Audit Report

OIG-18-004

INFORMATION TECHNOLOGY: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2017 Performance Audit

October 27, 2017

Office of Inspector General

Department of the Treasury

THIS PAGE INTENTIONALLY LEFT BLANK

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 27, 2017

MEMORANDUM FOR KODY KINSLEY
ASSISTANT SECRETARY FOR MANAGEMENT

ERIC OLSON
ACTING 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 2017 Performance Audit*

We are pleased to transmit the following reports:

- *Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2017 Performance Audit*, dated October 26, 2017, (Attachment 1); and

- *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017*, dated September 29, 2017 (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 programs and practices for its unclassified systems were established and have been maintained for the 5 Cybersecurity Functions and 7 FISMA program areas. However, KPMG identified 7 deficiencies within 3 of the 5 Cybersecurity Functions and within 4 of the 7 FISMA program areas. Accordingly, KPMG made 32 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. Specifically, TIGTA rated 3 of the 5 Cybersecurity Functions and 4 out of the 7 FISMA program areas as not effective.

Appendix III of the attached KPMG report includes *The Department of the Treasury's Consolidated Response to DHS's FISMA 2017 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 2017 Performance Audit
October 26, 2017

Department of the Treasury
Federal Information Security Modernization Act
Fiscal Year 2017 Performance Audit

October 26, 2017

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

Department of the Treasury
Federal Information Security Modernization Act Fiscal Year 2017 Performance Audit

Table of Contents

FISMA Performance Audit Report

Appendices

KPMG

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 2017 Performance Audit

Dear Mr. Thorson:

This report presents the results of our independent performance audit of the Department of the Treasury's (Treasury or Department) information security program and practices for its unclassified systems. The Federal Information Security Modernization Act of 2014 (FISMA) requires Federal agencies, including 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' FISMA 2017 Questions for Inspectors General,* dated April 17, 2017, provides Treasury's response to the CyberScope questionnaire*.* We also considered applicable OMB policy and guidelines and the National Institute of Standards and Technology (NIST) standards and guidelines. FISMA requires that the agency Inspector General (IG) or an independent external auditor perform the annual evaluation as determined by the IG. The Treasury Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct an audit of Treasury's information security program and practices for its unclassified systems.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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. We also followed the American Institute of Certified Public Accountants (AICPA) standards applicable to performance audits.

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, 2016 through June 30, 2017. As part of our audit, we responded to the DHS *FISMA 2017 Questions for Inspectors General*, dated April 17, 2017, 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 2017 Questions for Inspectors General*.

Additional details regarding the scope of our independent performance audit are included in Appendix I, *Objectives, 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 7 FISMA Metric Domains.[2] However, the program was not fully effective as reflected in the 7 deficiencies within 3 of the 5 Cybersecurity Functions and within 4 of the 7 FISMA program areas that we identified as follows:

Cybersecurity Function: Identify

1. Information security policies, procedures, and security plans were either outdated or incomplete at the Bureau of Engraving and Printing (BEP) and United States Mint (Mint). (Risk Management)
2. Asset management processes were not fully implemented at the Bureau of the Fiscal Service (Fiscal Service). (Risk Management)
3. System inventory reviews were inconsistent at the Alcohol and Tobacco Tax and Trade Bureau (TTB). (Risk Management)

Cybersecurity Function: Protect

4. Configuration compliance and vulnerability scanning were not consistently performed at BEP, Fiscal Service, Department Offices (DO), and TTB. (Configuration Management)
5. Missing or inconsistent patch management practices existed at BEP, DO, and TTB. (Configuraton Management)
6. Account management activities were not compliant with System Security Policies (SSPs) at Mint, Financial Crimes Enforcement Network (FinCEN), TTB, and BEP. (Identity and Access Management)

Cybersecurity Function: Recover

7. Contingency planning activities were not compliant with policies at BEP and Mint. (Contingency Planning)

We made 32 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 Acting Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO) agreed with our findings and recommendations (see *Management Response).* Treasury's planned corrective actions are responsive to the intent of our recommendations.

[1] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the FY 2017 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers (CIO) Council. In FY 2017, the seven IG FISMA Metric Domains were 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' *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0,* the 7 FISMA Metric Domains are: risk management, configuration management, identity and access management, security training, information security continuous monitoring, incident response, and contingency planning. The contractor systems metrics were consolidated into the risk management FISMA metric domain.

During our audit, we noted some bureaus and offices self-identified weaknesses in NIST Standard Publication 800-53, Revision 4, controls and documented them in 4 Plan of Actions and Milestones (POA&M). We reviewed each self-identified weakness and noted that each one had a corrective action plan documented within a POA&M, and therefore, did not provide any additional recommendations (see *Self-identified Weaknesses*).

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 26, 2017

BACKGROUND

Federal Information Security Modernization Act of 2014 (FISMA)

The Federal Information Security Modernization Act of 2014, commonly referred to as 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 Inspector Generals (IGs) in complying with requirements of FISMA. The act is supported by the Office of Management and Budget (OMB), 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.

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 Inspector General (IG) or an independent external auditor as determined by the IG.

FY 2017 Inspector General FISMA Reporting Metrics

For Fiscal Year (FY) 2017, the OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) implemented changes to the IG FISMA Reporting Metrics to organize them around the five information security functions outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. In addition, CIGIE implemented maturity models for the FY 2017 FISMA Metric Domains: Risk Management (RM), Configuration Management (CM), Identity and Access Management (IA), Security Training (ST), and Contingency Planning (CP), which are similar to the Information Security Continuous Monitoring (ISCM) and Incident Response (IR) maturity models that were instituted in FY 2015 and FY 2016, respectively. **Table 1** shows the alignment of Cybersecurity Framework to the FISMA Metric Domains.

Cybersecurity Framework Security Functions	FY 2017 IG FISMA Metric Domains
Identify	Risk Management[3]
Protect	Configuration Management Identity and Access Management Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Table 1: *Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FY 2017 IG FISMA Metric Domains*

In the past, the ISCM and IR models had maturity levels for people, process, and technology. In FY 2017, CIGIE eliminated specific people, process, and technology elements and, instead, issued specific questions. These models have five levels: ad-hoc, defined, consistently implemented, managed and measurable, and optimized. The introduction of a 5-level maturity model is a deviation from previous DHS guidance over the CyberScope questions. As such, a year-to-year comparison of FISMA compliance may not be feasible due to the fundamental change in how CyberScope is scored and evaluated.

Department of the Treasury Bureaus/Offices (Bureaus)

The Department of the Treasury (Treasury or Department) consists of 12 operating bureaus and offices, including:

1 **Alcohol and Tobacco Tax and Trade Bureau (TTB)** – Responsible for enforcing and administering laws covering the production, use, and distribution of alcohol and tobacco products. TTB also collects excise taxes for firearms and ammunition.

2 **Bureau of Engraving and Printing (BEP)** – Designs and manufactures United States paper currency, securities, and other official certificates and awards.

3 **Bureau of the Fiscal Service (Fiscal Service)** – Promotes the financial integrity and operational efficiency of the U.S. government through exceptional accounting, financing, collections, payments, and shared services.

4 **Community Development Financial Institutions (CDFI) Fund** – Created to expand the availability of credit, investment capital, and financial services in distressed urban and rural communities.

5 **Departmental Offices (DO) –** Primarily responsible for policy formulation. DO, while not a formal bureau, is composed of offices headed by Assistant Secretaries, some of whom report to Under Secretaries. These offices include Domestic Finance, Economic Policy, General Counsel, International Affairs, Legislative Affairs, Management, Public Affairs, Tax Policy, and Terrorism and 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.

6 **Financial Crimes Enforcement Network (FinCEN)** – Supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and

[3] FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics V.1.0, April 17, 2017. In 2017, Contractor Systems was included as part of the Risk Management FISMA metric domain.

international financial crimes. It also provides United States policy makers with strategic analyses of domestic and worldwide trends and patterns.

7 **Internal Revenue Service (IRS)** – Responsible for determining, assessing, and collecting internal revenue in the United States. (Not within the scope of this audit.)

8 **Office of the Comptroller of the Currency (OCC)** – Charters, regulates, and supervises national banks and thrift institutions to ensure a safe, sound, and competitive banking system that supports the citizens, communities, and economy of the United States.

9 **Office of Inspector General (OIG)** – Conducts and supervises audits and investigations of Treasury's programs and operations except for IRS which is under the jurisdictional oversight of the Treasury Inspector General for Tax Administration and the Troubled Asset Relief Program (TARP), which is under the jurisdictional oversight of SIGTARP. The OIG also keeps the Secretary and the Congress fully and currently informed about problems, abuses, and deficiencies in Treasury's programs and operations.

10 **United States Mint (Mint)** – Designs and manufactures domestic, bullion, and foreign coins as well as commemorative medals and other numismatic items. The Mint also distributes United States coins to the Federal Reserve banks as well as maintains physical custody and protection of our nation's silver and gold assets.

11 **SIGTARP** – Has the responsibility to conduct, supervise, and coordinate audits and investigations of the purchase, management, and sale of assets under the TARP. SIGTARP's goal is to promote economic stability by assiduously protecting the interests of those who fund the TARP programs (i.e., the American taxpayers).

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

For the FY 2017 FISMA Unclassified performance audit, we selected the following bureaus and offices for testing: BEP, DO, FinCEN, Fiscal Service, Mint, and TTB. 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 CDFI Fund, OCC, OIG, and TIGTA. As in prior years, IRS was evaluated by TIGTA. 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 2017 Questions for Inspectors General*.

Department of the Treasury Information Security Management Program

Treasury Office of the Chief Information Officer

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

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 (TCSIRC)** – Provides incident reporting with external reporting entities and conducts performance monitoring and analyses of the Computer Security Incident Response Center (CSIRC) within Treasury and each bureau's CSIRC.
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 Federal Information Security Modernization of 2014 (FISMA) requirements, Office of Management and Budget's policy and guidance, and the National Institute of Standards and Technology (NIST) standards and guidelines, the Department of the Treasury's (Treasury or Department) information security program and practices for its unclassified systems were established and have been maintained for the 5 Cybersecurity functions and 7 FISMA Metric Domains. The FISMA program areas are outlined in the *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0* and were prepared by the Department of Homeland's Office of Cybersecurity and Communications Federal Network Resilience. The 7 Metric Domains are Risk Management, Contractor Systems, Configuration Management, Identity and Access Management, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning.[4] However, while the security program has been implemented across the Treasury for its non-IRS bureaus, the program was not fully effective as reflected in 7 findings within 4 of the 7 FISMA Metric Domains.

We have made 32 recommendations that, if effectively addressed by management, should strengthen the respective bureau's, office's, and Treasury's information security programs. The *Findings* section of this report presents the detailed findings and associated recommendations. We noted 4 self-identified control weaknesses by 2 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 2017 independent evaluation.

Additionally, we evaluated the prior-year findings from the fiscal year (FY) 2016, FY 2015, and FY 2011 FISMA performance audits, as well as the FY 2014 and FY 2013 FISMA evaluations and noted that management had closed a total of 11 of 20 findings. We did not evaluate any FY 2012 FISMA findings as those findings were already closed. See Appendix II*, Status of Prior-Year Findings*, for additional details.

In a written response to this report, the Acting Deputy Assistant Secretary for Information Systems and Chief Information Officer agreed with our findings and recommendations (See *Management Response).*

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

FINDINGS

1. Information security policies, procedures, and security plans were either outdated or incomplete at the Bureau of Engraving and Printing (BEP) and the United Stated Mint (Mint).

The Treasury Directive Publication (TD P) 85-01, *Department of the Treasury Information Technology (IT) Security Program,* requires Department of the Treasury (Treasury or Department) bureaus to upload required artifacts into the “Treasury Federal Information Security Modernization Act of 2014 (FISMA) Inventory Management System” (TFIMS) as the documents are completed. Additionally, TD P 85-01 requires bureaus to develop security plans for the information system that is consistent with the organization’s enterprise structure and that is updated to address changes to the information system/environment of operation. Further, bureaus are required to review their information security policies and procedures on an annual basis and update as necessary to address risks and changes within their environment. This control falls under the Identify Cybersecurity domain and the Risk Management FISMA program area. We noted the following:

- For the selected system, BEP did not upload required documentation (e.g., Accreditation Letter and Security Test & Evaluation) to TFIMS as required by TD P 85-01. Management maintained information in the tool for all Treasury and Bureau Key Performance Indicators but did not upload these additional artifacts because of a misunderstanding of the Treasury policy requirements. By not uploading the required artifacts into TFIMS, the Treasury Office of the Chief Information Officer (OCIO) had no visibility into the security status of the system. The Department would not have timely access to the current Security Assessment & Authorization (SA&A) package that supports the current Authorization to Operate (ATO) and will be unaware if annual testing is occurring. Additionally, if BEP did not load required documentation into TFIMS, the OCIO would not be able to monitor the Department’s compliance with the NIST Risk Management Framework (RMF) and to assess the effectiveness of the Department’s overall information security program. (*See recommendation #1.*)

- Mint management did not update and approve the bureau-wide information security policies and procedures in accordance with TD P 85-01 and the NIST Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* Specifically, the following bureau-wide policies were outdated for several years: Risk Management Policy (last updated in March 2015), Security Control Implementation and Status Template (last updated in February 2015), Security Assessment Report Template (last updated in May 2014), and Bureau-wide Plan of Actions and Milestones (POA&M) Policy (last updated in February 2014). Mint management stated that the Information Security Division was understaffed based on the current project portfolio demands, which affected the updating policies and procedures in a timely manner. Due to limited resources, publishing of updated, necessary, bureau-wide policies and procedures was delayed. Bureau-wide information security polices provide guidance over controls implemented over the information system. Outdated documentation can lead to a misunderstanding of the information system control environment. This can lead to improper control implementation, thus causing a vulnerability to risks. *(See recommendations #2 & 3.)*

We recommend the Acting Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO) ensures that BEP management:

1. Implement a process or mechanism to ensure all required documentation (e.g., System Security Plan, Contingency Plan, and Risk Assessments) is uploaded into TFIMS based on the frequency stipulated in TD P 85-01.

   Management Response: BEP will validate all the required artifacts are transferred from the internal BEP system to TFIMS and establish periodic reviews to verify TFIMS artifacts remain updated. Target completion date: March 30, 2018.

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

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that Mint management:

2. Review and approve Mint-wide information security policies and procedures on an annual basis.

   Management Response: Mint will review, update, and post revised and approved information security policies and procedures on the agency Intranet website. Target completion date: May 31, 2018.

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

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, Rev 4.

   Management Response: Mint will conduct an annual review of all bureau information security policies and procedures for review and approval by Mint management for Mint-wide access and distribution. Target completion date: May 31, 2018.

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

2. Asset management processes were not fully implemented at the Bureau of the Fiscal Service (Fiscal Service).

Both NIST SP 800-53, Rev. 4, and the Fiscal Service Baseline Security Requirements (BLSR) direct bureaus to employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information systems. This control falls under the Identify Cybersecurity domain and the Risk Management FISMA program area. We noted the following:

- Fiscal Service had not fully implemented a Software Asset Management (SAM) tool to discover, identify, and measure the utilization of installed software on the Fiscal Service network and to manage software product signatures, analyze software use (i.e., license consumption), and serve as a source of SAM reporting. Due to the limitations of the Fiscal Service's current SAM tool, the tool was not capable of measuring utilization of all installed software on the Fiscal Service network. The current SAM tool was only capable of measuring the utilization of software licensed by a single vendor. The SAM tool not being fully deployed creates delays and inefficiencies in tracking software and associated licenses, and in detecting unauthorized software on the network. Additionally, reviewing the software assets for accuracy will be difficult without an enterprise-wide SAM tool. (*See recommendation #4.)*

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that that Fiscal Service management:

4. Implement an enterprise-wide SAM tool to discover and identify installed software on the Fiscal Service network, manage software product signatures, analyze software use (i.e., license consumption), and facilitate software asset management reporting.

   Management Response: Fiscal Service will implement and utilize an enterprise-wide SAM tool to perform software asset discovery, signature management, license usage analysis, and SAM program reporting. The enterprise-wide SAM tool will be implemented as part of the Continuous Diagnostics and Mitigation (CDM) Phase 1 project. Target completion date: June 30, 2019.

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

3. System inventory reviews were inconsistent at the Alcohol and Tobacco Tax and Trade Bureau (TTB).

NIST 800-53, Rev.4, the TTB Automated Information Systems (AIS) Security Program Policy, and the system security plan (SSP) for the selected TTB system require that TTB develop and maintain an inventory of all TTB general support systems, major applications, and minor applications and review and update the inventory on a quarterly basis to ensure that it is complete and accurate. This control falls under the Identify Cybersecurity Domain and the Risk Management FISMA program area. We noted the following:

- For the selected system, TTB management was only reviewing the TTB system inventories on an annual basis. TTB management had not fully developed plans to implement the quarterly reviews of system inventories. Lack of consistent system inventory reviews, according to TTB's policy and the SSP for the selected system, increases the risk that system inventories do not reflect the current system operating environment. Additionally, inconsistent system inventory reviews increases the risk of delays in the detection of unapproved assets in the operating environment. (*See recommendation #5.)*

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that TTB management:

5. Develop and implement plans to review system inventories quarterly as established by the bureau policy and the SSP for the selected system.

   Management Response: TTB re-evaluated the frequency with which it needs to review its system inventory. This frequency was changed from quarterly to annually. The SSP for the TTB selected system and the TTB AIS Policy, which address the system inventory reviews, were updated to indicate that annual reviews will be performed.

Completion date: September 30, 2017.

Auditor Comment: Management's reported corrective action meets the intent of the recommendation. .

4. Configuration compliance and vulnerability scanning were not consistently performed at BEP, Fiscal Service, Departmental Offices (DO), and TTB.

TD P 85-01 requires bureaus to scan for vulnerabilities in the information system and hosted applications every 30 days or (a shorter duration if specified by bureau policy) when new vulnerabilities potentially affecting the system/applications are identified and reported. In addition, TD P 85-01 directs bureaus to remediate legitimate vulnerabilities in accordance with an organizational assessment of risk. This control falls under the Protect Cybersecurity domain, and Configuration Management FISMA program area. We noted the following:

- BEP did not conduct recurring Security Content Automation Protocol (SCAP) compliance scans on its network in accordance with TD P 85-01 requirements. Technical challenges associated with a recent upgrade in its network scanning tool resulted in the temporary suspension of SCAP scanning from that tool. BEP continued the use of a NIST validated government-off-the-shelf (GOTS) Microsoft System Center Configuration Management (SCCM) tool to perform manual scans of representative systems. Not scanning the system for compliance with bureau-established configuration baselines could result in the system not being adequately configured. This may result in weaknesses that allow unauthorized access and/or bugs that jeopardize the confidentiality, integrity, and availability of the BEP environment and network. *(See recommendation #6.)*

- The Fiscal Service BLSR directs management to perform system and application vulnerability and configuration scans at least every two weeks. However, from May 18, 2017 through June 21, 2017, the vulnerability and configuration scans were not being performed for a selected Fiscal Service system. Furthermore, Fiscal Service management did not identify these missing scans as part of its review process. Fiscal Service management stated that the scanning and the associated reviews for the selected system were not conducted due to human error. Not scanning the system for vulnerabilities and deviations from baseline configurations could result in the system being inadequately patched. By not having scan results to review, management will not be able to remediate known flaws. This may result in weaknesses that allow unauthorized access and/or bugs that jeopardize the confidentiality, integrity, and availability of the selected system's environment and network. *(See recommendations #7 & 8.)*

- Although DO has documented risk assessment and system and information integrity security controls to address vulnerabilities in the *DO IT Security Policy Handbook* (DO P-910), version 3.3, 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) controls did not adequately define the time period for which security-related software patches and updates were to be implemented. Moreover, through inspection of the March and April 2017 vulnerability scan results for selected system 1 and selected system 2, we identified the following populations of vulnerabilities: 7 vulnerabilities in March and 9 vulnerabilities in April for system 1; 37 vulnerabilities in March and 39 vulnerabilities in

April for system 2. Furthermore, DO management had a process 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:

- System 1: 2 of 2 selected critical and high vulnerabilities that were identified during March and April also existed during the subsequent vulnerability scans, and no policy or program was in place to prioritize the timeframe to remediate these weaknesses.
- System 2: 3 of 5 selected critical and high vulnerabilities that were identified during March also existed during the April and May vulnerability scans, and no policy or program was in place to prioritize the timeframe to remediate these weaknesses.

DO management stated it uses a risk-based approach to remediating vulnerabilities; therefore, it only requires vulnerabilities to be remediated “as soon as reasonable.” Lack of a defined remediation timeframe does not allow management the ability to manage and monitor the remediation process to ensure vulnerabilities are being remediated timely, which increases the risk that high impact vulnerabilities are not remediated within the DO environment. Also, lack of consistent vulnerability prioritization and remediation increases the risk that management is unaware of the current security posture of the environment for known and unknown weaknesses, thereby increasing the likelihood of computing resources being compromised. *(See recommendation #9.)*

- Multiple instances of end-of-life software packages were installed on the TTB network. Specifically, seven installations of outdated Extensible Markup Language (XML) Parser[5] software were present on the July 2017 vulnerability scan. These software packages were deemed end-of-life by Microsoft in April of 2014. The vulnerability scanner provides a variety of information for each identified vulnerability including, but not limited to, plugin “ID”, description, first observed date, last observed date, patch publication date, and plugin release date. TTB’s process was to inspect the vulnerability report for open vulnerabilities based upon the vendor’s patch publication date; however, the report did not indicate instances end-of-life software packages. Since end-of-life software vulnerabilities did not align to vendor published patches, the vulnerability report did not alert management to remove the end-of-life software packages to install new versions. These vulnerabilities did not have vendor patch publication dates because the appropriate corrective action was to remove the end-of-life software packages. By having end-of-life software installed on the network, TTB will not be alerted to potential security and software flaws. The noted end-of-life software is considered a high risk as it is utilized in electronic communications. By not having the most up to date version, the TTB network is exposed to significant risks to data confidentially, availability, and integrity. *(See recommendations #10, 11, & 12.)*

[5] The XML standard is a flexible way to create information formats and share structured data through the Internet, as well as through organizations’ networks. An XML parser is a piece of XML program that takes a physical representation of some data and converts it into an in-memory form for the program as a whole to use. Many web applications that accept and respond to XML requests are vulnerable to XML External Entity (XXE) attacks due to default XML parser settings. This vulnerability can be exploited to read arbitrary files from the server, including sensitive files, such as the application configuration files.

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures 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; and
   - remediate configuration deviations noted during SCAP scanning within a timely manner.

   Management Response: BEP will establish periodic reviews to validate SCAP scanning and that deviation remediations are being executed in accordance with policy. The target completion date: April 27, 2018.

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

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that Fiscal Service management:

7. Complete vulnerability scans over the selected system according to the frequency established by the BLSR.

   Management Response: Fiscal Service will develop and implement a process to ensure scans are completed to the frequency established by the BLSR. This includes reconfiguring the scanning tool to ensure all routine scans are able to start and complete within the timeframe allowed by adjusting the black-out window to avoid interruption. Target completion date: January 31, 2018.

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

8. Develop a process to ensure that all selected vulnerability scans are successfully completed and reviewed.

   Management Response: Fiscal Service will develop a process to ensure that scans are successfully completed and reviewed by analyzing the scan logs to identify, investigate and remediate failed or partial scans. Target completion date: January 31, 2018.

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

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that DO Management:

9. Update the *DO IT Security Policy Handbook* (DO P-910), Version 3.3, specifically the RA (Risk Assessment)-5 and SI (System and Information Integrity)-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.

   Management Response: DO will develop a Continuous Monitoring Program as recommended. Target completion date: May 31, 2018.

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

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that TTB Management:

10. Establish a current enterprise baseline of software and related configurations.

    Management Response: TTB ensured that it has an updated and complete list of enterprise approved software. This list will be used going forward to identify all instances of unsupported and unapproved software. Completion date: September 30, 2017.

    Auditor Comment: Management's reported corrective action meets the intent of the recommendation.

11. Establish a process to review and revise enterprise software baselines to maintain TTB's risk posture.

    Management Response: TTB began reviewing the list of enterprise approved software on a monthly basis to identify all instances of unsupported and unapproved software. Completion date: September 30, 2017.

    Auditor Comment: Management's reported corrective action meets the intent of the recommendation.

12. Update systems to be compliant with enterprise baselines resulting from the enterprise software baseline review.

    Management Response: Based on the enterprise approved software review, TTB identified instances of unsupported or unapproved software will be removed. Additionally, TTB ensured that its base operating system images were updated with recent patches to limit the number of new, old vulnerabilities being introduced into the environment. Completion date: September 30, 2017.

    Auditor Comment: Management's reported corrective action meets the intent of the recommendation.

5. Missing or inconsistent patch management practices existed at BEP, DO, and TTB.

TD P 85-01 requires Treasury bureaus to identify, report, and correct information systems flaws; to test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; to install security-related software and firmware updates within a bureau-defined period of release of the updates; and to incorporate flaw remediation into the organizational configuration management process. Additionally, TD P 85-01 directs the bureaus to review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analysis; to document configuration change decisions associated with the information system; and to implement approved configuration-controlled changes to the information system. This control falls under the Protect Cybersecurity domain and the Configuration Management FISMA program area. We noted the following:

- BEP did not install critical patches to the Local Area Network (LAN)/Wide Area Network (WAN) in a timely manner or have an associated 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 for associated security patches to be installed or to have an associated POA&M in place. BEP pushes patches to the LAN/WAN via SCCM. Due to the need to restart certain devices (e.g., servers and switches) as part of the patching process, updates can only take place on certain hardware during scheduled outages. There are instances where these scheduled downtimes are postponed due to user requirements. The BEP operations team utilizes the results of the vulnerability scans to assist in tracking instances where patches have not been applied to specific hardware and works to resolve the issue. In addition, due to development of virtual machines being turned on and off at a rapid pace, BEP's network scanning tool has trouble tracking the status of these systems, which creates confusion on the date a vulnerability is first observed. Not installing patches in a timely manner exposes the system to increased risk of compromise and errors. This may allow unauthorized access and/or bugs that jeopardize the confidentiality, integrity, and availability of the BEP environment and network. *(See recommendations #13, 14, & 15.)*

- Although DO has documented its patch management process in its *IT Security Policy Handbook* (DO P-910), Version 3.3, 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 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 selected patches for the operating systems supporting selected systems 1 and 2. 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 selected operating system patches

  According to DO management, the test environment is not a complete representation of the production environment supporting selected systems 1 and 2. Thus, the possibility exists that not all operating system patches are tested prior to implementation. Further, due to competing priorities and resource constraints, management has not emphasized the approval process for patches prior to installation. The lack of testing and approving operating system component patches increases the risk of an adverse effect on the system and could impact the availability of the system. *(See recommendations #16 & 17.)*

- Although TTB has documented its patch management process in the *TTB Configuration Management Handbook* (TTB H 7260.1C), management did not consistently approve operating system security patches prior to installation. Specifically, management did not approve 2 of 5 operating system patches until after the FISMA testing period as follows:

  - For the patch installed in July 2016, TTB management approved it on August 17, 2016.

- For the patch installed in February 2017, TTB management approved it on July 27, 2017

Due to lack of training, the individual who installed the patches did not properly follow the required change request process. Further, due to lack of oversight and competing priorities, management did not identify the missing change approval. An inconsistent patch management process and the lack of testing increases the risk to the current security posture of the information system and of unauthorized changes being implemented into the production environment. This increases this risk of adverse effects on the system and on the integrity of system data. *(See recommendations #18 & 19.)*

- 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 Standard Operating Procedures (SOP). We noted that on the June 2017 vulnerability scan report, these 7 vulnerabilities had been open for more than 30 days. A Plan of Action and Milestones (POA&M) was created for only 1 out of 7 of these vulnerabilities. The June vulnerabilities that were not addressed by a POA&M all relate to one vulnerability plugin. This plugin was not included as a POA&M because the patch publication date for it was listed as “not applicable” by the TTB vulnerability scanner and did not have a date associated with it. The reason it was listed as “not applicable” was because this particular vulnerability is not a patch, but rather a detection for if the vulnerable file exists on the file system or not. The same situation applies to the vulnerability noted in July. TTB will change its process in September 2017, to use the plugin publication date since there is always a date associated with a plugin. Not installing patches and updating software in a timely manner exposes the system to increased risk of compromise and errors. This may allow unauthorized access and/or bugs that jeopardize the confidentiality, integrity, and availability of the TTB environment and network. *(See recommendations #20, 21, & 22.)*

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures 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.

    Management Response: BEP will establish periodic reviews to validate existing procedures are consistently followed when investigating the small percentage of systems that failed the initial patch deployment. Target complete date: May 31, 2018.

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

14. Develop and implement procedures to apply patches in a timely manner for hardware with uptime requirements.

    Management Response: During the next scheduled process review, BEP will determine if there are any process improvement opportunities to streamline the process. Target completion date: May 31, 2018.

    Auditor Comment: Management’s response meets the intent of our recommendation so long as the indicated action addresses applying patches in a timely manner with uptime requirements.

15. Develop and implement procedures to ensure temporary virtual machines are patched.

    Management Response: During the next scheduled process review, BEP will determine if there are any process improvement opportunities to streamline the process. Target completion date: May 31, 2018.

    Auditor Comment: Management's response meets the intent of our recommendation so long as the indicated action addresses applying patches to virtual machines.

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that DO management:

16. Update the *IT Security Policy Handbook* (DO P-910) and supporting patch management policies and procedures to enforce a patch management process for the operating systems supporting selected system 1, selected system 2, and other moderate or high risk information systems to test, document, and approve patches prior to installation.

    Management Response: The DO Cybersecurity office will discuss within OCIO and other DO offices to determine the best path forward for patch management policies, procedures, and implementation. DO will update patch management policies and procedures accordingly. Target completion date: May 31, 2018.

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

17. Perform and document a cost benefit analysis to determine if a complete test environment is warranted for all DO systems to include tracking of all patch management decisions.

    Management Response: DO will perform the cost benefit analysis. Target completion date: May 31, 2018.

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

18. Test patches in adherence to the updates to IT Security Handbook and supporting patch management policies and procedures.

    Management Response: DO will test patches in accordance with updates to DO-910 and supporting patch management policies/procedures. Target Completion date: May 31, 2018.

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

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that TTB management:

19. Ensure individuals who install patches are properly trained to follow the required configuration and patch management processes.

    Management Response: TTB ensured that individuals who install patches were properly trained to follow the required configuration and patch management processes. Completion date: September 30, 2017.

    Auditor Comment: Management's the reported corrective action meets the intent of the recommendation.

20. Approve security patches prior to installing them on the operating system.

    Management Response: Going forward, monthly Request for Changes (RFCs) will be submitted for the applicable month's patches using the current RFC approval process. Completion date: September 30, 2017.

    Auditor Comment: Management's reported corrective actions meets the intent of our recommendation.

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.

    Management Response: TTB will review and update its patch management reporting process to ensure all of its vulnerabilities are properly identified and accounted. The identified vulnerabilities will then be remediated or a POA&M will be created with an associated timeline for completion. Target completion date: November 30, 2017.

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

22. Establish review processes to ensure that all vulnerabilities, regardless of patch publication, are following the bureau process.

    Management Response: TTB modified the process used to identify and review vulnerabilities from using the patch publication date to plugin publication date to ensure that all vulnerabilities will be accounted for and tracked. Completion date: September 30, 2017.

    Auditor Comment: Management's reported corrective actions meets the intent of our recommendation.

6. Account management activities were not compliant with System Security Policies (SSPs) at Mint, Financial Crimes Enforcement Network (FinCEN), TTB, and BEP.

NIST SP 800-53, Rev.4, and TD P 85-01 require Treasury bureaus and offices to create, enable, modify, disable, and remove information system accounts in accordance with organization-defined procedures or conditions. Additionally, NIST SP 800-53, Rev. 4, requires that bureaus develop, document, and disseminate access control and personnel security policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. In addition, bureaus should review and update their access control policies, as well as the procedures to facilitate the implementation of the personnel security policies and controls. Moreover, this control falls under the Protect Cybersecurity domain and the Identity and Access Management FISMA program area. We noted the following:

- Mint did not perform the annual user account review and recertification for the selected system in accordance with its SSP and NIST SP 800-53, Rev. 4 guidance. Mint management did not ensure the performance of periodic user access review in accordance with NIST 800-53, Rev.4, for the selected system, which is hosted and maintain by a cloud service provider (CSP). Not performing periodic user access reviews and validation of user access for the selected system increases the risk of unauthorized access, disclosure, and modification of production data. (*See recommendations #23 & 24)*

- One of 45 new Mint users did not complete the Rules of Behavior and Access Agreement forms as required by TD P 85-01. Due to lack of management oversight, management did not obtain these completed forms. Failure to complete Rules of Behavior and Access Agreement forms in a timely manner for each user granted access to the system increases the risk of users performing actions that may cause data corruption and/or loss due to a lack of understanding of the system. *(See recommendation #25)*

- For the selected system, FinCEN did not perform the annual periodic account access review and the semiannual privileged user account access review as required by its SSP and TD P 85-01. FinCEN relied on the main network account review process to fulfill the review of all systems. To gain access to any resources (privileged and unprivileged), all FinCEN users had to logon on to the network using their Personal Identity Verification (PIV) cards. Once their accounts are disabled at the network level, these users cannot log onto any other system. Not performing a periodic access review for users' system accounts and associated rights and roles increases the risk of unauthorized accounts and access in the selected system. Additionally, not performing a periodic access review for users' system accounts increases the risk of unmonitored user accounts being used for malicious activities. *(See recommendation #26.)*

- For the selected TTB system, its SSP requires semi-annual reviews for privileged users. However, none of the 15 selected TTB privileged users had records of completing the semi-annual reviews for the selected system. TTB management had not implemented procedures to ensure semi-annual reviews were appropriately conducted. Lack of a consistent review process for privileged user accounts increases the risk of unauthorized accounts and unauthorized access to the selected system. Additionally, an inconsistent account review process increases the risk of unmonitored user accounts being used for malicious activities. *(See recommendation #27.)*

- For the selected system, BEP management did not retain the Nondisclosure Agreements (NDA), Acceptable Use Agreements, and Rules of Behavior forms and require training documentation for 1 of 5 new users. Due to lack of training, the individual who on-boarded these new users did not properly file the required account management documentation. Without properly retaining the required account management documentation, the Chief Information Security Officer (CISO) cannot ensure that the selected system users are properly aware of the system or application rules, their responsibilities, and their expected behavior. *(See recommendation #28.)*

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that Mint management:

23. Develop and implement a process to ensure that periodic user access reviews are completed for the selected system.

    Management Response: The Mint will develop policies and procedures for completion of quarterly user access reviews for the selected system. Target completion date: March 31, 2018.

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

24. Ensure all active selected system accounts are consistently reviewed in accordance with NIST 800-53, Rev. 4.

    Management Response: The Mint will develop policies and procedures for completion of quarterly user access reviews for the selected system. Target completion date: March 31, 2018.

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

25. Establish a process to ensure that all users are consistently completing a Rules of Behavior and Access Agreement form within a timely manner, and a process to revoke or disable accounts when a Rules of Behavior and an Access Agreement has not been completed.

    Management Response: Mint will conduct quarterly reviews for completion of Cyber Security Training that includes Rules of Behavior and conduct quarterly network account reviews. Target completion date: January 31, 2018.

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

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that FinCEN management:

26. Perform a periodic review of all active system user and privileged accounts and associated rights and privileges in accordance with its SSP and TD P 85-01.

    Management Response: FinCEN will ensure that all accounts for the selected FinCEN system are reviewed in accordance to FinCEN policy and NIST guidance. Target completion date: May 31, 2018.

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

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that TTB management:

27. For the selected system, develop and implement its semi-annual user access review for privileged infrastructure users that support the application.

    Management Response: A semi-annual review of the selected accounts that have the permission to grant access to Treasury accounts has been implemented going forward. Two (2) new scripts have been developed:

    1. An “Inactive [selected] Accounts” script has been developed to run monthly to disable any selected account that has not been logged into in 60 days.
    2. A “List [selected] Accounts” script has been developed to run semi-annually in September and March. It will generate a list of all selected accounts for review.

    The Information System Security Officer (ISSO) reviews and validates all active accounts. The results of the review are stored in SharePoint. Target completion date: September 30, 2017.

    Auditor Comment: Management’s reported corrective actions meets the intent of our recommendation.

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that BEP management:

28. For the selected system, ensure that new users complete the NDAs, Acceptable Use Agreements, Rules of Behavior, and required training documentation.

    Management Response: BEP will update existing account activation process to incorporate a flagging mechanism to support validation of required documentation prior to account activation. Target completion date: March 30, 2018.

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

7. Contingency planning activities were not compliant with policies at BEP and Mint

TD P 85-01 and NIST SP 800-34 provides directions to bureaus and offices to complete Business Impact Analyses (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 from configuration-controlled and integrity-protected information representing a known, operational state for the components. This control falls under the Recover Cybersecurity domain and the Contingency Planning FISMA program area. We noted the following:

- For the selected system, Mint did not conduct and document a BIA as part of the process of developing an Information System Contingency Plan (ISCP) in accordance with NIST SP 800-34. Mint management relied on the CSP to perform necessary contingency planning activities and did not ensure that the CSP conducted a BIA. By not conducting and continually reviewing a formal BIA, the recovery objectives and business impacts of an outage could misalign with the Mint environment. During a disaster, an extended outage has the potential for unintended ripple effects throughout the organization. *(See recommendations #29 & 30.)*

- BEP did not conduct and document a BIA for the selected system as part of the process of developing an ISCP in accordance with NIST SP 800-34. According to BEP management, while developing the contingency plan for the selected system, the work items used during the analysis phase were not captured and retained as the BIA artifact for the system. By not conducting and continually reviewing a formal BIA, the recovery objectives and business impacts of an outage could misalign with the BEP environment. During a disaster, an extended outage has the potential for unintended ripple effects throughout the organization. *(See recommendation #31 & 32.)*

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that Mint management:

29. For the selected system, ensure that the CSP conducts and documents a BIA prior to the next major ISCP update.

    Management Response: The Mint will coordinate the completion of a BIA with the CSP for the selected system during the next security re-authorization for the selected system. Target completion date: May 31, 2018.

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

30. For the selected system, complete BIAs per TD P 85-01 and NIST 800-34, as part of its contingency planning process.

    Management Response: The Mint will complete agency BIAs per TD P 85-01 and NIST 800-53 Rev.4 guidance. Target completion date: May 31, 2018.

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

We recommend the Acting Deputy Assistant Secretary for Information Systems and CIO ensures that BEP management:

31. For the selected system, conduct and document a BIA prior to the next major ISCP update.

    Management Response: BEP will update existing COOP documentation for the BEP selected system that is already tested and reviewed biannually to capture analysis work items as the for the selected BIA. Target completion date: January 31, 2018.

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

32. For the selected system, implement a process to ensure that BIAs are completed per TD P 85-01 and NIST 800-53 Rev. 4.

    Management Response: BEP will incorporate a review process prior to the major ISCP update to ensure BIA and other artifacts are documented and exist. Target completion date: March 30, 2018.

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

SELF-IDENTIFIED WEAKNESSES

During the Fiscal Year (FY) 2017 Department of the Treasury (Treasury or Department) Federal Information Security Modernization Act of 2014 (FISMA) performance audit, we noted some bureaus and offices had self-identified weaknesses. Specifically, we noted 4 Departmental Offices' (DO) systems, 7 Bureau of the Fiscal Services' (Fiscal Service) systems and 1 Alcohol and Tobacco Tax and Trade Bureau (TTB) system had in aggregate 12 NIST SP 800-53, Rev. 4, controls that had weaknesses that were self-identified. These self-identified weaknesses were associated with 14 open Plan of Action and Milestones (POA&M) and 4 POA&Ms that were closed from April – June 2017. We reviewed each self-identified weakness and noted that each weaknesses had a corrective action plan documented within a POA&M, and therefore, did not provide any additional recommendations.

FY17 FISMA Self-Identified Weaknesses – Department of the Treasury

Bureau	System	NIST SP 800 53 Control	Weakness
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
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 **<u>Note:</u>** 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.
	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
	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
	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

Bureau	System	NIST SP 800 53 Control	Weakness
	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
	Enterprise Common Control for Fiscal Service System #1, 2, and 3	CA-3	POA&M #10902 All ISAs were note updated annually
	Fiscal Service #2	CA-2	POA&M #11715 Unknown if security assessments performed on control enterprise infrastructure control
	Fiscal Service #2	AC-6	POA&M #16055 Least functionality
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.

MANAGEMENT RESPONSE TO THE REPORT

The following is the Acting Deputy Assistant Secretary for Information Systems and Chief Information Officer's response, dated October 17, 2017, to the Fiscal Year (FY) 2017 Federal Information Security Modernization Act of 2014 (FISMA) Performance Audit Report.

DEPARTMENT OF THE
TREASURY
WASHINGTON, D.C.
20220

October 17, 2017

MEMORANDUM FOR LARISSA KLIMPEL
DIRECTOR, INFORMATION TECHNOLOGY AUDIT

FROM: Eric Olson /s/
Acting 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
2017 Performance Audit"

Thank you for the opportunity to comment on the draft report entitled, *Fiscal Year 2017 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 acknowledge recent changes to the five-level maturity model deviates from previous guidance in how performance audits are scored and evaluated. Incorporating these changes, we still noted a moderate improvement in the overall results of this year's performance audit.

The Department remains committed to improving its security program. We have made notable progress over the past year and have accomplished a number of achievements, to include:

- Implemented Einstein 3Acclerated requirements at applicable Trusted Internet Connections and achieved compliance with December 2016 Congressional mandate.

- Improved Incident Response by expanding the Departmental Incident Response plan to incorporate new incident handling, breach handling, and recovery planning requirements. Increased functional efficiency of GSOC reporting portal to meet new US-CERT requirements. Launched a program of Department-wide cyber exercises with all bureaus to improve Treasury's Incident Response program.

- The Department implemented SANS Institute's "Securing the Human" training courseware as the standard for Annual Cybersecurity Awareness Training. This new courseware is available to Treasury users (Federal and Non-Federal) with reported completion reports at 99.96% during FY17 Q3.

- Upgrade to Splunk Architecture provides improved logging capabilities and advanced behavior analytic capabilities.

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

Attachment

cc: Kody Kinsley, 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: Information security policies, procedures, and security plans were either outdated or incomplete at the Bureau of Engraving and Printing (BEP) and the United Stated Mint (Mint).

KPMG Recommendation 1: We recommend BEP management: For the selected system, implement a process or mechanism to ensure all required documentation (e.g., System Security Plan, Contingency Plan, and Risk Assessments) is uploaded into TFIMS based on the frequency stipulated in TD P 85-01.

Treasury's Response: Validate all the required artifacts are transferred from the internal BEP system to TFIMS and establish periodic reviews to verify TFIMS artifacts remain updated. Target completion date: March 30, 2018.

Responsible Official: BEP, Chief Information Security Officer

KPMG Recommendation 2: We recommend Mint management: For the selected system, review and approve Mint-wide information security policies and procedures on an annual basis.

Treasury's Response: United States Mint will review, update, and post revised and approved information security policies and procedures on agency Intranet website. Target completion date: May 31, 2018.

Responsible Official: Mint, Acting Chief Information Security Officer.

KPMG Recommendation 3: 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: United States Mint will conduct annual review of all bureau 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, 2018.

Responsible Official: Mint, Acting Chief Information Security Officer.

KPMG Finding 2: Asset management processes not fully implemented at the Bureau of the Fiscal Service (FS).

KPMG Recommendation 4: We recommend Fiscal Service (FS) management: For the selected system, implement an enterprise-wide SAM tool to discover and identify installed software on the Fiscal Service network, manage software product signatures, analyze software use (i.e., license consumption), and facilitate software asset management reporting.

> **Treasury's Response:** Fiscal Service will implement and utilize an enterprise-wide SAM tool to perform software asset discovery, signature management, license usage analysis, and SAM program reporting. The enterprise-wide SAM tool will be implemented as part of the Continuous Diagnostics and Mitigation (CDM) Phase 1 project. Target completion date: June 30, 2019.
>
> **Responsible Official:** FS, Chief Information Security Officer

KPMG Finding 3: System inventory reviews were inconsistent at the Alcohol and Tobacco Tax and Trade Bureau (TTB).

KPMG Recommendation 5: We recommend TTB management: For the selected system: develop and implement plans to review system inventories quarterly as established by the bureau policy and the SSP for the selected system.

> **Treasury's Response:** TTB has re-evaluated the frequency with which it needs to review its system inventory. This is being changed from quarterly to annually. The System Security Plan (SSP) and the TTB Automated Information System (AIS) Policy, which address the system inventory reviews, have been updated to indicate that annual reviews will be performed. Completion date: September 30, 2017.
>
> **Responsible Official:** TTB, Chief Information Security Officer

KPMG Finding 4: Configuration compliance and vulnerability scanning were not consistently performed at BEP, Fiscal Service, Departmental Offices (DO), and TTB.

KPMG Recommendation 6: We recommend BEP management: For the selected system, 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; and
- Remediate configuration deviations noted during SCAP scanning within a timely manner.

> **Treasury's Response:** Establish periodic reviews to validate SCAP scanning and deviations remediation are being executed in accordance with policy. The target completion date: April 27, 2018.
>
> **Responsible Official:** BEP, Chief Information Security Officer

KPMG Recommendation 7: We recommend Fiscal Service management: For the selected system, complete vulnerability scans over the selected system according to the frequency established by the BLSR.

> **Treasury's Response:** Fiscal Service will develop and implement a process to ensure scans are completed to the frequency established by the BLSR. This includes reconfiguring the scanning tool to ensure all routine scans are able to start and complete

within the timeframe allowed by adjusting the black-out window to avoid interruption. Target completion date: January 31, 2018.

Responsible Official: FS, Chief Information Security Officer

KPMG Recommendation 8: We recommend Fiscal Service management: For the selected system, develop a process to ensure that all selected vulnerability scans are successfully completed and reviewed.

Treasury's Response: Fiscal Service will develop a process to ensure that scans are successfully completed and reviewed by analyzing the scan logs to identify, investigate and remediate failed or partial scans. Target completion date: January 31, 2018.

Responsible Official: FS, Chief Information Security Officer

KPMG Recommendation 9: We recommend DO management: For the selected system, update the *DO IT Security Policy Handbook* (DO P-910), Version 3.3, specifically the RA (Risk Assessment)-5 and SI (System and Information Integrity)-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.

Treasury's Response: DO will develop a Continuous Monitoring Program as recommended. Target completion date: May 31, 2018.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 10: We recommend TTB management: For the selected system, establish a current enterprise baseline of software and related configurations.

Treasury's Response: TTB will ensure that it has an updated and complete list of enterprise approved software. This list will be used to identify all instances of unsupported and unapproved software. Completion date: September 30, 2017.

Responsible Official: TTB, Chief Information Security Officer

KPMG Recommendation 11: We recommend TTB management: For the selected system, establish a process to review and revise enterprise software baselines to maintain TTB's risk posture.

Treasury's Response: The list of enterprise approved software will be reviewed on a monthly basis to identify all instances of unsupported and unapproved software. Completion date: September 30, 2017.

Responsible Official: TTB, Chief Information Security Officer

KPMG Recommendation 12: We recommend TTB management: For the selected system, update systems to be compliant with enterprise baselines resulting from the enterprise software baseline review.

> **Treasury's Response:** Based on the enterprise approved software review, identified instances of unsupported or unapproved software will be removed. Additionally, TTB will ensure that its base operating system images are updated with recent patches to limit the number of new, old vulnerabilities being introduced into the environment. Completion date: September 30, 2017.
>
> **Responsible Official:** TTB, Chief Information Security Officer

KPMG Finding 5: Missing or inconstant patch management practices existed at BEP, DO, and TTB.

KPMG Recommendation 13: We recommend BEP management: For the selected system, 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.

> **Treasury's Response:** Establish periodic reviews to validate existing procedures are consistently followed when investigating the small percentage of systems that failed the initial patch deployment. Target complete date: May 31, 2018.
>
> **Responsible Official:** BEP, Chief Information Security Officer

KPMG Recommendation 14: We recommend BEP management: For the selected system, develop and implement procedures to apply patches in a timely manner for hardware with uptime requirements.

> **Treasury's Response:** During the next scheduled process review, determine if there are any process improvement opportunities to streamline the process. Target completion date: May 31, 2018.
>
> **Responsible Official:** BEP, Chief Information Security Officer

KPMG Recommendation 15: We recommend BEP management: For the selected system, develop and implement procedures to ensure temporary virtual machines are patched.

> **Treasury's Response:** During the next scheduled process review, determine if there are any process improvement opportunities to streamline the process. Target completion date: May 31, 2018.
>
> **Responsible Official:** BEP, Chief Information Security Officer

KPMG Recommendation 16: We recommend DO management: For the selected system, update the *IT Security Policy Handbook* (DO P-910) and supporting patch management policies and procedures to enforce a patch management process for the operating systems supporting selected system 1, selected system 2, and other moderate or high risk information systems to test, document, and approve patches prior to installation.

> **Treasury's Response:** The DO Cybersecurity office will discuss within OCIO and other DO offices to determine the best path forward for patch management policies, procedures, and implementation. DO will update patch management policies and procedures accordingly. Target completion date: May 31, 2018.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Recommendation 17: We recommend DO management: For the selected system, perform and document a cost benefit analysis to determine if a complete test environment is warranted for all DO systems to include tracking of all patch management decisions.

> **Treasury's Response:** DO will perform the cost benefit analysis. Target completion date: May 31, 2018.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Recommendation 18: We recommend DO management: For the selected system, test patches in adherence to the updates to IT Security Handbook and supporting patch management policies and procedures.

> **Treasury's Response:** DO will test patches in accordance with updates to DO-910 and supporting patch management policies/procedures. Target Completion date: May 31, 2018.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Recommendation 19: We recommend TTB management: For the selected system, ensure individuals who install patches are properly trained to follow the required configuration and patch management processes.

> **Treasury's Response:** Ensure individuals who install patches are properly trained to follow the required configuration and patch management processes. Completion date: September 30, 2017.
>
> **Responsible Official:** TTB, Chief Information Security Officer

KPMG Recommendation 20: We recommend TTB management: For the selected system, approve security patches prior installing them on the operating system.

> **Treasury's Response:** Monthly RFC's will be submitted for the applicable month's patches using the current RFC approval process. Completion date: September 30, 2017.

> **Responsible Official:** TTB, Chief Information Security Officer

KPMG Recommendation 21: We recommend TTB management: For the selected system, 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.

> **Treasury's Response:** TTB will review and update its patch management reporting process to ensure all of its vulnerabilities are properly identified and accounted. The identified vulnerabilities will then be remediated or a POA&M will be created with an associated timeline for completion. Target completion date: November 30, 2017.
>
> **Responsible Official:** TTB, Chief Information Security Officer

KPMG Recommendation 22: We recommend TTB management: For the selected system, establish review processes to ensure that all vulnerabilities, regardless of patch publication, are following the bureau process.

> **Treasury's Response:** TTB will modify the process used to identify and review vulnerabilities from using the patch publication date to plugin publication date to ensure all that vulnerabilities are accounted for and tracked. Completion date: September 30, 2017.
>
> **Responsible Official:** TTB, Chief Information Security Officer

KPMG Finding 6: Account management activities were not compliant with System Security Policies (SSPs) at Mint, Financial Crimes Enforcement Network (FinCEN), TTB, and BEP.

KPMG Recommendation 23: We recommend Mint management: For the selected system, develop and implement a process to ensure that periodic user access reviews are completed for the selected system.

> **Treasury's Response:** The United States Mint will develop policies and procedures for completion of quarterly user access reviews for the selected system. Target completion date: March 31, 2018.
>
> **Responsible Official:** Mint**,** Acting Chief Information Security Officer

KPMG Recommendation 24: We recommend Mint management: For the selected system, ensure all active selected system accounts are consistently reviewed in accordance with NIST 800-53, Rev. 4.

> **Treasury's Response:** The United States Mint will develop policies and procedures for completion of quarterly user access reviews for the selected system. Target completion date: March 31, 2018.

Responsible Official: Mint**,** Acting Chief Information Security Officer

KPMG Recommendation 25: We recommend Mint management: For the selected system, establish a process to ensure that all users are consistently completing a Rules of Behavior and Access Agreement form within a timely manner, and a process to revoke or disable accounts when a Rules of Behavior and an Access Agreement has not been completed.

Treasury's Response: United States Mint will conduct quarterly reviews for completion of Cyber Security Training that includes Rules of Behavior and conduct quarterly network account reviews. Target completion date: January 31, 2018.

Responsible Official: Mint**,** Acting Chief Information Security Officer

KPMG Recommendation 26: We recommend FinCEN management: For the selected system, perform a periodic review of all active system user and privileged accounts and associated rights and privileges in accordance with its SSP and TD P 85-01.

Treasury's Response: FinCEN concurs, FinCEN will ensure that all BSA E-Filing system accounts are reviewed in accordance to FinCEN policy and NIST guidance. Target completion date: May 31, 2018.

Responsible Official: FinCEN, Chief Information Security Officer

KPMG Recommendation 27: We recommend TTB management: For the selected system, develop and implement its semi-annual user access review for privileged infrastructure users that support the application.

Treasury's Response: A semi-annual review of the selected accounts that have the permission to grant access to DOT accounts will be implemented going forward. Two (2) new scripts have been developed:

1. An "Inactive [selected] Accounts" script has been developed to run monthly to disable any selected account that has not been logged into in 60 days.
2. A "List [selected] Accounts" script has been developed to run semi-annually in September and March. It will generate a list of all selected accounts for review.

The ISSO will review and validate all active accounts. The results of the review will be stored in SharePoint. Target completion date: September 30, 2017.

Responsible Official: TTB, Chief Information Security Officer

KPMG Recommendation 28: We recommend BEP management: For the selected system, ensure that new users complete the NDAs, Acceptable Use Agreements, Rules of Behavior, and required training documentation.

Treasury's Response: Update existing account activation process to incorporate a flagging mechanism to support validation of required documentation prior to account activation. Target completion date: March 30, 2018.

Responsible Official: BEP, Chief Information Security Officer

KPMG Finding 7: Contingency planning activities were not compliant with policies at BEP and Mint.

KPMG Recommendation 29: We recommend Mint management: For the selected system, ensure that the CSP conducts and documents a BIA prior to the next major ISCP update.

Treasury's Response: United States Mint will coordinate the completion of a BIA with the CSP for the selected system during the next security re-authorization for the selected system. Target completion date: May 31, 2018.

Responsible Official: Mint**,** Acting Chief Information Security Officer

KPMG Recommendation 30: We recommend Mint management: For the selected system, complete BIAs per TD P 85-01 and NIST 800-34, as part of its contingency planning process.

Treasury's Response: United States Mint will complete agency BIAs per TD P 85-01 and NIST 800-53 Rev.4 guidance. Target completion date: May 31, 2018.

Responsible Official: Mint**,** Acting Chief Information Security Officer

KPMG Recommendation 31: We recommend BEP management: For the selected system, conduct and document a BIA prior to the next major ISCP update.

Treasury's Response: Update existing DMM COOP documentation that is already tested and reviewed biannually to capture analysis work items as the DMM BIA. Target completion date: January 31, 2018.

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

KPMG Recommendation 32: We recommend BEP management: For the selected system, implement a process to ensure that BIAs are completed per TD P 85-01 and NIST 800-53 Rev. 4.

Treasury's Response: Incorporate a review process prior to the major ISCP update to ensure BIA and other artifacts are documented and exist. Target completion date: March 30, 2018.

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

APPENDIX I – OBJECTIVES, SCOPE, AND METHODOLOGY

The objective for this performance audit was to assess the effectiveness of the Department of the Treasury's (Treasury or Department) information security program and practices for its unclassified systems (with exception to the Internal Revenue Service (IRS) systems) for the period July 1, 2016 through June 30, 2017. 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 *DHS' FISMA 2017 Questions for Inspectors General,* dated April 17, 2017, and assessed the maturity levels on behalf of the Treasury Office of Inspector General. Finally, we followed up on the status of prior-year Federal Information Security Modernization Act of 2014 (FISMA) findings.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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. We also followed the American Institute of Certified Public Accountants (AICPA) standards applicable to performance audits.

To accomplish our audit objective, we evaluated security controls in accordance with applicable legislation; the DHS *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0,* dated April 17, 2017; 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 Department 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 7 FISMA Metric Domains from the FY 2017 FISMA Reporting Metrics for IGs:

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 7 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 7 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 (optimal) test procedures for the Department, in-scope Bureau, and in-scope system (where applicable) for the maturity level 5 questions within the 7 FISMA Metric Domains. The test procedures evaluated the design of the controls.

We performed our fieldwork from June 1, 2017 to July 31, 2017 at Treasury's headquarters offices in Washington, D.C., and bureau locations and data centers in Washington, D.C.; Hyattsville, Maryland; and Vienna, Virginia. During our audit, we met with Treasury management to discuss our preliminary conclusions.

Criteria

We focused our FISMA audit approach on federal information security guidance developed by NIST and 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 fiscal year (FY) 2017 FISMA performance audit:

- The Federal Information Security Modernization Act of 2014
- NIST Federal Information Processing Standard (FIPS) and/or SPs[6]
    - 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*
    - NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

[6] 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 800-61 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 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*
  - 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 Year (FY) 2016, FY 2015, FY 2012, and FY 2011 we conducted a FISMA Performance Audit in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. In Fiscal Year (FY) 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. We did not evaluate the status of any FY 2012 FISMA findings as they were already closed.

Prior Year Findings – 2016 Performance Audit

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 1 – Community Development Financial Institutions (CDFI) Fund Risk management activities were not compliant with policies.	For the selected system, CDFI Fund management did not upload required documentation in the Department of Treasury's centralized FISMA inventory management tool.	We recommend that CDFI management: 1. For the selected system, implement a process or mechanism to ensure all required documentation (e.g., SSP, Contingency Plan, Risk Assessments, etc.) is uploaded into the Department's FISMA inventory management tool on the frequency stipulated in TD P 85-01. 2. For the selected system, update the SSP to include CDFI Fund's control implementation.	**Closed** We noted within TFIMS that CDFI Fund management uploaded the required documentation, including the System Security Plan, Contingency Plan and Risk Assessments. Further, we obtained and inspected the SSP and noted it was updated to include CDFI's control implementation

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 1 – Office of Inspector General (OIG) Risk management activities were not compliant with policies.	For the selected system, OIG management did not ensure that the SSP completely addressed NIST SP 800-53, Rev. 4, controls and control enhancements. Specifically, OIG management did not completely document the control requirement for 73 controls and control enhancements within the SSP, did not include 6 controls within the SSP, and did not consistently document within the SSP the selected system's control environment. Additionally, OIG management did not perform or document a formal risk assessment for the system since April 2013. Also, the accompanying system security control assessment did not include all NIST SP 800-53, Rev. 4, controls and control enhancements required for a Moderate system.	We recommend that OIG management: 1. For the selected system, ensure all controls/control enhancement sections and statuses that indicate the control implementation are fully documented in the SSP as required by NIST SP 800-53, Rev. 4. 2. For the selected system, conduct and document a formal risk assessment for the system in accordance with TD P 85-01. 3. For the selected system, develop a security assessment plan that describes the scope of the assessment to include, security controls and control enhancements, assessment procedures to be used to determine security control effectiveness and the assessment environment. 4. For the selected system, conduct a security control assessment based upon the security assessment plan. 5. For the selected system, document the results of the assessment in a security assessment report.	**Closed** We inspected the OIG SSP and noted that all controls/control enhancement sections and statuses were fully documented. Further, we inspected the OIG's risk assessment and noted that it was in accordance with TD P 85 01. In addition, We inspected the OIG security assessment plan and noted that includes security controls and control enhancements under assessment, assessment procedures, and describes the assessment environment. We further inspected that a security control assessment was completed based on the security assessment plan and documented the results of the assessment within the security assessment report.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 1 – Departmental Offices (DO) Risk management activities were not compliant with policies.	For one of the selected systems, DO management did not document all of the NIST SP 800-53, Rev. 4, moderate controls and control enhancements in the SSP. DO policy requires management to use an approved template. Instead, DO management separately documented its security controls in the system Security Controls Requirements Compliance Matrix (SRCM). We noted that a selection of 12 controls and control enhancements in the SRCM were inadequately or inappropriately documented. For the second selected system, DO management did not update the SSP during the FISMA period, resulting in an SSP that does not reflect the implementation status of its controls or the current state of the system.	We recommend that DO management: 1. For the first selected system, align the system documentation of minimum control requirements with the DO SSP template requirements. 2. For the first selected system, review the control implementation documentation to ensure that the NIST 800-53, Rev. 4, controls and control enhancements are fully documented in the SSP. 3. For the second selected system, ensure that the system's current SSP is being reviewed and updated according to NIST SP 800-53, Rev 4., guidance. 4. For the second selected system, ensure descriptions of controls in place are reflective of inherited controls by the service provider. 5. For the second selected system, ensure implementation statuses are being updated to reflect the system more accurately.	**Closed** We obtained and inspected the most recent DO system's SSP and noted it aligns with the SSP template. We analyzed the NIST controls for a moderate system in the SSP and note that moderate controls applicable to the system were included in the SSP with a status of implemented.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 2 – DO POA&Ms were not tracked in accordance with NIST and Treasury requirements.	DO management did not regularly update and monitor progress towards remediating existing POA&Ms and did not close POA&Ms by the established milestones documented. For the first system, DO management had a total of 17 system POA&Ms that were past due and were not updated nor provided a justification of why they had not been closed during the FISMA reporting period of July 1, 2015 through June 30, 2016. For the second system, management had a total of 15 POA&Ms that were past due and did not update and revise these past due POA&Ms with any justification explaining why they had not been updated within established timeframes.	We recommend that DO management: 1. For the first selected system, develop a process to ensure that POA&Ms are being monitored according to DO security policies and NIST guidance. 2. For the first selected system, ensure POA&Ms are updated with revised milestones and provide adequate justification for missed remediation dates. 3. For the second selected system, develop a process to ensure that system POA&Ms are being monitored according to NIST guidance. 4. For the second selected system, ensure POA&Ms are updated with revised milestones and provide adequate justification for missed remediation dates.	**Closed** We noted the CISO hosts quarterly meetings with Systems to review the status of their POA&Ms on a monthly basis. For the first selected system, we obtained and inspected a POA&M and noted it included the following fields: • System Name • Time Frame • POA&M ID • Weakness • Status/Progress Comments • Due Date For the second selected system, we inquired of management and noted system POA&Ms were being monitored on a regular basis. Further, we obtained and inspected a sample of POA&Ms and noted they were updated in a timely manner.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 2– Bureau of the Fiscal Service (Fiscal Service) POA&Ms were not tracked in accordance with NIST and Treasury requirements	Fiscal Service management had one POA&M past due and did not update or provide a justification of why it was past due.	We recommend that Fiscal Service management: 1. For the selected system, develop a process to ensure that POA&Ms are being monitored according to Fiscal Service policies and NIST guidance. 2. For the selected system, ensure POA&Ms are updated with revised milestones and provide adequate justification for missed remediation dates.	**Closed** We inquired of management and noted system POA&Ms were being monitored on a regular basis. We inspected TFIMS and noted that there were no overdue POA&M and POA&M are being monitored and updated with revised milestones and provide adequate justification.
Prior Year FY 2016 Finding # 3 –Fiscal Service Configuration management plan was incomplete and missing key information regarding system baseline configurations.	For the selected system, the configuration management plan (CMP) was incomplete and did not address controls and security requirements over the baseline configuration, which is essential to supporting system rollback procedures. In addition, the plan did not specify the responsibilities regarding the system baseline configuration, the retention and availability of previous baseline configurations, and the frequency that management should review the baseline.	We recommend that Fiscal Service management: 1. For the selected system, ensure that information security controls and requirements, including controls over the system baseline configuration, shared configuration management responsibilities, and the retention of previous baselines, are addressed adequately in the system CMP.	**Closed** We obtained and inspected the updated Configuration Management Plan and noted that it included controls of the system's baseline configuration, management responsibilities, and the retention of previous baselines.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 4 – Bureau of Engraving and Printing (BEP) Vulnerability scans were not being conducted in accordance with TD P 85-01 polices.	For the selected system, BEP management has a Federal Risk and Authorization Management Program (FedRAMP) authorized system that is hosted by a cloud service provider who performs vulnerability scans on its environment monthly instead of every two weeks as required by TD P 85-01.	We recommend that BEP management: 1. For the selected system, work with the Cloud Service Provider to increase the scanning frequency for the system components or create a formal risk acceptance for the reduced scanning frequency. 2. For the selected system, document the actions taken in the above step(s) in the SSP.	**Closed** We obtained and inspected a signed risk acceptance signed by the Designated Approving Authority (DAA) on September 20, 2016.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 4 – DO Vulnerability scans were not being conducted in accordance with TD P 85-01 polices.	DO management did not conduct vulnerability scans for two months for the servers hosted at the Fiscal Service data center. Management did not perform vulnerability scans every two weeks as required by the TD P 85-01. Additionally, the DO *Information Technology Security Handbook* (DO P-910) defines the frequency of vulnerability scans to be conducted at least every thirty days, which does not comply with the biweekly frequency specified by TD P 85-01.	We recommend that DO management: 1. For the selected system, work with Fiscal Service to ensure the system server IP addresses are added to the scanning policy and ensure all future scans are performed at least every two weeks. 2. For the selected system, enhance vulnerability-scanning procedures to ensure a lack a scans will be noted in the event of failure in the future. 3. At the bureau level, update the DO Information Technology Security Policy Handbook (DO P 910) to align with the vulnerability scan frequency of every two weeks, as specified by TD P 85-01. 4. At the bureau level, ensure all DO system’s corresponding SSPs are updated to reflect the scanning frequency as TD P 85-01 and conduct vulnerability scans accordingly.	**Closed** We inquired of management and noted the root cause of this NFR was vulnerability scans not being conducted because of incorrect IP addresses. We further noted that management issued correct IP addresses to the vulnerability scanning to Fiscal Service. We selected a sample of vulnerability scans and noted they were being performed. We also noted the presence of the vulnerability scans as they previously were not generated due to utilization of an invalid IP address. At the bureau level, we inquired with management and were informed that the Department of Treasury amended the TD P 85-01 to require vulnerability scanning to be conducted every 30 days. Therefore, the recommendation to update to DO SSPs was not required.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 5 – CDFI Fund Account management activities were not compliant with policies.	For the selected CDFI Fund system, 5 of 21 sampled user accounts had gone unused for more than 60 days and were not disabled as required by the Security Policy Handbook. Of these five accounts, three had never logged into the system after the account was created.	We recommend CDFI management: 1. For the selected system, work with TTB to revise the inactive user script. 2. For the selected system, test and verify that the script is configured to disable all inactive users after 60 days of inactivity. 3. For the selected system, implement a periodic account review process that will identify any inactive users who have not been disabled.	**Closed** We obtained and inspected the inactive user script created by TTB and noted it was configured to disable all inactive users after 60 days of inactivity. We further noted a copy of the email notification that is generated after execution of the script and that sample of users who had 60 days of inactivity were removed.
Prior Year FY 2016 Finding # 5 – Alcohol and Tobacco Tax and Trade Bureau (TTB) Account management activities were not compliant with policies.	For the selected TTB system, 3 of 8 sampled users for one subcomponent were inactive for more than 60 days and were not disabled automatically within the system, which does not adhere to the SSP. Additionally, we inspected the completed Rules of Behavior (ROB) for system users and noted that one user completed the ROB three months after the account was created, which does not comply with the SSP.	We recommend TTB management: 1. For the selected system, perform a periodic review/analysis, as required by policy, of the accounts for the system to validate that no enabled accounts have gone unused for more than 60 days. 2. For the selected system, establish procedures to be performed by TTB management to ensure that users consistently complete the TTB Rules of Behavior and Access Agreements prior to granting users' access to the system.	**Closed** We obtained and inspected a user listing to include last log on dates and noted that there were no users of the system that were inactive for more than 60 days**.** We selected a sample of users and noted that all of the selected users completed a Rules of Behavior and Access Agreement form.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 5 – OIG Account management activities were not compliant with policies.	For the selected OIG system, access authorizations and user agreements (e.g., Rules of Behavior ROB and Access Agreements) were not consistently documented, approved, and retained during the FY 2016 FISMA performance period. Specifically, 1 of 15 sampled access authorization email notifications was not retained; 2 of 15 sampled ROB/User Agreement forms were not retained for users given access to the system; and 5 of 15 sampled ROB/User Agreement forms were not signed by the ISSO.	We recommend that OIG management: 1. For the selected system, establish a process for consistently completing the Rules of Behavior and Access Agreements and update policies to reflect this policy. 2. For the selected system, establish a process and a centralized location to store and retain completed forms.	**Closed** We inspected the SSP and noted that it documents the established process for completing Rules of Behavior and Access Agreement forms. We further selected a sample of users and noted that all of the sampled users had a completed form and are retained in a centralized location.
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: For the selected system, configure the system to disable user accounts automatically after 120 days of inactivity.	**Partially Implemented/Open** We noted that DO developed a script to disable accounts that have been inactive for over 90 days, and management included the output of this script in TFIMS. However, we independently assessed the appropriateness of the script through inspecting the active directory list and noted that there were accounts that had been inactive for over 90 days but not disabled. Management was able to provide justification for only some accounts.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 5 –Fiscal Service Account management activities were not compliant with policies.	Management utilizes Non-Disclosure Agreements (NDAs) for users as a form of Rules of Behavior and Access Agreement for the first selected Fiscal Service system. Two of 15 sampled system users did not complete their NDAs in a timely manner (within 21 days as stated on the Fiscal Service NDA form). In addition, three of 15 sampled users were missing NDAs. For the second selected system, the SSP and Fiscal Service Baseline Security Requirements (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: 1. 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. 2. For the second 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. 3. For the second system, configure or acquire additional system capability to automatically disable user accounts in accordance with system and Fiscal Service defined frequency.	**Partially Implemented/Open** We obtained and inspected a formal risk acceptance waiver and noted that management performs a manual monthly review of all system user accounts and manually disables or deletes accounts that no longer need access. In addition, we were further informed that they plan to find a feasible way to acquire additional system capability to automatically disable user's accounts in FY18. For the second selected system, we selected a sample of users to ensure they were consistently completing a NDA within in a manner. We noted that NDAs were completed for all of the selected users.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 5 – The United States Mint (Mint) Account management activities were not compliant with policies.	For the selected Mint system, we noted that Mint retains the access authorizations in its Information Technology Service Management (ITSM) ticketing system for the selected system. We noted that 2 of the 8 sampled tickets only identified the customer requesting access and not the actual user who was granted access. Mint management required validation for the two users located at a Mint field office, and the Mint field office IT manager was unable to readily validate ticket information for two users through the ITSM ticketing system. The user listing provided included Customer Names from ITSM tickets; however, the Customer Name was not always the actual user. To determine the user added, each ITSM ticket from the original listing had to be reviewed to identify and validate the user receiving approval for access.	We recommend that Mint management: 1. For the selected system, review established processes and procedures for creation of ITSM tickets for user access requests to specifically identify users receiving access and not just the customers submitting ITSM tickets for user access to system. Furthermore, require that the actual individuals save a copy of their ITSM ticket email notification and email messages for their own access authorization requests for their records. 2. For the selected system, ensure that all current users have their completed ITSM ticket request for access authorizations on file.	**Closed** We obtained and inspected established procedures for creating ITSM tickets for user access requests. We further selected a sample of users and noted that the selected users had a completed ITSM ticket.
Prior Year FY 2016 Finding # 6 – DO A DO System Contingency planning activities were not compliant with policies.	DO's annual contingency plan testing for the selected DO system was not consistent with DO requirements. A PowerPoint presentation was presented to contingency team members explaining general contingency plan concepts. However, DO did not perform formal contingency planning testing during the FISMA year, which is not consistent with DO P-910.	We recommend that DO management: 1. For the selected system, revise the Contingency Plan Test to adhere to DO P-910 and TD P 85-01 requirements for a moderate system and perform testing as required. 2. For the selected system, integrate testing on backups in coordination with Fiscal Services during contingency plan testing occurring twice a year.	**Closed** We obtained and inspected the DO Contingency Plan and noted it was aligned with DO P-910 and TD P 85-01. Additionally, we noted that the contingency plan for the selected DO system was tested.

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: 1. 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.	**Open** We were unable to obtain the Mint's system updated and approved Contingency Plan.
Prior Year FY 2016 Finding # 6– Financial Crimes Enforcement Network (FinCEN) Contingency planning activities were not compliant with policies	FinCEN management did not conduct a contingency plan test and exercise for the system during the FISMA year. Further, management provided a contingency plan that was last reviewed and updated on December 11, 2015, but was not finalized or approved as of the end of the FISMA reporting period.	We recommend that FinCEN management: 1. For the selected system, ensure that the system Contingency Plans are tested on an annual basis and documented according to NIST guidance. 2. 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 plan update.	**Closed** We obtained and inspected the Contingency Plan Test and noted it was tested for FY17. The Contingency Plan included management's approvals, which were added to the plan after it was updated.
Prior Year FY 2016 Finding # 6 – OIG Contingency planning activities were not compliant with policies	For the selected OIG system, the backup integrity test was neither formally conducted nor documented during the FISMA performance period.	We recommend that OIG management: 1. For the selected system, conduct and document formal tests of backup information to ensure media reliability and information integrity on a semi-annual basis.	**Closed** We selected a sample of two quarters and noted during both quarters backup integrity test was conducted and documented.

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.	For a selected Mint system, the help desk did not document or retain records for 4 of the sampled 25 new user access authorizations for the application. Mint management indicated that there was a need to increase support for a large increase in call center volume. During this time, they were receiving user account requests on a daily basis and were trying to setup the call center as quickly as possible, which resulted in some users not properly going through the formal ticketing process.	We recommend that Mint management, for the selected system: 1. Ensure access forms are completed, properly reviewed by the help desk prior to granting access, and centrally retained by the help desk.	**Open** Authorization documentation for a selection of new users was not available.

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: 1. 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. 2. 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. However, we noted in the SSP that the following sections had been updated and fully documented: 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.

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 Federal Risk and Authorization Management Program (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 cloud service provider (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: 1. 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. 2. For the selected system, ensure that third-party CSP provides FISMA-related artifacts to demonstrate FISMA compliance to the Mint security compliance team. 3. 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 April 28, 2017 through April 30, 2018 because the Service Provider has determined that the timeframe for completion of the FedRAMP Agency ATO is 12 months to include conducting a gap analysis of the existing system security documentation.

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.	**Partially Implemented/Open** We inspected the selected system's SSP and noted that the SSP is includes all relevant Rev. 4 controls; however, the implementation statuses were not identified. Mint was unable to provide evidence that all NIST 800-53, Rev. 4, controls in place for the selected system were assessed**.**

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 plan of action and milestones (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.	**Open** BEP had not finished completing its corrective action during the course of this performance audit. We noted that the enterprise-wide POA&M due date to update the policies has been changed to December 31, 2017.

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.	**Partially Implemented/Open** TIGTA has not finished completing its corrective action. We noted that the POA&M due date has been revised to June 1, 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.	**Partially Implemented/Open** TIGTA has not finished completing its corrective action. We noted that the POA&M due date has been revised to January 31, 2017.

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 fiscal year (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 August 31, 2017.
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.	**Partially Implemented/Open** TIGTA has not finished completing its corrective action. We noted that the POA&M due date has been revised to October 31, 2017.

FY16 FISMA Self-Identified Weaknesses – Department of the Treasury

Bureau	System	NIST SP 800 53 Control	Weakness	Status
DO	DO System #1	CA-3	POA&M #11087 ISAs for 1 system interconnection is expired.	**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.
	DO System #1	CM-2	POA&M #11084 Baseline configuration settings are not in compliance. POA&M #16533: Website and Database Scans Required for new system and remediation of vulnerabilities	**Open** POA&M #11084 – Canceled POA&M #16533 – 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 #8395: Account creation, modification, enabling, disabling, or removal of accounts is not automatically audited. POA&M #15524: Password policies not up to FISMA standard.	**Open** POA&M #8395 – Canceled POA&M #15524 - Open We obtained and examined supporting evidence in support of this finding and noted that the finding was cancelled and opened with POA&M #15524, which remained open
	DO System #2	AC-2	POA&M #8410: The system has no process by which the Organization Administrator is notified if general users transfer/resign, therefore neither the account nor passwords are updated.	**Risk Accepted/Closed** We obtained and examined supporting evidence in support of this finding and noted management accepted the risk and closed this finding.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	DO System #2	AU-6	POA&M #8411: Information system monitoring logs/alerts are not provided to DO. POA&M #15528: Information system monitoring logs/alerts are not provided to DO.	**Open** POA&M #8411 – Canceled POA&M #15528 - Open We obtained and examined supporting evidence in support of this finding and noted that the finding was cancelled and closed with POA&M #15528.
	DO System #2	CA-5	POA&M #8397: Plan of Action and Milestones is not up to FISMA standards.	**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.
	DO System #2	CM-2 CM-6	POA&M #8398: Baseline configuration is outdated.	**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.
	DO System #2	CM-6 SI-2	POA&M #8419: Vulnerability scanning is only executed monthly and the application is only scanned when being promoted from development to production. POA&M #15526: Vulnerability scanning is executed monthly; application scanned when promoted from dev. To production.	**Open** POA&M #8419 – Canceled POA&M #15526 - Open We obtained and examined supporting evidence in support of this finding and noted that the finding was cancelled and opened with POA&M #15526, which remained opened

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	DO System #2	CM-6	POA&M #8407: USB ports are not disabled on the servers. POA&M #15531: USB ports are not disabled on the servers.	**Open** POA&M #8407 – Canceled POA&M #15531 – Open We obtained and examined supporting evidence in support of this finding and noted that the finding was cancelled and opened with POA&M #15531, which remained opened
	DO System #2	CM-2 CM-6 CM-8	POA&M #8418; Inventory reports are not provided monthly to the CISO.	**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.
	DO System #2	CP-4	POA&M #8420: CP Test results are documented but are not provided to the SO/ISSO. POA&M #15532: The CP Test results are documented but are not provided to the SO/ISSO for review/upload to the FISMA monitoring system.	**Closed** POA&M #8420 – Canceled POA&M #15532 – 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 cancelled and closed with POA&M #15532.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	DO System #2	IA-2	POA&M #8399: System does not implement PIV enabled features. POA&M #8408: System does not employ multi-factor authentication. POA&M #15522: IA-2 Assurance Level requires identify proofing and multi-factor authentication is not implemented	**Risk Accepted/Closed** POA&M #8399 – Closed POA&M #8408 – Closed POA&M #15522 – Closed We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that both findings POA&M #8399 and POA&M #8408 and noted management accepted the risk and addressed this finding with POA&M #15522, which was closed.
	DO System #2	PL-4 PS-6	POA&M #8401: Third-party personnel are not required to sign a DO NDA nor a ROB.	**Open** DO has not finished completing its corrective action. We noted that the POA&M due date has been revised to November 30, 2017.
	DO System #2	RA-5	POA&M #8400: System Incidents discovered by the third party are not reported to DO.	**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 cancelled and closed with POA&M #8397.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	DO System #2	SI-2	POA&M #8403: 2015 SA&A scanning effort identified numerous vulnerabilities. POA&M #15523: 2015 and 2017 SA&A scanning effort identified numerous vulnerabilities.	**Closed** POA&M #8403 – Canceled POA&M #15523 – 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 cancelled and closed with POA&M #15523.
	DO System #3	CA-3	POA&M #9277: Insufficient interconnection Security Agreements.	**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.
	DO System #3	CM-2	POA&M #10970: The systems Baseline Configurations not adequately documented.	**Open** DO has not finished completing its corrective action. We noted that the POA&M due date has been revised to October 30, 2017.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	DO System #3	CM-6	POA&M #9286: Autocomplete HTML attribute not disabled for password field. POA&M #9287: Cacheable SSL Page Found. POA&M #9288: Missing HTTP only attribute in session cookie. POA&M #9289: Missing secure attribute in encrypted session (SSL) cookie. POA&M #9290: Permanent cookie contains sensitive session information. POA&M #9291: Query parameter in SSL request.	**Closed** POA&M # 9286 – Closed POA&M # 9287 – Closed POA&M # 9288 – Closed POA&M # 9289 – Closed POA&M # 9290 – Closed POA&M # 9291 – 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.
Fiscal Service	FS System #1	PL-4	POA&M #10642: The System SSP and SCM are out of date.	**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.
	FS System #2	IA-2	POA&M #7273: Multifactor Authentication Not Being Utilized.	**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.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
FinCEN	FinCEN System #1	CA-5	POA&M #9803: POA&Ms are not updated in a timely manner.	**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.
Mint	Mint System #1	AC-2	POA&M #10707: The systems users and roles have been granted predefined options.	**Risk Accepted/Closed** We obtained and examined supporting evidence in support of this finding and noted management accepted the risk and closed this finding.
	Mint System #1	AU-2 AC-2	POA&M #10694: The system does not implement automated audit actions to include automatic notification of the ISSO.	**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.
	Mint System #1	CM-6	POA&M #10702: Application server configuration settings do not meet established criteria. POA&M #10696: Oracle configuration settings do not meet established criteria.	**Risk Accepted/Closed** POA&M # 10702 – Closed POA&M # 10696 – Closed We obtained and examined supporting evidence in support of this finding and noted management accepted the risk for POA&M #10702 and closed POA&M #10696.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	Mint System #1	SI-2	POA&M #10699: The system does not have the latest patches/updates installed.	**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.
OCC	OCC System #1	AC-2	POA&M #9327, #9950, #9249: Account Creation Auditing.	**Closed** POA&M # 9327 – Canceled POA&M # 9950 – Closed POA&M # 9249 – Closed We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that the POA&M #9327 was cancelled and closed with both POA&M #9950 and POA&M #9249.
	OCC System #1	CA-5	POA&M #11206: POA&MS are not updated in a timely manner.	**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.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	OCC System #1	CM-6	POA&M #10378, #9247, #9248: System Configuration Settings	**Closed** POA&M # 10378 – Closed POA&M # 9247 – Closed POA&M # 9248 – Closed We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that these findings were remediated.
	OCC System #1	CM-8	POA&M #6400: System Inventory does not accurately reflect inventory of system components.	**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.
	OCC System #1	AC-2	POA&M #9229 System is not configured to automatically deactivate inactive accounts. POA&M #9961 System is not configured to automatically deactivate inactive accounts.	**Closed** POA&M #9229 – Canceled POA&M #9661 – 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 cancelled and closed with POA&M #9661.

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.	**Open** BEP has not finished completing its corrective action. We noted that the policy had been updated and was in management review, but had not been signed yet. Signature is expected later this year.
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.	**Open** DO has not finished completing its corrective action. We noted that the POA&M due date has been revised to December 31, 2017.
	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 POA&M #7314: The database scanning tool used does not have the ability to update itself prior to running a new scan	**Partially Implemented/Open** POA&M #6736 – Open POA&M #7314 – Closed in FY 2016 We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were not fully implemented and that the finding was still open.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	DO System #1	IA-2	POA&M #6368: IA-2 Identification and Authentication: Partially Implemented. Two-factor authentication has not been implemented for Remote Access by all users. POA&M #7328: The application can support authentication of Government employees via their PIV Card, but this capability is not used.	**Risk Accepted/Closed** POA&M 6368 – Closed POA&M 7328 – Closed We obtained and examined supporting evidence in support of these findings and noted management accepted the risk and closed these findings.
	DO System #1	AU-2	POA&M #7412: The SSP does not identify what security events captured by the OS, Database and application and how the list of audited events supports incident response efforts. Database auditing limited to capturing account logon/logoff.	**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.
	DO System #1	AU-6	POA&M #7413: Application logs are not forwarded to the centralized log server for automated review, analysis, and reporting.	**Open** We obtained and inspected supporting evidence in support of this finding and noted that DO has not finished completing its corrective action.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	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.	**Partially Implemented/Open** Although management included hardening guides for both the Oracle database and Microsoft SQL Server in TFIMS, management only applied the hardening guide to the Oracle database. The Authorizing Official (AO) accepted the risk of not hardening the SQL Server because DO is planning to update the SQL server in the future. However, the current system was still operating throughout FY 2017, thus subject to security risks and vulnerabilities from not being hardened.
	DO System #2	SI-2	POA&M #575: SI-2: Numerous weaknesses were discovered during the vulnerability scanning conducted in conjunction with the FY 2013 SA&A effort. POA&M #8631: SI-2: Configuration scans revealed that numerous weaknesses were identified in June 2015. POA&M 10454: April 2016 Vulnerability Report	**Closed** POA&M #575 – Canceled POA&M #8631 – Canceled POA&M #10454 – Closed We obtained and examined supporting evidence in support of this finding and noted that the findings were canceled and closed with POA&M #10454.
	DO System #3	AU-12	POA&M #7645: No application-level auditing capability for application.	**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.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	DO System #3	CP-4	POA&M #3508: Contingency plan testing cannot currently be performed, and emergency preparedness, with regard to system reconstitution, is insufficient.	**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.
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** We obtained and examined supporting evidence in support of this finding and noted this POA&M was transferred to POA&M #6336, 6329, and 6339. We noted that POA&M #6336 has a revised due date of January 24, 2018, POA&M #6329 has a revised due date of March 1, 2018, and POA&M #6339 has a revised due date of November 30, 2017.
	OCC System #1	CM-6	POA&M #3741: CM-6 Configuration Settings, CM-7 Least Functionality System vulnerability scans show numerous vulnerabilities due to unnecessary system services. The results of automated configuration management scans have shown a number of missing patches that are more than 60 days old. Based on this, it has been determined that while a flaw remediation process exists, it has failed to ensure that the system remains correctly configured and up to date.	**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.

APPENDIX III – DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS' FISMA 2017 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 2017 questions for Inspectors General. We prepared responses to DHS questions based on an assessment of 10 information systems across 6 Treasury components. During the FISMA performance audit, we requested that Treasury management communicate its self-assessed maturity levels, and we then designed and executed test procedures to evaluate whether management's security program and practices over Risk Management, Configuration Management, Identity and Access Management, Security Training, and Contingency Planning were at that self-assessed maturity level. We provided the assessed maturity level for each metric using the available options from CyberScope. In most cases, if we determined that one or more bureaus had a finding related to the metric, we assessed the maturity level at 1 ("Ad Hoc") or 2 ("Defined"). For metrics that were assessed as maturity level 1, 2, or 3 ("Consistently Implemented"), we provided explanations in the "Comment" areas to explain why a maturity level 4 ("Management and Measurable") were not obtained.

Treasury Inspector general for Tax Administration (TIGTA) performed audit procedures over the IRS information systems and provided its answers to the Treasury 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.

Since OMB, DHS, and CIGIE changed the FISMA IG reporting metrics and maturity models in FY 2017, a year-on-year comparison for FISMA compliance may not be feasible.

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:

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 seven FISMA program areas. However, the program was not fully effective as reflected deficiencies that we identified in risk management, configuration management, identity and access management, and contingency planning metric domains. In addition, we did not assess any of the FISMA Metric Domains as Managed and Measurable (Level 4). The FY 2017 IG FISMA Reporting Metrics define an effective information security program as Managed and Measurable (Level 4).

Function 1: Identify – Risk Management

1 Does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800-53: CA-3 and PM-5; OMB M-04-25; NIST Cybersecurity Framework (CSF): ID.AM-1 –4)?

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: Fiscal Service self-reported in POA&M #10905 that existing Inter-Agency Security Agreements (ISA) and Memorandum of Understanding (MOU) expired in May and June. In POA&M #10902, Fiscal Service self-reported that ISAs are not updated annually.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that IRS had not identified or formalized specific cloud inventory management processes.

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)?

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: Fiscal Service did not use an automated tool to manage hardware assets consistently across the bureau. Although TTB utilizes a tool to manage hardware assets, the assets are not stored by system to the enable an efficient review of the selected system's assets in this tool.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported instances of inaccurate inventory at IRS, including the lack of detailed information necessary for tracking and reporting.

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 consistently utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment and uses this taxonomy to inform which assets can/cannot be introduced into the network.

Comments: Fiscal Service did not fully implement a comprehensive asset management process. There is no reference within TTB's polices for updating security awareness and training strategy based on assessments of workforce needs.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that, while the IRS is in the early stages of establishing a framework for software asset management, the IRS has not compiled a reliable baseline inventory of software licenses or documented cost savings and cost avoidance attributable to improved software license management in accordance with recent laws and regulations.

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)?

Maturity Level: **Consistently Implemented (Level 3)** - Information on the organization's defined importance/priority levels for its missions, business functions, and information is consistently used and integrated with other information security areas to guide risk management activities and investments in accordance with applicable requirements and guidance.

Comments: In addition, the following prior-year self-identified BEP POA&M remained open: #4001 – the system implementation for NIST SP 800-53, Rev.4, is incomplete.

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 800-39; NIST 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; CFO Council ERM Playbook)?

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: Mint had not reviewed and updated its information security risk management policies, procedures, and templates in over two years. Although the current TTB General Support System (GSS) Risk Assessment was approved and communicated at the enterprise level, there was no evidence of communication at the system and business process levels.

6 Has the organization defined an information security architecture and described how that architecture is integrated into and supports the organization 's enterprise architecture to provide a disciplined and structured methodology for managing risk (NIST 800-39; FEA; NIST 800-53: PL-8, SA-3, and SA-8)?

Maturity Level: **Consistently Implemented (Level 3**) - The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. Security architecture reviews are consistently performed for new/acquired hardware/software prior to introducing systems into the organization's development environment.

Comments: The following prior-year self-identified BEP POA&Ms remained open: #4001 – the system implementation for NIST SP 800-53, Rev.4, is incomplete.

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer, 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 800-39: Section 2.3.1 and 2.3.2; NIST 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 information security risk management program, Treasury should utilize an integrated risk management governance structure for implementing and overseeing an enterprise risk management (ERM) capability that manages risks from information security, strategic planning and strategic reviews, internal control activities, and applicable business areas.

8 To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53: CA-5; OMB M-04-25)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently implements POA&Ms, in accordance with the organization's policies and procedures, to effectively mitigate security weaknesses.

Comments: In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS is in the process of improving its POA&M tracking and remediation processes to ensure effective mitigation of security weaknesses (please see TIGTA’s report for the full text).

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) selecting and implementing security controls to mitigate system-level risks (NIST 800-37; NIST 800-39; NIST 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: FY 2016 DO Finding #6, FY 2015 Mint Finding #2, and FY 2014 Mint Finding #3, regarding not implementing all NIST 800-53, Rev. 4 security controls for SSPs for selected DO and Mint systems, remained open. In addition, the following prior-year self-identified BEP POA&M remained open: #4001 – the system implementation for NIST SP 800-53, Rev.4, is incomplete.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS was not timely correcting vulnerabilities identified by scans primarily due to the lack of resources, and improvements were needed over vulnerability remediation tracking, metrics, and the need for an escalation process.

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)?

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 improve its information security risk management program, Treasury should employ robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, the IRS does not yet have the "robust diagnostics and reporting frameworks" required for the managed and measureable rating; its dashboard is in its infancy stage

11 To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (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 2017 CIO FISMA Metrics: 1.7, 1.8).

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: The FY 2015 Mint Finding #5, regarding Mint contract with third-party cloud service provider did not address Federal Risk and Authorization Management Program (FedRAMP) requirements, remained open.

Fiscal Service self-reported in POA&M #10905 that existing Inter-Agency Security Agreements (ISA) and a Memorandum of Understanding (MOU) expired in May and June.

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: **Defined (Level 2**) - The organization has identified and defined its requirements for an automated solution that provides a centralized, enterprise wide view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.

Comments: DO, BEP, Fiscal Service, FinCEN, and Mint had not implemented bureau-wide technologies to provide a centralized view of risks across the bureaus. Further, these bureaus had not documented policies and/or standard operating procedures for the tools currently being leveraged for tracking and monitoring risk. At TTB, there was no integrated platform for monitoring enterprise-wide risks from different sources.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS continues work with DHS to implement Continuous Diagnostics and Mitigation (CDM) solutions.

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

Consistently Implemented (Level 3)

Comments: 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. Additionally, TIGTA reported that the IRS risk management program is not effective because it did not meet the managed and measurable maturity level.

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

Comments: We had no additional information that was not already covered in metric questions 1 to 12 above. According to DHS criteria, we assessed the Risk Management program to be ineffective. 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; 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: To improve its Configuration Management program, Treasury should assign staff with responsibilities to develop and maintain metrics on the effectiveness of information system configuration management activities. Treasury should consistently collect, monitor, analyze, and update qualitative and quantitative performance measures across the organization and report data on the effectiveness of the agency's information system configuration management program to the Chief Information Security Officer.

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 location within an organization's SDLC;[7] configuration monitoring; and applying configuration management requirements to contracted systems (NIST 800-128: Section 2.3.2; NIST 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: In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS has developed a configuration management plan template that meets standards; however, only four of seven IRS organizational divisions have completed and approved configuration management plans.

[7] 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."

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 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 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that, while the IRS has defined policies and procedures for managing the configurations of its information systems, the IRS has not consistently implemented its policies and procedures, based on the maturity levels of metrics 17, 18, 19, and 21.

17 To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53: CM-2, CM-8; FY 2017 CIO FISMA Metrics: 1.4, 1.5, and 2.1; 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: TTB did not implement current baseline configurations for some systems. The FY 2014 BEP Finding #5, regarding IT security configuration management policy not updated or reviewed to address NIST or Treasury requirements, remained open.

In POA&M #10903, Fiscal Service self-reported that the control implementation statement does not fully address the control requirement of the configuration baseline being approved by the bureau.

The following prior-year self-identified DO POA&Ms remained open: (a) #11084 – baseline configuration settings are not in compliance; (b) #10970 – system baseline configurations not adequately documented; and (c) #576 – although several security hardening guides exist, the system only employs vendor-recommended settings; additionally, the baseline is not documented.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that, while the IRS has defined baseline configurations, it has not ensured that its information systems consistently maintain the baselines or component inventories in compliance with IRS policy.

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 2017 CIO FISMA Metrics: 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Maturity Level: **Defined (Level 2)** - The organization has developed, documented, and disseminated its policies and procedures in this area and developed common secure configurations (hardening guides) that are tailored to its environment. Further, the organization has established a deviation process.

Comments: BEP did not consistently perform configuration baseline compliance scans, and TTB did not implement a current baseline configuration for some systems. In POA&M #16061, TTB self-reported that vulnerabilities for a system were not remediated.

The following prior-year self-identified DO POA&Ms remained open: (a) #8419 – vulnerability scanning only executed monthly and application is only scanned when being promoted from development to production, and (b) #6861 – load balancers affected by multiple vulnerabilities. Furthermore, the following prior-year self-identified BEP POA&M was open: #4001 – the system implementation for NIST SP 800-53, Rev.4, is incomplete.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, 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.

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 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20 Control 4.5; and DHS Binding Operational Directive 15-01)?

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 security relevant updates and patches within organizational defined timeframes, and incorporating flaw remediation into the organization's configuration management processes

Comments: BEP did not fully install patches in a timely manner. TTB did not consistently remediate vulnerability within established timelines, and did not consistently approve operating system patches prior to installation. DO did not maintain testing documentation for patches implemented and did not remediate/mitigate vulnerabilities in a timely manner. Fiscal Service did perform vulnerability and configuration baseline compliance scans on a consistent basis.

The following prior-year self-identified DO POA&Ms remained open: (a) #8419 – vulnerability scanning only executed monthly and application is only scanned when being promoted from development to production, and (b) #8407 – USB ports not disabled on the servers.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, 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. In addition, the IRS indicated that its enterprise patch management has a number of risks and challenges that cannot be appropriately addressed without the adoption and implementation of patch automation.

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (FY 2017 CIO Metrics: 2.26, 2.27, 2.29; OMB M-08-05)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization has consistently implemented its TIC approved connections and critical capabilities that it manages internally. The organization has consistently implemented defined TIC security controls, as appropriate, and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate.

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

21 To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST 800-53: CM-2, CM-3)?

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

Comments: In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, 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. In addition, TIGTA 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 overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

Comments: In POA&Ms #167460-64, Fiscal Service self-reported that security patches and security relevant updates had not been applied within organizational timeframes.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS anticipates that the implementation of DHS' CDM solution will improve its configuration management program. In the meantime, the IRS had made some improvements. The IRS implemented automated scanning of its firewall, router, and switches in January 2016, which updates a dashboard daily with compliance data.

According to DHS criteria, we assessed the Configuration Management program to be ineffective. Please refer to 13.1 for explanation.

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 800-53: AC-1, IA-1, PS-1; and the 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: To improve its Identity and Access Management program, Treasury should assign staff responsibilities for developing, managing, and monitoring metrics on the effectiveness of Identity, Credential, and Access Management (ICAM) activities. Treasury's staff should consistently collect, monitor, and analyze qualitative and quantitative performance measures across Treasury, and the staff should report data on the effectiveness of the Treasury's ICAM program.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS indicated that, while it has resources to implement the ICAM, it has identified certain activities that would benefit from increased resources which would better support improved process efficiency and effectiveness.

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: DO self-reported that the selected DO system did not utilize multifactor authentication.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS utilizes the Treasury Enterprise Identity Credential and Access Management 3–5 Year Roadmap to guide its ICAM initiatives and identify gaps.

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 27 through 31) (NIST 800-53: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); and SANS/CIS Top 20: 14.1)?

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: Both FinCEN and Mint did not consistently implement and perform periodic user access reviews. TTB did not perform semi-annual privileged account access reviews. Although we noted no testing exceptions, Fiscal Service had not defined procedures to ensure the timely removal of user access when the annual user recertification process discovered a user who no longer needed access. TTB did not define a timeframe for the removal of separated user accounts.

In addition, DO self-reported that accounts for the selected system are not automatically disabled after a period of inactivity and that the selected DO system did not use multifactor authentication.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS follows the

Department of the Treasury's policies and procedures for the ICAM as set forth in the Treasury Enterprise Identity, Credential, and Access Management 3–5 Year Roadmap.

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)?

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.

Comments: To improve its Identity and Access Management program, Treasury should employ automation to document and track centrally and share risk designations and screening information with necessary parties, as appropriate.

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: **Consistently Implemented (Level 3)** - The organization ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. The organization utilizes more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate.

Comments: BEP did not retain NDA, rules of behavior, acceptable use agreement, and required training documentation, and Mint did not retain rules of behavior and access agreement forms for a user.

The following prior-year self-identified DO POA&M remained open: #8401 – third-party personnel not required to sign a DO or a ROB.

28 To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

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

Comments: DO self-reported that the DO selected system did not use multifactor authentication.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS has completed e-authentication risk assessments for 28 of its online applications, but only six of the 28 reassessed applications are currently using an appropriate level of assurance to authenticate users.

29 To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

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: Although we noted not testing exceptions, Fiscal Service had not defined procedures to ensure the timely removal of user access because of the annual user recertification process. To improve its Identity and Access Management program, Treasury should ensure that all bureaus require all privileged users utilize strong authentication mechanisms to authenticate to Department and bureau systems.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that, while the IRS reported that 100 percent of its privileged users are required to use PIV cards to access the IRS network, it reported that only eight of 136 internal systems are configured to require PIV cards.

30 To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2017 CIO FISMA metrics: Section 2; 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: FinCEN did not consistently implement and perform a periodic access review. The FY 2016 Fiscal Service Finding #2, that the selected Fiscal Service system failed to disable or remove inactive users, remained open. In addition, the FY 2015 Mint Finding #3, FY 2013 TIGTA Finding #1, and FY 2011 TIGTA Finding #1, regarding logical account management activities were not compliant with policies, in place, and consistently performed, remained open.

BEP FY 2016 Finding #5, related to account management activities compliant with policies, remained open. DO self-reported POA&Ms #16460 and 16465 because DO accounts were not automatically disabled after a period of inactivity and because the DO selected system did not require the use of multifactor authentication. Fiscal Service self-reported POA&Ms #15699, 15700, and 15701 because the Fiscal Service user access recertification process needed improvement. Fiscal Service also self-reported POA&Ms #10904 and 10922 because Fiscal Service inactive accounts were not automatically disabled after 120 days. The following prior-year OCC POA&M remained opened: POA&M #47 – component-level audit requirements have not yet been determined and documented and lack of auditing for the following: audit database management event and audit database object management event.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that IRS plans to use the CDM Phase 2 privilege management solution to enhance its privileged user management process. Additionally, TIGTA referenced a GAO report that numerous authorization control deficiencies still exist in the IRS's computing environment, including not restricting system access based on "least privilege."

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 2017 CIO FISMA Metrics: Section 2)?

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

Comments: TTB has not implemented a process to review consistently remote connections that are logged.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS has not implemented encryption compliant with Federal Information Processing Standard Publication 140-2 on all its remote access connections.

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

Comments: In POA&M #16055, Fiscal Service self-reported least privilege functionality with the selected system. The following prior-year self-identified DO POA&Ms remained open: (a) #7413 – application logs are not forwarded to the centralized log server for automated review, analysis, and reporting, (b) #15528 – information system monitoring logs/alerts are not provided to DO, and (c) #6736 – monthly vulnerability scan data (operating system, database, and application levels) and summary reports are not provided to Treasury. According to DHS criteria, we assessed the Identity and Access Management program to be ineffective. Please refer to 39.1 for explanation.

Function 2C: Protect – Security Training

33 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 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: To enhance its Security Training program, Treasury should assign responsibility for monitoring and tracking the effectiveness of security awareness and training activities. Treasury staff should consistently collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of security awareness and training activities.

34 To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST 800-53: AT-2 and AT-3; NIST 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181 (Draft); 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: There was no reference in Fiscal Services policies and procedures to updating security awareness and training strategy based on assessments of workforce needs. To improve its Security Training program, Treasury should address all of its identified knowledge, skills, and abilities gaps. Treasury should obtain appropriate resources and develop and implement the appropriate metrics to measure the effectiveness of its training program in closing identified skill gaps.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA that the IRS has not yet addressed all of its identified knowledge, skills, and abilities gaps.

35 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 800-53: AT-1; NIST 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 enhance its Security Training program, Treasury should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. Treasury should ensure that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

36 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 questions 37 and 38 below) (NIST 800-53: AT-1 through AT-4; and NIST 800-50)

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

Comments: A Mint user did not complete or sign a Rules of Behavior or Access Agreement form in a timely manner.

37 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 800-53: AT-2; FY 17 CIO FISMA Metrics: 2.23; NIST 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: Mint did not retain rules of behavior and access agreement forms for a user.

38 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 800-53: AT-3 and AT-4; FY 17 CIO FISMA Metrics: 2.23)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization ensures 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. Furthermore, the organization maintains specialized security training completion records.

Comments: To enhance its Security Training program, Treasury should obtain feedback on its security training content and make updates to its program, as appropriate. In addition, Treasury should measure the effectiveness of its specialized security-training program.

39.1 Please provide the assessed maturity level for the agency's Protect - Configuration Management/Identity and Access Management/Security Training (Functions 2A - 2C).

Consistently Implemented (Level 3)

Comments: We determined that Treasury's security program and practices for Configuration Management, Identity and Access Management, and 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.

39.2 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?

Comments: We had no additional information that was not already covered in metric questions 33 to 38 above. According to DHS criteria, we assessed the Security Training program to be ineffective. Please refer to 39.1 for explanation.

Function 3: Detect – ISCM

40 To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM (NIST SP 800-137: 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: TTB management self-assessed it maturity level for this metric as Defined. TTB management should update the TTB Risk Management Framework Standard Operating Procedure to reference the current Department of Treasury ISCM framework.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS did not provide information to support that the organization monitors and analyzes qualitative and quantitative measures on the effectiveness of its ISCM strategy.

41 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; collecting 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 43)

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: Management for the Department, BEP, and TTB management self-assessed their maturity levels for this metric as Defined. TTB management should update the TTB Risk Management Framework Standard Operating Procedure to reference the current Department of Treasury ISCM framework. However, Fiscal Service, DO, FinCEN, and Mint self-assessed their maturity levels for this metric as Consistently Implemented.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS did not provide information to support that the organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies and procedures and makes updates as appropriate.

42 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 2017 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: BEP and TTB management self-assessed their maturity levels for this metric as Defined. However, management for the Department, Fiscal Service, DO, FinCEN, and Mint self-assessed their maturity levels for this metric as Consistently Implemented.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS is in the process of establishing a cybersecurity training plan to follow NIST Special Publication 800-181, *National Institute for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (August 2017).

43 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 implement its process 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, technical) and types (common, hybrid, and system-specific) are assessed and monitored.

Comments: TTB management self-assessed their maturity levels for this metric as Defined. TTB management should update the TTB Risk Management Framework Standard Operating Procedure to reference the current Department of Treasury ISCM framework.

In POA&M 11715, Fiscal Service self-reported that it was unknown if security assessments were performed on the enterprise infrastructure.

44 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: The Department, BEP, DO, and TTB management self-assessed their maturity levels for this metric as Defined. TTB management should update the TTB Risk Management Framework Standard Operating Procedure to reference the current Department of Treasury ISCM framework. In addition, the following prior-year self-identified BEP POA&M remained open: #4001 – the system implementation for NIST SP 800-53, Rev.4, is incomplete.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS is still in the process of implementing a data analysis tool and reporting system to achieve requirements for data collection, storage, analysis, retrieval, and reporting.

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

Consistently Implemented (Level 3)

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

45.2 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: We had no additional information that was not already covered in metric questions 40 to 44 above. According to DHS criteria, we assessed the ISCM program to be ineffective. Please refer to 45.1 for explanation.

Function 4: Respond – Incident Response

46 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; FY 2017 CIO FISMA Metrics: 4.1, 4.3, and 4.6)? (Note: The overall maturity level should take into consideration the maturity of questions 48 - 52)

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 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS did not provide sufficient information to support that it is consistently capturing and sharing lessons learned.

47 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; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-16-03; OMB M-16-04; FY 2017 CIO FISMA Metrics: 1.6 and 4.5; 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 program, Treasury should assign responsibility for monitoring and tracking the effectiveness of incident response activities. Treasury staff should collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of its IR activities.

48 How mature are the organization's processes for incident detection and analysis (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; 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 enhance its Incident Response 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. Through profiling techniques, the Treasury should maintain a comprehensive baseline of network operations and expected data flows for users and systems.

In the *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017* (Reference Number 2017-20-087), dated September 29, 2017, TIGTA reported that the IRS did not provide sufficient information to support that it maintains a comprehensive baseline of network operations and expected data flows for users and systems.

49 How mature are the organization's processes for incident handling (NIST 800-53: IR-4)?

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 Incident Response program, Treasury should manage and measure the impact of successful incidents and should establish a process to mitigate related vulnerabilities quickly on other systems so that they are not subject to exploitation of the same vulnerability.

50 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-16-03; NIST 800-53: IR-6; US-CERT Incident Notification Guidelines)?

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 Incident Response program, Treasury should employ metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.

51 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 and enter into contracts, as appropriate, for incident response support (FY 2017 CIO FISMA Metrics: 4.4; NIST SP 800-86)?

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 is utilizing DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its network.

Comments: This is the highest level for this metric.

52 To what degree does the organization utilize the following technology to support its incident response program?
- Web application protections, such as web application firewalls
- Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools
- Aggregation and analysis, such as security information and event management (SIEM) products
- Malware detection, such as antivirus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2)

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: Mint did not retain evidence of testing results for its incident reporting capabilities. To enhance its Incident Response program, Treasury should use technologies for monitoring and analyzing qualitative and quantitative performance across the organization and should collect, analyze, and report data on the effectiveness of its technologies for performing incident response activities.

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

Consistently Implemented (Level 3)

Comments: 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.

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

Comments: We had no additional information that was not already covered in metric questions 46 to 52 above. According to DHS criteria, we assessed the Incident Response program to be ineffective. Please refer to 53.1 for explanation.

Function 5: Recover – Contingency Planning

54 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 800-53: CP-1 and CP-2; NIST 800-34; NIST 800-84; FCD-1: Annex B)?

Maturity Level: **Consistently Implemented (Level 3)** - Roles and responsibilities of stakeholders involved in information system contingency planning have been fully defined and communicated across the organization. In addition, 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: The FY 2013 TIGTA Finding #4, regarding contingency planning and testing controls were not fully implemented or operating as designed, remained open.

55 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 56-60) (NIST SP 800-34; NIST SP 800-161).

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: To enhance its Contingency Planning program, Treasury should understand and manage its information and communications technology (ICT) supply chain risks related to contingency planning activities. As appropriate, Treasury should integrate ICT supply chain concerns into its contingency planning policies and procedures, define and implements a contingency plan for ICT supply chain infrastructure, applies appropriate ICT supply chain controls to alternate storage and processing sites, and consider alternate telecommunication services providers for its ICT supply chain infrastructure to support critical information systems.

56 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST 800-53: CP-2; NIST 800-34, Rev. 1, 3.2, FIPS 199, FCD-1, OMB M-17-09)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization incorporates the results of organizational and system level BIAs[8] 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: This is the highest level for this metric. Additionally, BEP and Mint did not employ BIAs for the selected systems.

57 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)?

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: To improve its Contingency Planning program, Treasury should integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of 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.

[8] National Institute Standards and Technology (NIST) Special Publication (SP) 800-34, Revision (Rev) 1, *Contingency Planning Guide for Federal Information Systems*, defines a Business Impact Analysis (BIA) as an "analysis of information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption."

58 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST 800-34; NIST 800-53: CP-3, CP-4)?

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/COOP[9]/BCP.[10]

Comments: The FY 2013 TIGTA Finding #4, regarding contingency planning and testing controls were not fully implemented or operating as designed, was still open.

59 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST 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; and NARA guidance on information systems security records)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently implements its processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and RAID,[11] 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: This is the highest level for this metric.

60 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 800-53: CP-2, IR-4)?

[9] NIST SP 800-34, Revision 1, defines a Continuity of Operations Plan (COOP) as a "predetermined set of instructions or procedures that describe how an organization's mission essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations."

[10] NIST SP 800-34, Revision 1, defines a Business Continuity Plan (BCP) as the "documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption."

[11] Redundant Array of Independent Disks (RAID) is a common practice of storing the same data in different places on many hard disks to protect the data in the event of a disk failure.

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: To enhance its Contingency Planning program, Treasury should communicate metrics on the effectiveness of recovery activities to relevant stakeholders. Treasury should ensure that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.

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

Consistently Implemented (Level 3)

Comments: 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.

61.2 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: We had no additional information that was not already covered in metric questions 54 to 60 above. According to DHS criteria, we assessed the Contingency Planning program to be ineffective. Please refer to 61.1 for explanation.

Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	11
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	0

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	7
Managed and Measurable	0
Optimized	0
Function Rating: Ad Hoc (Level 1)	0

Function 2B: Protect - Identity and Access Management

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

Function 2C: Protect - Security Training

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

Function 3: Detect - ISCM

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

Function 4: Respond - Incident Response

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

Function 5: Recover - Contingency Planning

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

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 2: Protect - Configuration Management / Identity Management / Security Training	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's security program and practices for Configuration Management, Identity and Access Management, and 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 ISCM did not meet the Managed and Measurable

			maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 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 seven FISMA program areas. However, the program was not fully effective as reflected 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 2017 IG FISMA Reporting Metrics defines an effective information

			security program as Managed and Measurable (Level 4).

APPENDIX IV – APPROACH TO SELECTION OF SUBSET OF SYSTEMS

In executing the Fiscal Year (FY) 2017 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 2017 Department of Treasury (Treasury or Department) at the Bureau of Engraving and Printing (BEP), Departmental Offices (DO), Financial Crimes Enforcement Network (FinCEN), Bureau of the Fiscal Service, (Fiscal Service), United States Mint (Mint), and Alcohol and Tobacco Tax and Trade Bureau (TTB).

In order to select our sample, working with Treasury Office of Inspector General (OIG), we judgmentally selected six bureaus from which to test. The basis of this judgment was bureaus that held systems of high operational value, mission, number of information systems managed, and potential information security risk.

DO, Fiscal Service, and TTB: With the exception of the Internal Revenue Service, DO and Fiscal Service had the largest number of systems in their system inventories; moreover, Fiscal Service, DO, and TTB hosted applications and information technology (IT) environments that other Treasury bureaus utilize to perform their day-to-day mission activities. For example:

- Many Treasury bureaus and other agencies utilized major applications hosted and managed by DO and Fiscal Service.
- TTB hosts and manages the Community Development Financial Institutions Fund's network and IT systems.

Due the size of their IT environments and sharing of services, there was an increased risk of unappropriated or unauthorized access and disclosure or modification of data at these bureaus. Therefore, we included Fiscal Service, DO, and TTB in the FY 2017 audit scope.

BEP, FinCEN, and Mint: BEP and Mint generate the nation's currency, and FinCEN assists law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes. Due to their missions, there could be an increased threat of internal or external cyber-attacks on these Bureaus. Therefore, we included BEP, FinCEN, and Mint in the 2017 audit scope.

Approach:

With the assistance of DO Management, we obtained a listing of all systems from the Department for the bureaus denoted above. 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 2017 FISMA Performance Audit for unclassified systems.

KPMG considered the following factors during the selection process:

- Department of the Treasury High Value Asset[12] listing.
- Total number of financial and operational systems per bureau, excluded systems in the implementation, development, and disposal phases.
- Number of operational major/minor applications and general support systems (GSS) at each bureau with a Federal Information Processing Standard (FIPS) system impact level of Moderate or High.

In addition, we excluded information systems that were selected in support of the FYs 2014, 2015, and 2016 FISMA audits to avoid redundancy. Table 2 summarizes our considerations for selecting the in-scope systems for the 2017 performance audit.

#	Bureau	Total # of Operational Info. Systems	Number of Information Systems Considered After Analysis	Number of Information Systems Selected
1	Bureau of Engraving and Printing (BEP)	11	7	1
2	Departmental Offices (DO)	54	43	3
3	Financial Crimes Enforcement Network (FinCEN)	10	7	1
4	Bureau of the Fiscal Service (Fiscal Service)	71	60	3
5	United States Mint (Mint)	17	14	1
6	Alcohol Tobacco Tax and Trade Bureau (TTB)	20	17	1
	Totals	183	148	10

Table 2: *Considerations for selecting systems for the 2017 performance audit.*

[12] 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.

Using a random number generator, KPMG randomly selected 10 of 148 operational systems. **Table 3** below denotes the selected application and systems for the 2017 performance audit.

Bureau	System	FIPS 199	System Type	Financial System	Disposition	High Value Asset
BEP	BEP System 1	Moderate	Major Application	Yes	Major Modification	No
DO	DO System 1	High	GSS	Yes	Operational	No
	DO System 2	Moderate	Major Application	No	Operational	No
	DO System 3	High	Major Application	No	Operational	No
FinCEN	FinCEN System 1	High	Major Application	No	Operational	No
Fiscal Service	Fiscal Service System 1	High	Major Application	No	Operational	Yes
	Fiscal Service System 2	High	Major Application	No	Operational	No
	Fiscal Service System 3	Moderate	Major Application	No	Operational	No
Mint	Mint System 1	Moderate	Major Application	No	Operational	No
TTB	TTB System 1	Moderate	Minor Application	No	Operational	No

Table 3: *Selected application and systems for the 2017 performance audit.*

APPENDIX V – GLOSSARY OF TERMS

Acronym	Definition
AC	Access Control
ACIOCS	Associate Chief Information Officer for Cyber Security
AICPA	American Institute of Certified Public Accounts
AT	Awareness and Training
AU	Audit and Accountability
ATO	Authority to Operate
BCP	Business Continuity Planning
BEP	Bureau of Engraving and Printing
BIA	Business Impact Analysis
BLSR	Baseline Security Requirements
BPD	Bureau of the Public Debt
Bureaus	Department of the Treasury Bureaus/Offices
CA	Security Assessment and Authorization
CDFI Fund	Community Development Financial Institutions Fund
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
CS	Contractor Systems
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	Federal Continuity Directive
FedRAMP	Federal Risk and Authorization Management Program
FinCEN	Financial Crimes Enforcement Network
FIPS	Federal Information Processing Standards
Fiscal Service	The Bureau of the Fiscal Service
FISMA	Federal Information Security Modernization Act of 2002
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
HSPD	Homeland Security Presidential Directive
IA	Identity and Access Management
IG	Inspector General

Acronym	Definition
IR	Incident Response
IRS	Internal Revenue Service
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
ISSO	Information Systems Security Officer
IT	Information Technology
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
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestone
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
Rev.	Revision
RM	Risk Management
ROB	Rules of Behavior
SA	System and Services Acquisition
SA&A	Security Assessment and Authorization
SC	System and Communication Protection
SCM	Security Controls Matrix
SI	System and Information Integrity
SIGTARP	Special Inspector General for the Troubled Asset Relief Program
SO	System Owner
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
TT&E	Test, Training & Exercise
US-CERT	United States Computer Emergency Readiness Team

THIS PAGE INTENTIONALLY LEFT BLANK

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 2

Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017
September 29, 2017

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 2017

September 29, 2017

Reference Number: 2017-20-087

This report remains the property of the Treasury Inspector General for Tax Administration (TIGTA) and may not be disseminated beyond the Internal Revenue Service without the permission of TIGTA. This report may contain confidential return information protected from disclosure pursuant to I.R.C. § 6103(a). Such information may be disclosed only to Department of the Treasury employees who have a need to know this information in connection with their official tax administration duties.

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 REPORT FOR FISCAL YEAR 2017

Highlights

Final Report issued on September 29, 2017

Highlights of Reference Number: 2017-20-087 to the Department of the Treasury, Office of the 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 and has an obligation to protect this sensitive information against unauthorized access or loss in accordance with FISMA requirements.

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 2017.

WHAT TIGTA FOUND

For Fiscal Year 2017, the Inspectors General FISMA reporting metrics were aligned with the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity* and measured the maturity levels for five functional areas: IDENTIFY (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 were 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 a maturity level 4, *Managed and Measured*, or above.

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

The IDENTIFY function area was based on the Risk Management performance metrics, which TIGTA deemed at a maturity level 3, *Consistently Implemented*. The PROTECT function area was based on metrics for three security program areas: Configuration Management, which was at a maturity level 2, *Defined*; Identity and Access Management, which was at a maturity level 3, *Consistently Implemented*; and Security Training, which was at a maturity level 4, *Managed and Measured*. The end result for this function area was a maturity level 3, *Consistently Implemented*. The DETECT function area was based on the Information Security Continuous Monitoring metrics, which TIGTA deemed at a maturity level 3, *Consistently Implemented*.

Until the IRS takes steps to improve its security program deficiencies and fully implement all security program areas 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 on only 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 29, 2017

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDIT
OFFICE OF THE 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 2017 (Audit # 201720001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Modernization Act (FISMA)[1] evaluation of the Internal Revenue Service (IRS) for Fiscal Year 2017. The Act requires Federal agencies to have an annual independent evaluation performed of their information security programs and practices and to report the results of the evaluation to the Office of Management and Budget. Our overall objective was to assess the effectiveness of the IRS's information security program, procedures, and practices and its compliance with FISMA requirements for the period July 1, 2016, to June 30, 2017. This audit is included in our Fiscal Year 2017 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

This report is being forwarded to the Treasury Inspector General for consolidation into a report issued to the Department of the Treasury, Chief Information Officer. We are also sending copies of this report to the IRS managers affected by the report.

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

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

Table of Contents

Appendices

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
PIV	Personal Identity Verification
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 source. 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 Internal Revenue Service is responsible for implementing appropriate security controls to protect the confidentiality of sensitive information against unauthorized access or loss in accordance with FISMA requirements.

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 the Inspector General. TIGTA is responsible for oversight of the Internal Revenue Service (IRS), while the Treasury Office of the Inspector General is responsible for all other Treasury bureaus.

The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. As a custodian of taxpayer information it receives and maintains, the IRS is

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

responsible for implementing appropriate security controls to protect the confidentiality of this sensitive information against unauthorized access or loss in accordance with FISMA requirements. Under the 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 the FISMA and related OMB policies and NIST procedures, standards, and guidelines.

Fiscal Year (FY)[2] 2017 Inspector General FISMA Reporting Metrics[3]

The FY 2017 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 2017 metrics represent a continuation of the 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*[4] (Cybersecurity Framework) and transition the evaluation of all the functional areas to the maturity model approach. The five Cybersecurity Framework function areas are:

- IDENTIFY – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, 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.

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

[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] DHS, *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (Version 1.0, Apr. 2017).

[4] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, Feb. 2014).

Figure 1: Alignment of the NIST Cybersecurity Framework's Function Areas to the FY 2017 Inspector General FISMA Metric Domains

Cybersecurity Function Areas	FY 2017 Inspector General FISMA Metric Domains
IDENTIFY	Risk Management
PROTECT	Configuration Management Identity and Access Management Security Training
DETECT	Information Security Continuous Monitoring (ISCM)
RESPOND	Incident Response
RECOVER	Contingency Planning

Source: FY 2017 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. Figure 2 details the five maturity model 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]

Figure 2: Inspector General's 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 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 2017 Inspector General FISMA Reporting Metrics.

[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.

This review was performed with information obtained from the IRS Information Technology organization's Office of Cybersecurity in New Carrollton, Maryland, during the period May through August 2017. This report covers the period from July 1, 2016, through June 30, 2017. 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 Three 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 IRS's Cybersecurity Program was not fully effective.

To determine the effectiveness of the IRS's Cybersecurity Program, we evaluated the maturity level of the program metrics specified by the DHS in the *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0* issued on April 17, 2017. We based our work, in part, on a representative subset of seven IRS information systems and the implementation status of key security controls. We also considered the results of TIGTA and Government Accountability Office (GAO) audits performed or completed during the FY 2017 FISMA evaluation period that contained results applicable to the FISMA metrics. See Appendix IV for a list of audits.

As shown in Figure 3, based on the DHS's scoring methodology for the FY 2017 FISMA evaluation period, we rated two Cybersecurity Framework functions as "effective" and three as "not effective."

Figure 3: Maturity Levels by Function Area

Function	Assessed Maturity Level	Effective Function
Function 1: IDENTIFY – Risk Management	**Consistently Implemented (Level 3)**	**No**
Function 2: PROTECT **Configuration Management** **Identity and Access Management** **Security Training**	 **Defined (Level 2)** **Consistently Implemented (Level 3)** **Managed and Measurable (Level 4)**	**No**
Function 3: DETECT – ISCM	**Consistently Implemented (Level 3)**	**No**
Function 4: RESPOND – Incident Response	**Managed and Measurable (Level 4)**	**Yes**
Function 5: RECOVER – Contingency Planning	**Managed and Measurable (Level 4)**	**Yes**

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

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

The FY 2017 Inspector General FISMA Reporting Metrics specified that, within the context of the maturity model evaluation process, maturity level 4, *Managed and Measurable*, represents an effective level of security. For the five Cybersecurity Framework function areas, we found that two areas, RESPOND and RECOVER, and their two security program areas, 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 24 and 26, respectively.

For the remaining three Cybersecurity Framework function areas, four of their five security program areas did not meet a managed and measurable maturity level for the reasons presented in the next three sections of the report. As a result, these function areas were deemed as "not effective." The details of the results of our evaluation of these three maturity levels are presented on pages 8, 13, 17, 20, and 22, respectively.

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

Based on the FY 2017 Inspector General FISMA Reporting Metrics, we found that the function area IDENTIFY and its security program area, Risk Management, met a *Consistently Implemented* maturity level 3. In order for the IRS to meet a *Managed and Measurable* maturity level 4 (and therefore an effective level), we believe that the IRS needs to improve on the following risk management program performance metrics.

- Maintain a comprehensive and accurate inventory of its information systems (including cloud systems).
- Maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.
- 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.
- Ensure that plans of action and milestones (POA&M) are used to effectively mitigate security weaknesses.
- Implement an automated solution that provides a centralized enterprise-wide view of risks, including risk control and remediation activities, dependencies, risk scores, and management dashboards.

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

The function area PROTECT is made up of three security program areas: Configuration Management, Identity and Access Management, and Security Training. Based on the FY 2017 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 area of Identity and Access Management rated at a *Consistently Implemented* maturity level 3, and the security program area of Configuration Management rated at a *Defined* maturity level 2. As a result, both of these program areas were considered "not effective." Therefore, because two of the three program areas 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 Identity and Access Management program area, we believe the IRS needs to improve on the following performance metrics:

- Ensure that all nonprivileged and privileged users use strong authentication to access IRS facilities, networks, and information systems, including remote access.
- Employ automated mechanisms to support the management of privileged accounts.
- Implement Federally compliant encryption on all remote access connections.

In order for the IRS to meet an effective level for the Configuration Management program area, we believe the IRS needs to improve on the following performance metrics:

- Complete and approve configuration management plans for all IRS organizations.
- Maintain baseline (and common secure) configurations consistently on information systems, and maintain inventories of related components at a level of granularity necessary for tracking and reporting.
- Ensure timely remediation of information system vulnerabilities and patching.
- Implement change control policies, procedures, and processes consistently IRS-wide.

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

Based on the FY 2017 Inspector General FISMA Reporting Metrics, we found that the function area DETECT and its security program area, ISCM, met a *Consistently Implemented* maturity level 3. In order for the IRS to meet an effective level for the ISCM program area, we believe the IRS needs to improve on the following performance metrics:

- Use the NIST *National Institute for Cybersecurity Education Framework* to define ISCM roles and responsibilities and map to Cybersecurity organization employees, complete a skills assessment, and make targeted training recommendations in order to support a workforce capable of meeting the IRS's cybersecurity needs.

- Consistently capture qualitative and quantitative performance measures on the effectiveness of its ISCM program.

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

TIGTA's responses to the DHS's FY 2017 Inspector General FISMA Reporting Metrics

The details of the results of our evaluation of the maturity level of each of the FY 2017 Inspector General FISMA Reporting Metrics are provided below. The metrics are based on Federal Government guidance and criteria, such as NIST Special Publication 800-53 and OMB memoranda. See the embedded guidance in Appendix I for the specific references for each metric. 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 2107 Inspector General FISMA Reporting Metrics.

Function 1: IDENTIFY – Risk Management

Function	Count
Ad-Hoc	**0**
Defined	**5**
Consistently Implemented	**4**
Managed and Measurable	**3**
Optimized	**0**
Function Rating: Consistently Implemented (Level 3)	

1. Does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems) and system interconnections?

   Maturity Level: **Defined (Level 2)** – The organization has defined, but not consistently implemented, a process to develop and maintain a comprehensive and accurate inventory of its information systems and system interconnections.

Comments: TIGTA reported[6] that the IRS had not identified or formalized specific cloud inventory management processes.

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?

   Maturity Level: **Defined (Level 2)** – The organization has defined, but not consistently implemented, 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] and the GAO[8] reported instances of inaccurate inventory, including the lack of detailed information necessary for tracking and reporting.

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, but not consistently implemented, 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: TIGTA reported[9] that, while the IRS is in the early stages of establishing a framework for software asset management, the IRS has not compiled a reliable baseline inventory of software licenses or documented cost savings and cost avoidance attributable to improved software license management in accordance with recent laws and regulations.

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)** – Information on the organization's defined importance/priority levels for its missions, business functions, and information is consistently used and integrated with other information security areas to guide risk management activities and investments in accordance with applicable requirements and guidance.

[6] 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).

[7] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017).

[8] GAO, GAO-17-140, *Financial Audit: IRS's Fiscal Years 2016 and 2015 Financial Statements* (Nov. 10, 2016).

[9] TIGTA, Ref. No. 2017-20-062, *The Internal Revenue Service Is Not in Compliance With Federal Requirements for Software Asset Management* (Sept. 2017).

Comments: This is the highest 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 reproducible format.

6. Has the organization defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture to provide a disciplined and structured methodology for managing risk?

   Maturity Level: **Consistently Implemented (Level 3)** – The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. Security architecture reviews are consistently performed for new/acquired hardware/software prior to introducing systems into the organization's development environment.

   Comments: This is the highest level for this metric.

7. To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer, 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 utilizes an integrated risk management governance structure for implementing and overseeing an enterprise risk management capability that manages risks from information security, strategic planning and strategic reviews, internal control activities, and applicable mission/business areas.

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

   Maturity Level: **Defined (Level 2)** – Policies and procedures for the effective use of the 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: The IRS is in the process of improving its POA&M tracking and remediation processes to ensure effective mitigation of security weaknesses. We reviewed 94 weaknesses that the IRS identified during the annual testing of controls of the seven selected systems. Of the 94 weaknesses, we could not track 17 weaknesses to either existing or closed POA&Ms that supported effective remediation. The IRS created the POA&Ms for 13 of these 17 weaknesses after we asked about them.

We also reviewed 22 POA&Ms that were closed in FY 2017 related to the seven selected systems. Of the 22 POA&Ms that were closed, three 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 has reopened two of them.

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) selecting and implementing security controls to mitigate system-level risks?

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

   Comments: TIGTA reported[10] that the IRS was not timely correcting vulnerabilities identified by scans primarily due to the lack of resources and that improvements were needed over vulnerability remediation tracking, metrics, and an escalation process.

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

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

    Comments: The IRS does not yet have the "robust diagnostics and reporting frameworks" required for the managed and measureable rating; its dashboard is in its infancy stage.

11. To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, Federal

[10] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017).

Acquisition Regulation[11] clauses, and clauses on protection, detection, and reporting of information) and Service Level Agreements[12] 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: **Defined (Level 2)** – The organization has identified and defined its requirements for an automated solution that provides a centralized, enterprise-wide view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.

    Comments: The IRS continues to work with the DHS to implement Continuous Diagnostic and Mitigation solutions.

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

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

    Comments: The IRS risk management program is not effective because it did not meet the managed and measurable maturity level.

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

[12] 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.

Function 2a: PROTECT – Configuration Management

Function	Count
Ad-Hoc	**0**
Defined	**6**
Consistently Implemented	**1**
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: **Managed and Measurable (Level 4)** – Staff are assigned responsibilities for developing and maintaining metrics on the effectiveness of information system configuration management activities. The organization's staff is consistently collecting, monitoring, analyzing, and updating qualitative and quantitative performance measures across the organization and is reporting data on the effectiveness of the organization's information system configuration management program to the Chief Information Security Officer.

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 location within an organization's System Development Lifecycle;[13] configuration monitoring; and applying configuration management requirements to contracted systems?

    Maturity Level: **Defined (Level 2)** – The organization has developed an organizationwide configuration management plan that includes the necessary components.

    Comments: The IRS has developed a configuration management plan template that meets standards; however, only four of seven IRS organizational divisions have completed and approved configuration management plans.[14]

[13] 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.

[14] The IRS's Metric or Key Performance Indicator for Configuration Management, July 18, 2017.

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 metrics 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, the IRS 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 baselines or component inventories in compliance with IRS policy. The IRS's annual security testing of systems reported that three of the seven systems that we selected for the FY17 FISMA evaluation did not consistently maintain baseline configurations. In addition, TIGTA[15] and the GAO[16] reported instances of baseline configurations not being consistently implemented and inaccurate system component inventories.

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

    Maturity Level: **Defined (Level 2)** – The organization has developed, documented, and disseminated its policies and procedures in this area and developed 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 that we selected for the FY17 FISMA evaluation did not maintain secure

[15] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017); and TIGTA, Ref. No. 2017-20-004, *Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners* (Oct. 2016).

[16] GAO, GAO-17-395, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 26, 2017).

configuration settings in accordance with IRS policy. Also, TIGTA[17] and the GAO[18] 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.[19] In addition, the GAO reported that the mainframe tool only tests compliance with a limited subset of the agency's policies.

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

    Maturity Level: **Defined (Level 2)** – The organization has developed, documented, and disseminated its policies and procedures for flaw remediation. Policies and procedures include processes for: identifying, reporting, and correcting information system flaws; testing software and firmware updates prior to implementation; installing security relevant updates and patches within organizationally defined time frames; and incorporating flaw remediation into the organization's configuration management processes.

    Comments: While the IRS has defined flaw remediation policies, including patching, it has not consistently implemented flaw remediation and patching on a timely basis. The IRS's annual security testing of systems reported that flaw remediation processes were not in place for four of the seven systems that we selected for the FY17 FISMA evaluation. Also, TIGTA[20] and the GAO[21] reported that the IRS did not remediate high-risk vulnerabilities or install security patches on systems in a timely manner. In addition, the IRS indicated that its enterprise patch management has a number of risks and challenges that cannot be appropriately addressed without the adoption and implementation of patch automation.

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

    Maturity Level: **Consistently Implemented (Level 3)** – The organization has consistently implemented its Trusted Internet Connection–approved connections and critical capabilities that it manages internally. The organization has consistently implemented defined Trusted Internet Connection security controls, as appropriate, and implemented actions to ensure that

[17] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017); and TIGTA, Ref. No. 2017-20-004, *Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners* (Oct. 2016).
[18] GAO, GAO-17-395, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 26, 2017).
[19] A method for using specific standardized testing methods to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements.
[20] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017); and TIGTA, Ref. No. 2017-20-004, *Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners* (Oct. 2016).
[21] GAO, GAO-17-140, *Financial Audit: IRS's Fiscal Years 2016 and 2015 Financial Statements* (Nov. 10, 2016); GAO, GAO-17-395, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 26, 2017).

all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate.

Comments: This is the highest maturity level 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,[22] as appropriate?

    Maturity Level: **Defined (Level 2)** – The organization has developed, documented, and disseminated its policies and procedures for managing configuration change control. The policies and procedures address, at a minimum, the necessary configuration change control related activities.

    Comments: While the IRS has defined policy and procedures for managing configuration change control, these policy and procedures have not been consistently followed at the information system level. The IRS's annual security testing of systems reported that three of the seven systems that we selected for the FY17 FISMA evaluation did not have a documented change management process in place. In addition, TIGTA[23] and the GAO[24] 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 previous metrics. Taking into consideration the maturity level generated from the previous metrics 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 anticipates that the implementation of the DHS's Continuous Diagnostic and Mitigation solution will improve its configuration management program. In the meantime, the IRS has made some improvements. In January 2016, the IRS implemented automated scanning of its firewall,

[22] A group of qualified people with responsibility 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.

[23] TIGTA, Ref. No. 2017-20-029, *The Big Data Analytics General Support System Security Controls Need Improvement* (June 2017).

[24] GAO, GAO-17-454R, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Internal Control over Financial Reporting* (May 17, 2017).

router, and switches that updates a dashboard daily with compliance data. Also, the IRS has begun implementing components of IBM BigFix, which is being deployed as part of the DHS's Continuous Diagnostic and Mitigation solution.

Function 2b: PROTECT – Identity and Access Management

Function	Count
Ad-Hoc	**0**
Defined	**3**
Consistently Implemented	**5**
Managed and Measurable	**1**
Optimized	**0**
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?

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

    Comments: The IRS indicated that, while it has resources to implement the ICAM, it has identified certain activities that would benefit from increased resources which would better support improved process efficiency and effectiveness.

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 IRS utilizes the Treasury Enterprise Identity Credential and Access Management 3–5 Year Roadmap to guide its ICAM initiatives and identify gaps.

25. To what degree have ICAM policies and procedures been defined and implemented? (Note: The maturity level should take into consideration the maturity of metrics 27 through 31)?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its policies and procedures for the ICAM, including for account management, separation of duties, least privilege, remote access management, identifier and authenticator management, and identification and authentication of non-organizational users. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policies, procedures, and processes to update the program.

Comments: The IRS follows the Department of the Treasury's policies and procedures for the ICAM as set forth in the Treasury Enterprise Identity, Credential, and Access Management 3–5 Year Roadmap.

26. To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems?

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

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) who access its systems are completed and maintained?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. The organization utilizes more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate.

    Comments: This is the highest level for this metric.

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

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

    Comments: The IRS has completed e-authentication risk assessments for 28 of its online applications, but only six of the 28 reassessed applications are currently using an appropriate level of assurance to authenticate users.

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

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

Comments: While the IRS reported that 100 percent of its privileged users are required to use PIV cards to access the IRS network, it reported that only eight of 136 internal systems are configured to require PIV cards. Therefore, it did not meet the managed and measurable maturity level for this metric.

30. To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed?

    Maturity Level: **Defined (Level 2)** – The organization has defined its processes for provisioning, managing, and reviewing privileged accounts. Defined processes cover approval and tracking, inventorying and validating, and logging and reviewing privileged users' accounts.

    Comments: In FY 2017, the GAO reported[25] that numerous authorization control deficiencies still exist in the IRS's computing environment, including not restricting system access based on "least privilege." The GAO reported that the IRS assigned database privileges to individual accounts instead of assigning the privileges to a specific role and that the IRS did not enable database logging, nor did it review, analyze, or report auditable and actionable events on a database supporting a tax payment system. The IRS plans to use the Continuous Diagnostic and Mitigation Phase 2 privilege management solution to enhance its privileged management process.

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

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

    Comments: The IRS has not implemented encryption compliant with Federal Information Processing Standard Publication 140-2 on all its remote access connections.

32. Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the previous metrics. Taking into consideration the maturity level generated from the previous metrics

[25] GAO, GAO-17-395, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 26, 2017).

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.

Function 2c: PROTECT – Security Training

Function	Count
Ad-Hoc	**0**
Defined	**0**
Consistently Implemented	**1**
Managed and Measurable	**5**
Optimized	**0**
Function Rating: Managed and Measurable (Level 4)	

33. 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 organizationwide security awareness and training program as well as the awareness and training–related roles and responsibilities of system users and those with significant security responsibilities?

    Maturity Level: **Managed and Measurable (Level 4)** – The organization has assigned responsibility for monitoring and tracking the effectiveness of security awareness and training activities. Staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures on the effectiveness of security awareness and training activities.

34. To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?

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

Comments: The IRS has not yet addressed all of its identified knowledge, skills, and abilities gaps.

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

36. 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 metrics 37 and 38.)

    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.

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

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

38. 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/or disciplinary actions, as appropriate.

39. Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the previous metrics. Taking into consideration the maturity level generated from the previous metrics 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 33 through 38, 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 3: DETECT – ISCM

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

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

Maturity Level: **Consistently Implemented (Level 3)** – The organization's ISCM strategy is consistently implemented at the organization/business process and information levels. In addition, the strategy supports clear visibility 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 did not provide information to support that the organization monitors and analyzes qualitative and quantitative measures on the effectiveness of its ISCM strategy.

41. To what extent does the organization utilize ISCM policies and procedures to facilitate organizationwide, 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; collecting security-related information required for metrics, assessments, and reporting; analyzing ISCM data; reporting findings; and reviewing and updating the ISCM strategy?

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 ISCM policies and procedures.

Comments: The IRS did not provide information to support that the organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies and procedures and makes updates as appropriate.

42. 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 structures of its ISCM team, roles and responsibilities of ISCM stakeholders, and levels of authority and dependencies.

Comments: The IRS is in the process of establishing a cybersecurity training plan to follow NIST Special Publication 800-181, *National Institute for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (August 2017). The *National Institute for Cybersecurity Education Framework* serves as a fundamental reference resource to support a workforce capable of meeting an organization's cybersecurity needs. It provides organizations with a common, consistent lexicon that categorizes and describes cybersecurity work. The framework contains seven categories, which are broken down into 30 specialty areas. The IRS Cybersecurity organization has developed a draft training plan with the next step to map Cybersecurity organization employees to the *National Institute for Cybersecurity Education Framework* and to make targeted training recommendations.

43. 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 utilizes the results of security control assessments and monitoring to maintain ongoing authorizations of information systems.

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

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

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

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

Maturity Level: **Consistently Implemented (Level 3)** – Based on the performance results for metrics 40 through 44, 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 4: RESPOND – Incident Response

Function	Count
Ad-Hoc	**0**
Defined	**1**
Consistently Implemented	**2**
Managed and Measurable	**3**
Optimized	**1**
Function Rating: Managed and Measurable (Level 4)	

46. 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 metrics 48 through 52.)

Maturity Level: **Defined (Level 2)** – The organization's incident response policies, procedures, plans, and strategies have been defined and communicated. In addition, the organization has established and communicated an enterprise-level incident response plan.

Comments: The IRS did not provide sufficient information to support that it is consistently capturing and sharing lessons learned, preventing it from achieving a *Consistently Implemented* maturity level 3.

47. 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.

48. 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 information to support that it maintains a comprehensive baseline of network operations and expected data flows for users and systems, which prevented it from achieving a *Managed and Measurable* maturity level 4.

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

    Maturity Level: **Optimized (Level 5)** – The organization utilizes dynamic reconfiguration (*e.g.*, changes to router rules, access control lists, and filter rules for firewalls and gateways) to stop attacks, misdirect attackers, and isolate components of systems.

50. 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.

51. 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 and enter into contracts, as appropriate, for incident response support?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently utilizes on-site technical assistance/surge capabilities offered by the 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 is utilizing the DHS's Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its network.

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

52. To what degree does the organization utilize the following technology to support its Incident Response program?

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

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

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

Maturity Level: **Managed and Measurable (Level 4)** – Based on the performance results for metrics 46 through 52, 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 measurable maturity level.

Function 5: RECOVER – Contingency Planning

Function	Count
Ad-Hoc	**0**
Defined	**0**
Consistently Implemented	**2**
Managed and Measurable	**5**
Optimized	**0**
Function Rating: Managed and Measurable (Level 4)	

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

    Maturity Level: **Managed and Measurable (Level 4)** – The organization has assigned responsibility for monitoring and tracking the effectiveness of information system contingency planning activities. Staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures on the effectiveness of information system contingency planning program activities, including validating the operability of an information technology system or system component to support essential functions during a continuity event.

55. 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 metrics 56 through 60.)

    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 communications technology supply chain concerns into its contingency planning policies and procedures, defines and implements a contingency plan for its information and communications technology supply chain infrastructure, applies appropriate information and communications 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.

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

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

57. 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.

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

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

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

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 a redundant array of independent disks, as appropriate. Alternate processing and storage sites are chosen based upon risk assessments which ensure that the potential disruption of the organization’s ability to initiate and sustain operations is minimized, and these sites 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: This is the highest possible rating for this metric.

60. 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.

61. Provide any additional information on the effectiveness (positive or negative) of the organization’s contingency planning program that was not noted in the previous metrics. Taking into consideration the maturity level generated from the previous metrics 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 54 through 60, this function was evaluated at a maturity level 4, *Consistently Implemented.*

Comments: The IRS Contingency Planning program is effective because overall it met the managed and measurable maturity level.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the effectiveness of the IRS's information security program, procedures, and practices and its compliance with FISMA requirements for the period July 1, 2016, to June 30, 2017. To accomplish our objective, we determined the maturity level for the metrics contained in the FY 2017 Inspector General FISMA Reporting Metrics (embedded in Appendix I) that pertain to the seven security program areas.

As instructed in the Reporting Metrics document, we determined the overall rating for each of the seven domains by a simple majority, by which 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 of the metrics, then the domain rating would be *Managed and Measurable*. However, we also considered agency-specific factors when determining final ratings, as instructed by the FY 2107 Inspector General FISMA Reporting Metrics. Inspectors General were required to provide comments explaining the rationale for why a given metric was rated lower than a maturity level 4, *Managed and Measurable*. The Treasury Office of the 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 IRS's Risk Management program.

II. Determine the effectiveness of the IRS's Configuration Management program.

III. Determine the effectiveness of the IRS's Identity and Access Management program.

IV. Determine the effectiveness of the IRS's Security Training program.

V. Determine the effectiveness of the IRS's ISCM program.

VI. Determine the effectiveness of the IRS's Incident Response program.

VII. Determine the effectiveness of the IRS's Contingency Planning program.

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

For the specific metrics within each program area, see the FY 2017 Inspector General FISMA Reporting Metrics embedded below:

PDF

Final FY 2017 OIG
FISMA Metrics v1.0 - !

We based our evaluation work, in part, on a representative subset of seven major IRS information systems. To select the representative subset of the IRS information systems, TIGTA follows the selection methodology that the Treasury Office of the Inspector General defined for the Department of the Treasury as a whole. We used the system inventory contained within the Treasury FISMA Information Management System of general support systems and major 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 reselect for that system.

We also considered the results of TIGTA audits performed or completed during the FY 2017 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
Jody Kitazono, Audit Manager
Midori Ohno, Lead Auditor
Bret Hunter, Senior Auditor
Steven Stephens, Senior Auditor
Esther Wilson, Senior Auditor
Linda Cieslak, 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 2017 Evaluation Period

1. TIGTA, Ref. No. 2017-2R-079, *Cybersecurity Act of 2015: Report on the Information Security Management Practices of the Internal Revenue Service* (Aug. 2016).
2. TIGTA, Ref. No. 2017-20-004, *Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners* (Oct. 2016).
3. TIGTA, Ref. No. 2017-20-024, *Information Technology: Improvements Are Needed in Enterprise-Wide Disaster Recovery Planning and Testing* (June 2017).
4. TIGTA, Ref. No. 2017-20-029, *The Big Data Analytics General Support System Security Controls Need Improvement* (June 2017).
5. 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).
6. TIGTA, Ref. No. 2017-20-049, *Analysis of Fiscal Year 2016 Additional Appropriations for Cybersecurity and Identity Theft Prevention Improvements* (Aug. 2017).
7. TIGTA, Ref. No. 2017-20-050, *The Computer Security Incident Response Center Is Preventing, Detecting, Reporting, and Responding to Incidents, but Improvements Are Needed* (Aug. 2017).
8. TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017).
9. TIGTA, Ref. No. 2017-20-062, *The Internal Revenue Service Is Not in Compliance With Federal Requirements for Software Asset Management* (Sept. 2017).
10. GAO, GAO-17-140, *Financial Audit: IRS's Fiscal Years 2016 and 2015 Financial Statements* (Nov. 10, 2016).
11. GAO, GAO-17-395, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 26, 2017).
12. GAO, GAO-17-454R, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Internal Control over Financial Reporting* (May 17, 2017).

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