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 has not addressed all of its identified knowledge, skills, and abilities.

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, 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 or training and 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 training program by, for

example, conducting phishing exercises and following up with additional awareness or training and disciplinary actions, 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?

    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*.

    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	**2**
Consistently Implemented	**2**
Managed and Measurable	**1**
Optimized	**0**
Function Rating: *Consistently Implemented* (Level 3)	

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

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

    Comments: The IRS is working to automate and develop additional performance measures for the processes and procedures that support ISCM.

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: ***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.

Comments: The IRS is working to automate and develop additional performance measures for the processes and procedures that support ISCM.

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: ***Defined*** (**Level 2)** – The organization has defined and communicated the structure of its ISCM team, roles and responsibilities of ISCM stakeholders, and levels of authority and dependencies.

    Comments: The IRS's roles and responsibilities are documented and the Information Technology organization's Cybersecurity Office said that its workforce had increased. However, TIGTA[29] reported that the IRS's limited resources placed additional burden on asset management (which is part of the ISCM program plan). In addition, the GAO[30] reported that the IRS has a shortage of human resources with critical skills and will continue to face challenges in assessing and addressing the gaps in knowledge and skills that are critical to the success of its key information technology investments.

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

    Maturity Level: ***Managed and Measurable*** **(Level 4)** – The organization uses the results of security control assessments and monitoring to maintain ongoing authorization of information systems.

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 ICSM program, achieve situational awareness, and control ongoing risk. In addition, the

[29] TIGTA, Ref. No. 2018-20-041, *Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability* (July 2018).
[30] GAO, GAO-18-298, *IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing* (June 2018).

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 is in the process of implementing a data analysis tool and reporting system to achieve requirements for data collection, storage, analysis, retrieval, and reporting.

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

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

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 through 58.)

Maturity Level: ***Consistently Implemented*** **(Level 3)** – The organization consistently implements its incident response policies, procedures, plans, and strategies. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of 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)** – The organization has assigned responsibility for monitoring and tracking the effectiveness of incident response activities. Staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures on the effectiveness of incident response activities.

    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: ***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, antivirus and antispam software, and file integrity checking software.

    Comments: The IRS did not provide sufficient evidence to support that it runs file integrity software to derive checksums for critical files.

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

    Maturity Level: ***Optimized*** **(Level 5)** – The organization uses 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: ***Managed and Measurable*** **(Level 4)** – Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.

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

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 uses Einstein 3 Accelerated to detect and proactively block cyberattacks or prevent potential compromises.

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

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

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

    Maturity Level: ***Managed and Measurable*** **(Level 4)** – The organization uses technology for monitoring and analyzing qualitative and quantitative performance across the organization and its 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?

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

    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: *Managed 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)** – The organization has established appropriate teams that are ready to implement its information system contingency planning strategies. Stakeholders and teams have adequate resources (people, processes, and technology) to effectively implement system contingency planning activities.

    Comments: This is the highest maturity level of this metric.

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

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

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

    Maturity Level: ***Consistently Implemented*** **(Level 3)** – The organization 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 resources 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/ high-value assets.

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

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

Maturity Level: ***Managed and Measurable*** **(Level 4)** – The organization is able to integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency, as appropriate to deliver persistent situational awareness across the organization.

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

    Maturity Level: ***Managed and Measureable*** **(Level 4)** – The organization employs automated mechanisms to more thoroughly and effectively test system contingency plans.

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,[31] as appropriate, have been defined. The organization has considered alternate 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. Alternate storage site and backup of information at the user and system levels are not in place for one of the seven systems we selected for the FY 2018 FISMA evaluation. In addition, the IRS's annual security testing of organizational common controls reported that it does not perform backup testing according to IRS standards. Furthermore, the GAO[32] reported that the IRS did not update the system security plan to reflect change to the operating environment.

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 supporting the metrics are obtained accurately, consistently, and in a reproducible format.

[31] 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.
[32] GAO, GAO-18-391, *IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 2018).

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?

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

    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 determine the progress made by the IRS in meeting the requirements of FISMA mandatory review of its unclassified information technology system security program. To accomplish our objective, we determined the maturity level for the metrics contained in the FY 2018 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 FY 2018 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 Prevention 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.

VII. Determine the effectiveness of the Contingency Planning program.

We based our evaluation work, in part, on a representative subset of seven major 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

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

Treasury FISMA Information Management System of general support systems, major applications, and minor applications with a security classification of “Moderate” or “High” as the population for this subset. We used a random number table to select information systems within this population. Generally, if an information system gets selected that was selected in the past three FISMA reviews, we reselected for that system.

We also considered the results of TIGTA audits performed or completed during the FY 2018 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
Jason McKnight, Acting Audit Manager
Ryan Perry, Acting Audit Manager
Midori Ohno, Lead Auditor
Charles Ekunwe, Senior Auditor
Bret Hunter, Senior Auditor
Steven Stephens, Senior Auditor
Esther Wilson, Senior Auditor
Linda Nethery, 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, Office of Audit Coordination

Appendix IV

Information Technology Security-Related Audits Performed or Completed During the Fiscal Year 2018 Evaluation Period

1. TIGTA, Ref. No. 2017-20-032, *The Internal Revenue Service Does Not Have a Cloud Strategy and Did Not Adhere to Federal Policy When Deploying a Cloud Service* (Aug. 2017).
2. TIGTA, Ref. No. 2017-20-064, *The Identity Theft Tax Refund Fraud Information Sharing and Analysis Center Generally Adhered to Data Protection Standards, but Additional Actions Are Needed* (Sept. 2017).
3. TIGTA, Ref. No. 2017-20-062, *The Internal Revenue Service Is Not in Compliance With Federal Requirements for Software Asset Management* (Sept. 2017).
4. TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017).
5. GAO, GAO-18-165, *IRS's Fiscal Years 2017 and 2016 Financial Statements* (Nov. 2017).
6. TIGTA, Ref. No. 2018-20-007, *Electronic Authentication Process Controls Have Been Improved, but Have Not Yet Been Fully Implemented* (Feb. 2018).
7. TIGTA, Ref. No. 2018-20-029, *Security Over High-Value Assets Should Be Strengthened* (May 2018).
8. TIGTA, Ref. No. 2018-20-030, *The Cybersecurity Data Warehouse Needs Improved Security Controls* (June 2018).
9. TIGTA, Ref. No. 2018-20-034, *Active Directory Oversight Needs Improvement and Criminal Investigation Computer Rooms Lack Minimum Security Controls* (June 2018).
10. GAO, GAO-18-298, *IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing* (June 2018).
11. TIGTA, Ref. No. 2018-20-041, *Management Controls Should Be Strengthened to Improve Hardware Asset Inventory Reliability* (July 2018).
12. TIGTA, Ref. No. 2018-20-036, *The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved* (July 2018).

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

14. GAO, GAO-18-391, *IRS Needs to Rectify Control Deficiencies That Limit Its Effectiveness in Protecting Sensitive Financial Taxpayer Data* (July 2018).

15. 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).

Treasury OIG Website

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

Report Waste, Fraud, and Abuse

OIG Hotline for Treasury Programs and Operations – Call toll free: 1-800-359-3898
Gulf Coast Restoration Hotline – Call toll free: 1-855-584.GULF (4853)
Email: Hotline@oig.treas.gov
Submit a complaint using our online form:
https://www.treasury.gov/about/organizational-structure/ig/Pages/OigOnlineHotlineForm.aspx