Audit Report

OIG-16-010

INFORMATION TECHNOLOGY: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2015 Performance Audit

November 12, 2015

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

November 12, 2015

MEMORANDUM FOR BRODI FONTENOT
ASSISTANT SECRETARY FOR MANAGEMENT

SANJEEV "SONNY" BHAGOWALIA
DEPUTY ASSISTANT SECRETARY FOR INFORMATION SYSTEMS AND CHIEF INFORMATION OFFICER

FROM: Tram J. Dang /s/
Director, Information Technology Audit

SUBJECT: Audit Report – *Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2015 Performance Audit*

We are pleased to transmit the following reports:

- *Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2015 Performance Audit*, dated November 11, 2015; and the

- *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2015*, dated September 25, 2015

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), an independent certified 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). Appendix III of the attached KPMG draft report includes *The Department of the Treasury's Consolidated Response to DHS's FISMA 2015 Questions for Inspectors General*. 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.

In brief, KPMG reported that, consistent with applicable FISMA requirements, OMB policy and guidance, and the National Institute of Standards and Technology standards and guidelines, Treasury's information security program and practices for its unclassified systems were established and have been maintained for the 10 FISMA program areas. However, the program was not fully effective in 4 of the 10 FISMA program areas. Accordingly, KPMG made 24 recommendations to the responsible officials to address the identified deficiencies.

With respect to IRS's unclassified systems, TIGTA reported that IRS's information security program generally complied with FISMA requirements. However, it found that 3 security program areas failed to meet FISMA requirements overall due to not meeting many of the performance attributes specified by the DHS.

If you have any questions or require further information, you may contact me at (202) 927-5171 or Larissa Klimpel, Manager, Information Technology Audit, at (202) 927-0361.

Attachments

cc: Terry Bartlett
Acting Associate Chief Information Officer,
Cyber Security

ATTACHMENT 1

Department of the Treasury
Federal Information Security Modernization Act
Fiscal Year 2015 Performance Audit
November 11, 2015

THIS PAGE INTENTIONALLY LEFT BLANK

Department of the Treasury
Federal Information Security Modernization Act
Fiscal Year 2015 Performance Audit

November 11, 2015

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

Department of the Treasury
Federal Information Security Modernization Act Fiscal Year 2015 Performance Audit

Table of Contents

FISMA Performance Audit Report

BACKGROUND 4
Federal Information Security Modernization Act of 2014 (FISMA) 4
Department of the Treasury Bureaus/Offices (Bureaus) 4
Department of the Treasury Information Security Management Program 5
OVERALL AUDIT RESULTS 8
FINDINGS 9
1. Logical account management activities were not compliant with policies at CDFI Fund, DO, Fiscal Service, and Mint 9
2. CDFI Fund, Mint, and OCC 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 10
3. TTB's security program policy and procedures were not consistent with the NIST SP 800-53, Rev. 4 security controls 12
4. POA&Ms were not tracked in accordance with NIST and Treasury requirements at DO and FinCEN 12
5. Mint's contract with their third-party cloud service provider did not address FedRAMP requirements. 14
SELF-IDENTIFIED WEAKNESSES 15
MANAGEMENT RESPONSE TO THE REPORT 19

Appendices

APPENDIX I – OBJECTIVES, SCOPE, AND METHODOLOGY 28
APPENDIX II – STATUS OF PRIOR-YEAR FINDINGS 31
APPENDIX III – DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS's FISMA 2015 QUESTIONS FOR INSPECTORS GENERAL 48
APPENDIX IV – APPROACH TO SELECTION OF SUBSET OF SYSTEMS 62
APPENDIX V – GLOSSARY OF TERMS 64

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 2015 Performance Audit

Dear Mr. Thorson:

This report presents the results of our independent audit of the Department of the Treasury's (Treasury) information security program and practices for its unclassified systems. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the Treasury, to have an annual independent evaluation performed of their information security programs and practices to determine effectiveness of such programs and practices, and to report the results of the evaluations to the Office of Management and Budget (OMB). The Department of Homeland Security (DHS) is responsible for the operational aspects of Federal cyber security, such as establishing government-wide incident response and operating CyberScope to collect FISMA metrics. Appendix III, *Department of the Treasury's Consolidated Response to DHS's FISMA 2015 Questions for Inspectors General,* dated June 19, 2015 provides the Treasury's response to the CyberScope questionnaire. FISMA requires that the agency Inspector General (IG) or an independent external auditor perform the annual evaluation as determined by the IG. The Treasury Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct an audit of Treasury's information security program and practices for its unclassified systems.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives for this audit were to assess the effectiveness of Treasury's information security program and practices for the period July 1, 2014 to June 30, 2015 for its unclassified systems, and to evaluate Treasury's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We based our work, in part, on a sample of bureau and office-wide security controls and a limited selection of system-specific security controls across 15-selected Treasury information systems. The scope of our work did not include the Internal Revenue Service (IRS), as that bureau was evaluated by the Treasury Inspector General for Tax Administration (TIGTA). The TIGTA report is appended to this report and the findings are included in Appendix III, *Department of the Treasury's Consolidated Response to DHS's FISMA 2015 Questions for Inspectors General*. Additional details regarding the scope of our independent 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. Appendix V contains a glossary of terms used in this report.

Consistent with applicable FISMA requirements, OMB policy and guidance, and the National Institute of Standards and Technology (NIST) standards and guidelines, the Treasury's information security program and practices for its unclassified systems were established and have been maintained for the 10 FISMA program areas.[1] However, the program was not fully effective as reflected in the 5 findings within 4 of the 10 FISMA program areas that we identified during fieldwork:

1. Logical account management activities were not compliant with policies at the Community Development Financial Institutions (CDFI) Fund, Departmental Offices (DO), the Bureau of the Fiscal Service (Fiscal Service), and the United States Mint (Mint). (Identity and Access Management)
2. CDFI Fund, Mint, and the Office of the Comptroller of the Currency (OCC) did not implement all of the NIST Special Publication (SP) 800-53, Revision (Rev.) 4, security controls for some of their System Security Plans (SSPs) and ensure completeness in accordance with NIST guidance. (Risk Management)
3. Alcohol and Tobacco Tax and Trade Bureau's (TTB) security program policy and procedures were not consistent with the NIST SP 800-53, Rev. 4 security controls. (Risk Management)
4. Plan of Action & Milestones (POA&Ms) were not tracked in accordance with NIST and Treasury requirements at DO and Financial Crimes Enforcement Network (FinCEN). (POA&Ms)
5. Mint's contract with their third-party cloud service provider (CSP) did not address Federal Risk and Authorization Management Program (FedRAMP) requirements. (Contractor Systems)

We made 24 recommendations related to these control deficiencies that, if effectively addressed by management, should strengthen the respective bureaus, offices, and Treasury's information security program. In a written response, the Treasury 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. Management also indicated corrective actions for some recommendations were completed. We will follow up on the status of all corrective actions as part of the FY 2016 independent evaluation.

During our audit, we noted some bureaus and offices self-identified weaknesses in NIST SP 800-53 Rev. 4 controls and documented them in 26 POA&Ms. We reviewed the self-identified weaknesses and noted that each POA&M had adequate corrective action plans established, 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.

[1] As described in the DHS' *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics Version 1.2*, the 10 FISMA program areas are: continuous monitoring management, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, and contractor systems.

Sincerely,

KPMG LLP

November 11, 2015

BACKGROUND

Federal Information Security Modernization Act of 2014 (FISMA)

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 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 IG or an independent external auditor as determined by the IG.

Department of the Treasury Bureaus/Offices (Bureaus)

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

1. **Alcohol and Tobacco Tax and Trade Bureau (TTB) –** Responsible for enforcing and administering laws covering the production, use, and distribution of alcohol and tobacco products. TTB also collects excise taxes for firearms and ammunition.
2. **Bureau of Engraving and Printing (BEP) –** Designs and manufactures United States paper currency, securities, and other official certificates and awards.
3. **Bureau of the Fiscal Service (Fiscal Service) –** A composition of the legacy Bureau of the Public Debt (BPD) who was responsible for borrowing public debt, and the legacy Financial Management Service (FMS), which received and disbursed all public monies, maintained government accounts, and prepared daily and monthly reports on the status of government finances.
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 Council, 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.

6. **Financial Crimes Enforcement Network (FinCEN) –** Supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes. It also provides United States policy makers with strategic analyses of domestic and worldwide trends and patterns.
7. **Internal Revenue Service (IRS) –** Responsible for determining, assessing, and collecting internal revenue in the United States.
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 the Special Inspector General for TARP. 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. **Special Inspector General for the Troubled Asset Relief Program (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.

The scope of our 2015 FISMA audit did not include the IRS, which 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 2015 Questions for Inspectors General*.

Department of the Treasury Information Security Management Program

Treasury Office of the Chief Information Officer (OCIO)

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, Treasury Directive Publication (TD P) 85-01 Volume I, *Treasury Information Technology Security Program*, 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 Cyber Security Program have responsibility to interpret and release updated policy for the Treasury. The ACIOCS and the 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 Treasury CIO and bureau-level CIOs. The CIOs are responsible for managing the IT security program for their bureau, as well as advising the bureau head on significant issues related to the bureau IT security program. The CIOs also have the responsibility for overseeing the development of procedures that comply with the Treasury OCIO's policy and guidance and federal statutes, regulations, policy, and guidance. The bureau Chief Information Security Officers (CISO) are tasked by their respective CIOs to serve as the central point of contact for the bureau's IT

security program, as well as to develop and oversee the bureau's IT security program. This includes the development of policies, procedures, and guidance required to implement and monitor the bureau IT security program.

Department of the Treasury – Bureau OCIO Collaboration

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

OVERALL AUDIT RESULTS

Consistent with applicable FISMA requirements, OMB policy and guidance, and the National Institute of Standards and Technology (NIST) standards and guidelines, the Treasury's information security program and practices for its unclassified systems were established and have been maintained for the 10 FISMA program areas. The FISMA program areas are outlined in the *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics Version 1.2* and were prepared by U.S. Department of Homeland Security (DHS) Office of Cybersecurity and Communications Federal Network Resilience. The 10 program areas are continuous monitoring management, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, and contractor systems.[2] 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 5 findings within 4 of the 10 FISMA program areas. We have made 24 recommendations related to these control deficiencies that, if effectively addressed by management, should strengthen the respective bureaus, offices, and Treasury's information security program. The *Findings* section of this report presents the detailed findings and associated recommendations. We noted 35 self-identified control weaknesses by 5 bureaus, which are in the *Self-Identified Weakness* section of the report. In a written response to this report, the Treasury Deputy Assistant Secretary for Information Systems and CIO agreed with our findings and recommendations and provided corrective action plans (see *Management Response*). Treasury's planned corrective actions are responsive to the intent of our recommendations. Management also indicated corrective actions for some recommendations were completed. We will follow up on the status of all corrective actions as part of the FY 2016 independent evaluation.

Additionally, we evaluated the prior-year findings from the fiscal year (FY) 2014 and FY 2013 FISMA Evaluation and the FY 2012 and 2011 FISMA Evaluation as a performance audit and noted that management had closed 21 of 29 findings. See Appendix II, *Status of Prior-Year Findings*, for additional details.

[2] TIGTA will provide a separate report evaluating the IRS's implementation of the Department of the Treasury's information security program.

FINDINGS

1. Logical account management activities were not compliant with policies at CDFI Fund, DO, Fiscal Service, and Mint

We identified instances of noncompliance with logical access policies at CDFI Fund, DO, Fiscal Service, and Mint. This control falls under the identity and access management FISMA program area. We noted the following:

1. Disabling of user accounts after a defined period of inactivity was not performed as required by TD P 85-01 Volume I, *Treasury Information Technology Security Program*, and bureau-specific policies at CDFI Fund and Fiscal Service.
   - For a selected CDFI Fund system, the associated system security plan (SSP) stated user accounts are disabled after 120 days of inactivity. However, the CDFI Fund IT Security Policy Handbook (CDFI Fund P-910) stated that systems needed to be configured to automatically disable any user account after 90 days of inactivity. In addition, we noted that 9 user accounts had been inactive for more than 120 days and were still enabled within the system. For the selected system, management stated that a thorough review of the updated SSP was not performed to ensure that the SSP was in compliance with the CDFI Fund P-910. Furthermore, the security configurations for disabling inactive users were not appropriately implemented. (*See Recommendations #1 and #2.*)
   - For a selected Fiscal Service system, the system relied on a user account management tool for creating and managing access to system. The user account management tool did not automatically disable 3 inactive users with last login date greater than 120 days. Fiscal Service management indicated there was a programming issue with the account management tool, which caused some inactive user accounts not being disabled after 120 days. This programming issue only affected accounts originally provisioned by the legacy Bureau of the Public Debt user provisioning system (*See Recommendations #3 and #4.*)
2. For a selected DO system, the system was not configured to disable user accounts that have not logged in the system within 90 days. Rather, it uses a password reset configuration as a mitigating control to disable user's accounts who have not reset their passwords within 90 days. However, some system administrators had the "password inactive" setting for their administrator accounts configured to "never," which would only force a password change every 90 days but not lock the account. We noted 7 of the 11 system administrator's accounts that were inactive for more than 90 days were not disabled within the system. In addition, management did not adhere to the account management policies and procedures as documented in the system's SSP as follows:
   - 8 accounts were not documented as service accounts.
   - 4 new user accounts were created prior to obtaining the appropriate approvals.

   DO management was unaware that the mitigating control (i.e., password reset configuration) was not appropriately configured for all users to disable accounts once the password expired. (*See Recommendations #5, #6, #7, and #8.*)
3. 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. (*See Recommendation #9.*)

These control deficiencies demonstrate that these bureaus did not appropriately implement policies for approving and reviewing user access. To the extent that inactive, but not disabled, accounts are present, user accounts have an increased risk of being compromised by unauthorized individuals. Further, by failing to retain evidence of all user and administrator accounts approvals, there is an increased risk that users could have unauthorized access to, and/or modify, production data on their respective systems or the network.

We recommend that CDFI Fund management:

1. For the selected system, update the SSP to require disabling of inactive user accounts after 90 days of inactivity as defined within the CDFI Fund IT Security Policy Handbook.

2. For the selected system, ensure the system is configured to automatically disable user accounts after 90 days of inactivity.

We recommend that Fiscal Service management:

3. For the selected system, develop or acquire additional system capability to automatically disable user accounts that have been inactive for more than 120 days.

4. For the selected system, in the absence of a long-term system capability solution, perform manual monthly reviews of all system user accounts and disable or delete accounts that no longer need access.

We recommend that DO management:

5. For the selected system, review the password reset configuration settings for all users on the servers to ensure they are configured to automatically disable user accounts who has not reset their passwords within 90 days.

6. For the selected system, perform a review/analysis of the administrative accounts for the system to validate no enabled accounts have gone unused for more than 90 days.

7. For the selected system, ensure all accounts are appropriately identified.

8. For the selected system, ensure the policies and procedures in place for appropriately approving and granting system access for new user accounts is followed.

We recommend that Mint management:

9. For the selected system, ensure access forms are completed, properly reviewed by the help desk prior to granting access, and centrally retained by the help desk.

2. CDFI Fund, Mint, and OCC 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

OMB Memorandum 14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, requires agencies to be compliant with NIST standards and guidelines within 1 year of the publication date unless otherwise directed by

OMB. NIST SP 800-53, Rev. 4, was released in April 2013 with an expected implementation date for all legacy information systems by April 2014. NIST and Treasury guidance require that Treasury SSPs remain up-to-date and current with the NIST Risk Management Framework and require the latest NIST Special Publication (SP) 800-53 security controls. This control falls under the risk management FISMA program area. We noted the following:

- CDFI Fund's SSP for the selected system did not comply with all required NIST SP 800-53 Rev. 4 controls and enhancements. We noted either 12 controls and 21 control enhancements were missing or the implementation descriptions of the controls were not documented. Although the SSP was not compliant, we noted that the annual assessment for system was performed based on the updated NIST SP 800-53 Rev. 4. CDFI Fund management indicated a thorough review of the updated SSP was not performed. As such, all NIST SP 800-53 Rev. 4 applicable controls and control enhancements for this system were not included. (*See Recommendation #10.*)
- 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. (*See Recommendations #11 and #12.*)
- OCC's SSP for the selected system did not address all required NIST SP 800-53 Rev. 4 controls, enhancements, and implementation descriptions. We noted 22 controls and 12 control enhancements did not fully address NIST SP 800-53 Rev. 4 controls. Furthermore, two control enhancements were missing from the SSP. OCC management indicated there were limitations in the application used to generate the SSP template and it did not include NIST SP 800-53 Rev. 4 controls, control enhancements, and implementation statuses. *(See Recommendation #13.*)

Failing to document an up-to-date baseline of security controls in the SSP may have a negative effect on subsequent security activities. Specifically, the bureaus and offices may not be able to implement, assess, authorize, and monitor the required NIST SP 800-53, Rev. 4, controls properly for the selected systems; therefore, the system security controls may not be sufficient to protect the confidentiality, integrity, and availability of sensitive bureau information.

We recommend that CDFI Fund management:

10. For the selected system, update the SSP to address and reference NIST SP 800-53 Rev. 4 controls and control enhancements, and ensure that the implementation description is specified for each control.

We recommend that Mint management:

11. 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.

12. 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.

We recommend that OCC management:

13. For the selected system, update the SSP to address and reference NIST SP 800-53 Rev. 4 controls, control enhancements, and ensure that the implementation description is specified for each control.

3. TTB's security program policy and procedures were not consistent with the NIST SP 800-53, Rev. 4 security controls

The TD P 85-01 requires Treasury bureaus to ensure their policies and procedures are updated and reviewed to reflect the latest NIST guidance. This control falls under the risk management FISMA program area. Specifically, we noted the TTB security program policy and procedures incorrectly reference controls from the outdated NIST SP 800-53 Rev. 4 initial public draft version, dated February 2012. The policies and procedures do not include all required controls and control enhancements from the NIST SP 800-53 Rev. 4 final version, dated April 2013. We noted that 63 controls did not meet NIST SP-800-53 Rev. 4 requirements or were missing all, or part, of the control. TTB management indicated they were not aware that the security program policy and procedures did not address final NIST SP 800-53 Rev. 4 controls. (*See Recommendation #14.*)

Having policies not updated to reflect the most current NIST SP 800-53 publications, could result in insufficient guidance to protect the confidentiality, integrity, and availability of information maintained by the bureau's systems.

We recommend that TTB management:

14. Review and update the TTB security program policy and procedures to include all relevant controls and control enhancements procedures in the NIST SP 800-53 Rev. 4 final version.

4. POA&Ms were not tracked in accordance with NIST and Treasury requirements at DO and FinCEN

TD P 85-01 Volume I requires Treasury bureaus and offices to maintain POA&Ms in order to help remedy weaknesses identified through audits, security assessments, and other risk management activities. POA&Ms document the responsible parties, time frames for mitigation, and necessary resources. This control falls under the POA&M FISMA program area. We noted the following:

- DO management did not document and track progress towards remediating existing POA&Ms and did not close POA&Ms by the established due date as documented in the POA&Ms for two selected systems. DO management had a total of 15 POA&Ms for one selected system and 6 POA&Ms for the other selected systems. None of the past due POA&Ms were updated with revised due dates or with any description in the "Status Comment" field explaining why they had not been closed. We also noted that there were seven closed POA&Ms for the first selected system did not include a remediation plan to describe the steps taken. DO Management indicated that due to competing priorities, DO management did not place emphasis on monitoring and closing POA&Ms on a timely basis. In cases where original POA&M due dates were not met

management also did not revise the due dates or enter an explanation in the "Status Comment" field to explain why the original due date was missed. (*See Recommendations #15, #16, and #17 for the first system, and Recommendations #18 and #19 for the second system.*)

- FinCEN management did not monitor progress towards remediating existing POA&Ms and did not close POA&Ms by the established milestones. As of June 30, 2015, FinCEN management had a total of 14 POA&M items that were past due and were not updated or provided with a justification for why they have not been closed. In addition, the selected system's POA&M report did not adequately outline the remedial actions with updated dates or the remediation plan. FinCEN management indicated that it is currently overhauling the system and that rather than spend limited resources fixing the old system, the POA&Ms will be addressed when the new system undergoes a formal security accreditation and authorization process. (*See Recommendations #20 and #21.*)

By not remediating known security control weaknesses and vulnerabilities in a timely fashion, systems could be vulnerable to unauthorized access, disclosure, and/or modification. Moreover, by not updating the status of past due milestones for identified system security vulnerabilities in their POA&M, Treasury bureaus' summary-level security metrics incorrectly report the true status of known security weaknesses to the Treasury OCIO. Additionally, senior Treasury management would be unable to adjust funding levels, human resources, and requested priorities in response to identified security weaknesses.

We recommend that DO management:

15. For the first selected system, ensure that the POA&Ms are being monitored according to NIST guidance.

16. For the first selected system, ensure POA&Ms are updated with revised milestones and provide adequate justification for missed remediation dates.

17. For the first selected system, ensure POA&Ms document the remedial actions taken to correct the weaknesses or deficiencies for which the POA&M was created.

18. For the second selected system, ensure that the selected system's POA&Ms are remediated and updated according to NIST guidance.

19. For the second selected system, ensure POA&Ms are updated with revised milestones and provide adequate justification for missed remediation dates.

We recommend that FinCEN management:

20. For the selected system, ensure that the POA&Ms are being monitored according to NIST guidance.

21. For the selected system, ensure POA&Ms are remediated accordingly with established milestones. If POA&Ms are not remediated, then POA&Ms should be updated with an adequate justification.

5. Mint's contract with their 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.

(*See Recommendations # 22, #23, and #24.*)

Mint management indicated though the system's contract includes requirements for compliance with FISMA, as well as high level monitoring with regard to incident response. However, it does not address FedRAMP requirements, which include stipulations for the CSP to provide monthly scan reports to the agency Information System Security Officer (ISSO). Additionally, Mint management communicated the May 1, 2015 deadline of the finalized CP Plan to the CSP as stated within the Authority to Operate (ATO) memo; however, the CSP provided a Disaster Recovery Plan (DRP) instead. The Mint informed the CSP that a DRP was not satisfactory and that a CP Plan was required.

Without including FedRAMP requirements in the CSP contract, Mint is unable to effectively monitor the CSP to ensure that FedRAMP requirements are being enforced. This could result in potential unauthorized access to data, data breach, and/or critical management decisions based on incorrect, invalid, or inconsistent data.

We recommend that Mint management:

22. 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.

23. For the selected system, ensure that third-party CSP provides FISMA-related artifacts to demonstrate FISMA compliance to the Mint security compliance team.

24. For the selected system, remind the Mint contracting officer to ensure FedRAMP contract-specific clauses regarding compliance with FISMA and NIST are in place.

SELF-IDENTIFIED WEAKNESSES

During the FY 2015 Treasury FISMA performance audit, we noted 1 BEP system, 3 DO systems, 1 Fiscal Service System, 1 Mint System, and 1 OCC system had in aggregate, 35 NIST SP 800-53 Rev. 4 controls that had self-identified weaknesses associated with 26 open POA&Ms. 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.

FY15 FISMA Self-Identified Weaknesses – Department of the Treasury

Bureau	System	NIST SP 800-53 Control	Weakness
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 #R4001 (enterprise-wide): The system implementation for NIST SP 800-53 Rev. 4 is incomplete.
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.
	DO System #1	CM-6	POA&M #7788: System does not meet 90% compliance with the Center for Internet Security (CIS) Benchmark for its Linux servers
	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
	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.

Bureau	System	NIST SP 800-53 Control	Weakness
			POA&M #7328: The application can support authentication of Government employees via their PIV Card, but this capability isn't used.
	DO System #1	AU-2	POA&M #7412: The SSP doesn't identify what security events captured by the OS, Database and application and how the list of audited events support incident response efforts. Database auditing limited to capturing account logon/logoff.
	DO System #1	AU-6	POA&M #7413: Application logs are not forwarded to the centralized log server for automated review, analysis and reporting.
	DO System #2	AC-2	POA&M #584: AC-2: Although accounts are reviewed on an annual basis, quarterly audits are not performed. In addition, the system does not automatically audit account management functions.
	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. POA&M #6149: CM-2: Previously documented versions of baseline configurations are not documented.
	DO System #2	CM-6	POA&M #578: CM-6: The system does employ any automated means to validate the configurations are maintained on a continual basis.
	DO System #2	IA-2	POA&M #6151: (IA-2) Multi-factor authentication is not implemented. Only username and password are required for administrator accounts.
	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 #8634: SI-2: The system does not have automated mechanisms to track the status of resolution for reported system flaws.
	DO System #3	AU-12	POA&M #7645: No application-level auditing capability for application.
	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.
	DO System #3	CP-9	POA&M #3506: The disaster recovery site was not operational at the time of the assessment. This gives rise to multiple weaknesses: 1) The viability and integrity of backups

Bureau	System	NIST SP 800-53 Control	Weakness
			cannot be ensured or validated; 2) Alternate storage viability cannot be validated; In addition, telecommunication services have not been established because the alternate site is not operational. As a result of this, the system cannot: - Test/examine emergency preparedness - Establish and validate Service Level Agreements (SLAs) - Identify points of failure
Mint	Mint System #1	IA-2	POA&M #111: Two components privileged accounts do not have multifactor authentication enabled. Multifactor authentication supports stronger protections for identity and access of privileged users over remote network access methods such as the Internet as in the case of this application. Exposing application management interfaces publically is generally not best practice and multifactor authentication would lessen the risk of credential compromise due to vulnerabilities in other confidentiality controls.
FS	FS System #1	AC-2 AU-2 AU-6 AU-12	POA&M #3140: The system has neither implemented nor documented a procedure to incorporate the audit data from the General Support System (GSS) pertaining to the security of the system. These data should be reviewed, analyzed, and reported to support incident response. Without sufficient review, analysis, and reporting, security incidents may go undetected. POA&M #3141: The system relies on the GSS to collect audit events. During an observation conducted to review these audit processes, the GSS was unable to produce the logs containing the events noted in the SSP. The inability of the GSS to provide appropriate audit logs to the system will significantly hinder after-the-fact investigations of events and general risk management.
	FS System #1	CA-2	POA&M #8393: 2015 Continuous Monitoring Test Results were not provided for the system for 5/01/14 - 4/30/15.
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.
	OCC System #1	CM-6	POA&M #3741: CM-6 Configuration Settings, CM-7 Least Functionality

Bureau	System	NIST SP 800-53 Control	Weakness
			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.

MANAGEMENT RESPONSE TO THE REPORT

The following is the Treasury CIO's response, dated November 9, 2015, to the FY 2015 FISMA Performance Audit Report.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

November 9, 2015

MEMORANDUM FOR TRAM J. DANG
DIRECTOR, INFORMATION TECHNOLOGY AUDIT

FROM: Sanjeev "Sonny" Bhagowalia /s/
Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO)

SUBJECT: Management Response to Final Evaluation Report – "Fiscal Year 2015 Audit of Treasury's Compliance with Federal Information Security Modernization Act"

Thank you for the opportunity to comment on the report entitled, *Fiscal Year 2015 Audit of Treasury's Compliance with the Federal Information Security Modernization Act [FISMA]*. We are pleased that the report states that our security program is consistent with FISMA requirements, the Office of Management and Budget (OMB) information security policy, and related information security standards and guidance published by the National Institute of Standards and Technology (NIST). We have carefully reviewed the report 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 of those Bureaus' 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.

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:

- Enhanced the Treasury's Information Technology Security Program policy to address the increasing sophistication of cyber-attacks and the operations tempo of adversaries across multiple threat areas by integrating state-of-the-practice security controls and control enhancements into the policy.

- Published the Treasury Information Security Continuous Monitoring (ISCM) Framework, which enables the adoption of ISCM in accordance with the OMB M 14-03 in a manner that allows for both a uniform adoption of ISCM while still allowing for bureau-level customization of their respective ISCM approaches.

- Drastically improved adoption of required Personal Identity Verification (PIV) credential authentication to Treasury networks (98% for general users and 100% for privileged users).

- Completed an initial identification and security review of Treasury's High Value Assets as required by OMB.

- Overhauled the Cyber Critical Infrastructure Protection (CIP) Program to better align support for Mission Essential Functions with designation as a Cyber Critical Infrastructure Asset.

- Achieved an Initial Operating Capability of a Data Loss Prevention (DLP) solution at two Fiscal Service-operated Trusted Internet Connections (TICs).

- Reached Maturity Level-1 thresholds in all five areas assessed in the President's Management Council (PMC) Cybersecurity Assessment, and achieved Maturity Level-2 in one of five areas.

- Protected 100 percent of remote access connections with FIPS 140-2 validated encryption, 30-minute activity timeouts, and prohibition of split tunneling.

- Provided data-at-rest encryption on 99.5 percent of mobile IT devices.

We appreciate the audit recommendations because they will help improve our security posture. If you have any questions, please contact Patricia Black, Associate CISO for Cyber Security, at 202-622-2056.

Attachment

cc: Patricia Black

Management Response to KPMG Recommendations

KPMG Finding 1: Logical account management activities were not compliant with policies at CDFI Fund, DO, Fiscal Service, and U.S. Mint.

KPMG Recommendation 1: We recommend that CDFI Fund management: For the selected system, update the SSP to require disabling of inactive user accounts after 90 days of inactivity as defined within the CDFI Fund IT Security Policy handbook**.**

> **Treasury's Response:** Treasury agrees with the finding and recommendation. CDFI Fund has updated the system SSP to require disabling of inactive user accounts after 90 days of inactivity as defined within the CDFI Fund IT Security Policy Handbook. The completion date was September 25, 2015.
>
> **Responsible Official:** CDFI Fund, Chief Information Security Officer

KPMG Recommendation 2: We recommend that CDFI Fund management: For the selected system, ensure the system is configured to automatically disable user accounts after 90 days of inactivity.

> **Treasury's Response:** Treasury agrees with the finding and recommendation. TTB/CDFI Fund is currently automatically disabling user accounts after 90 days of inactivity. The competition date was September 25, 2015.
>
> **Responsible Official:** CDFI Fund, Chief Information Security Officer

KPMG Recommendation 3: We recommend that Fiscal Service management: For the selected system, develop or acquire additional system capability to automatically disable user accounts that have been inactive for more than 120 days.

> **Treasury Response:** Treasury agrees with the finding and recommendation. Fiscal Service has revised the software code for the automated script to ensure all accounts for the three remaining applications on the system are disabled after 120 days of inactivity. Evidence to support this will be validated by the Bureau. The target completion date is January 31, 2016.
>
> **Responsible Official:** Fiscal Service, Chief Information Officer

KPMG Recommendation 4: We recommend that Fiscal Service management: For the selected system, in the absence of a long-term system capability solution, perform manual monthly reviews of all system user accounts and disable or delete accounts that no longer need access.

> **Treasury Response:** Treasury agrees with the finding and recommendation. Fiscal Service has completed a review of the accounts to ensure that the automated script has captured 100% of the current population. Fiscal Service will ensure that the automated script used to disable inactive accounts remains current. This will be added as a discussion topic to the Quarterly Infrastructure Planning Meeting covering Fiscal IT and infrastructures so that any change is planned and communicated across the enterprise. The target completion date is March 31, 2016.
>
> **Responsible Official:** Fiscal Service, Chief Information Officer

KPMG Recommendation 5: We recommend that DO management: For the selected system, review the password reset configuration settings for all users on the servers to ensure they are configured to automatically disable user accounts who have not reset their passwords within 90 days.

> **Treasury Response:** Treasury agrees with the finding and recommendation. As part of the continuous monitoring effort Treasury Cyber Security will review/verify (at least twice a year) password reset configurations for all users (privileged) on the system servers to ensure these accounts are configured to automatically disable users who have not reset their passwords within 90 days. The completion date is June 30, 2016.
>
> **Responsible Official:** DO, Chief Information Officer

KPMG Recommendation 6: We recommend that DO management: For the selected system, perform a review/analysis of the administrative accounts for the system to validate no enabled accounts have gone unused for more than 90 days.

> **Treasury Response:** Treasury agrees with the finding and recommendation. As part of the continuous monitoring effort Treasury Cyber Security will review/verify (at least twice a year) password reset configurations for all users (privileged) on the system servers to ensure there are no enabled accounts that are inactive for more than 90 days. The target completion date is June 30, 2016.
>
> **Responsible Official:** DO, Chief Information Officer

KPMG Recommendation 7: We recommend that DO management: For the selected system, ensure all accounts are appropriately identified.

> **Treasury Response:** Treasury agrees with the finding and recommendation. During the account review process, Cyber will verify accounts are appropriately identified. The target completion date is June 30, 2016.
>
> **Responsible Official:** DO, Chief Information Officer

KPMG Recommendation 8: We recommend that DO management: For the selected system, ensure the policies and procedures in place for appropriately approving and granting system access for new user accounts are followed.

> **Treasury Response:** Treasury agrees with the finding and recommendation. Cyber will work closely with the system project team and will review quarterly, new and/or updated system Access Request forms for accurate completion. The completion date is June 30, 2016.
>
> **Responsible Official:** DO, Chief Information Officer

KPMG Recommendation 9: We recommend that Mint management: For the selected system, ensure access forms are completed, properly reviewed by the help desk prior to granting access, and centrally retained by the help desk.

> **Treasury Response:** ISD Compliance will ensure Account Management processes and procedures are reviewed to ensure access forms are completed, properly reviewed by the help desk prior to granting access, and centrally retained by the help desk. The target completion date is January 31, 2016.

Responsible Official: Mint, Chief Information Officer

KPMG Finding 2: CDFI Fund, Mint, and OCC 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.

KPMG Recommendation 10: We recommend that CDFI Fund management:
For the selected system, update the SSP to address and reference NIST SP 800-53 Rev. 4 controls and control enhancements, and ensure that the implementation description is specified for each control.

Treasury Response: Treasury agrees with the finding and recommendation. CDFI Fund has reviewed and updated the system SSP. CDFI Fund has addressed and referenced NIST SP 800-53 Rev. 4 controls and control enhancements, and ensured that the implementation description is specified for each control. The completion date was September 12, 2015.

Responsible Official: CDFI Fund, Chief Information Officer

KPMG Recommendation 11: We recommend that Mint management: 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.

Treasury Response: Treasury agrees with the finding and recommendation. Information Security Division (ISD) will ensure the control implementation statements and statuses for all NIST SP 800-53 Rev. 4 controls and control enhancements are fully addressed in the selected system's SSP. The target completion date is April 13, 2016.

Responsible Official: Mint, Chief Information Officer

KPMG Recommendation 12: We recommend that Mint management: 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.

Treasury Response: Treasury agrees with the finding and recommendation. Information Security Division (ISD) will 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. The target completion date is April 13, 2016.

Responsible Official: Mint, Chief Information Security Officer

KPMG Recommendation 13: We recommend that OCC management: For the selected system, update the SSP to address and reference NIST SP 800-53 Rev. 4 controls, control enhancements, and ensure that the implementation description is specified for each control.

Treasury Response: Treasury agrees with the finding and recommendation. OCC initiated corrective actions to address this gap through the implementation of a Governance, Risk, and Compliance (GRC) application, which is also serving as a foundational capability supporting

OCC's transition to Information System Continuous Monitoring (ISCM) and Ongoing Authorization (OA). The system was brought into production in May 2015, and the selected system's SSP was migrated to the GRC in August 2015. We have verified that each missing control element identified by the auditors was addressed during the migration of the system to the GRC. Remediation was completed on October 6, 2015.

Responsible Official: OCC, Chief Information Security Officer

KPMG Finding 3: TTB's security program policy and procedures were not consistent with the NIST SP 800-53, Rev. 4 security controls.

KPMG Recommendation 14: We recommend that TTB management: Review and update the TTB security program policy and procedures to include all relevant controls and control enhancements procedures in the NIST SP 800-53 Rev. 4 final version.

Treasury Response: Treasury agrees with the finding and recommendation. TTB will incorporate the NIST SP 800-53 revision 4 controls into TTB's policy and procedures. The policy has been updated to reference NIST SP 800-53 revision 4 and is currently undergoing review. Both documents will be finalized by February 1, 2016.

Responsible Official: TTB, Chief Information Security Officer

KPMG Finding 4: POA&Ms were not tracked in accordance with NIST and Treasury requirements at DO and FinCEN.

KPMG Recommendation 15: We recommend that DO management: For the first selected system, ensure that the POA&Ms are being monitored according to NIST guidance.

Treasury Response: Treasury agrees with the finding and recommendation. System management and Treasury Cyber Security Officials will meet monthly until the delayed POA&Ms have been resolved and continue to meet on a quarterly basis thereafter. The target completion date of these actions is June 30, 2016.

Responsible Official: DO, Chief Information Officer

KPMG Recommendation 16: We recommend that DO management: For the first selected system, ensure POA&Ms are updated with revised milestones and provide adequate justification for missed remediation dates.

Treasury Response: Treasury agrees with the finding and recommendation. Treasury will ensure that the reporting system is updated to reflect improved status tracking of POA&Ms to include additional information on any delays and how POA&Ms are corrected. The target completion date is June 30, 2016.

Responsible Official: DO, Chief Information Officer

KPMG Recommendation 17: We recommend that DO management: For the first selected system, ensure POA&Ms document the remedial actions taken to correct the weaknesses or deficiencies for which the POA&M was created.

Treasury Response: Treasury agrees with the finding and recommendation. Treasury will ensure that the reporting system is updated to reflect improved status tracking of POA&Ms to include additional information on any delays and how POA&Ms are corrected. The target completion date is June 30, 2016.

Responsible Official: DO, Chief Information Officer

KPMG Recommendation 18: We recommend that DO management: For the second selected system, ensure that the selected system's POA&Ms are remediated and updated according to NIST guidance.

Treasury Response: Treasury agrees with the finding and recommendation. Treasury will ensure that the reporting system is updated to reflect improved status tracking of POA&Ms to include additional information on any delays and how POA&Ms are corrected. The target completion date is June 30, 2016.

Responsible Official: DO, Chief Information Officer

KPMG Recommendation 19: We recommend that DO management: For the second selected system, ensure POA&Ms are updated with revised milestones and provide adequate justification for missed remediation dates.

Treasury Response: Treasury agrees with the finding and recommendation. Treasury will ensure that the reporting system is updated to reflect improved status tracking of POA&Ms to include additional information on any delays and how POA&Ms are corrected. The target completion date is June 30, 2016.

Responsible Official: DO, Chief Information Officer

KPMG Recommendation 20: We recommend that FinCEN management: For the selected system, ensure that the POA&Ms are being monitored according to NIST guidance.

Treasury Response: Treasury agrees with the finding and recommendation. FinCEN will review the Plan of Action and Milestones for the system based on the FinCEN Information Security Publication – 002.0 for 'Plan of Action and Milestone' procedural guide. Additionally, FinCEN will update the system POA&M with current status and remediation effort. This is planned to be completed by December 30, 2015.

Responsible Official: FinCEN, Chief Information Security Officer

KPMG Recommendation 21: We recommend that FinCEN management: For the selected system, ensure POA&Ms are remediated accordingly with established milestones. If POA&Ms are not remediated, then POA&Ms should be updated with an adequate justification.

Treasury Response: Treasury agrees with the finding and recommendation. FinCEN will review the Plan of Action and Milestones for the system based on the FinCEN Information Security Publication – 002.0 for 'Plan of Action and Milestone' procedural guide. Additionally, FinCEN will update the system POA&M with current status and remediation effort. This is planned to be completed by December 30, 2015.

Responsible Official: FinCEN, Chief Information Security Officer

KPMG Finding 5: Mint's contract with their third-party cloud service provider (CSP) did not address FedRAMP requirements.

KPMG Recommendation 22: We recommend that Mint management: 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.

> **Treasury Response:** Treasury agrees with the finding and recommendation. ISD Compliance will review third-party CSP's contract and ensure the appropriate FedRAMP security clauses and requirements related to FISMA and NIST guidance are incorporated in the contract. The target completion date is March 31, 2016.
>
> **Responsible Official:** Mint, Chief Information Officer

KPMG Recommendation 23: We recommend that Mint management: For the selected system, ensure that third-party CSP provides FISMA-related artifacts to demonstrate FISMA compliance to the Mint security compliance team.

> **Treasury Response:** Treasury agrees with the finding and recommendation. ISD will ensure that third-party CSP provides FISMA-related artifacts to demonstrate FISMA compliance. The target completion date is March 31, 2016.
>
> **Responsible Official:** Mint, Chief Information Officer

KPMG Recommendation 24: We recommend that Mint management: For the selected system, remind the Mint contracting officer to ensure FedRAMP contract-specific clauses regarding compliance with FISMA and NIST are in place.

> **Treasury Response:** Treasury agrees with the finding and recommendation. ISD Compliance will review third-party CSP's contract and ensure the appropriate FedRAMP security clauses and requirements related to FISMA and NIST guidance are incorporated in the contract. ISD will also ensure that third-party CSP provides FISMA-related artifacts to demonstrate FISMA compliance. The target completion date is March 31, 2016.
>
> **Responsible Official:** Mint, Chief Information Officer

APPENDIX I – OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives for this audit were to assess the effectiveness of the Department of the Treasury's (Treasury's) information security program and practices for the period July 1, 2014 to June 30, 2015 for its unclassified systems and to evaluate Treasury's compliance with the Federal Information Security Modernization Act of 2014 (FISMA) and related information security policies, procedures, standards, and guidelines. Specifically, the objectives of this audit were to:

- Perform the annual independent FISMA audit of the Treasury's information security programs and practices.
- Respond to Department of Homeland Security (DHS) FISMA Questions on behalf of the Treasury Office of Inspector General (OIG).
- Follow up on the status of prior-year FISMA findings.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To accomplish our audit objectives, we evaluated security controls in accordance with applicable legislation; Presidential directives; the DHS *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics Version 1.2,* dated June 19, 2015; 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 bureau and office complied with the implementation of these policies and procedures.

We took a phased approach to satisfy the audit's objectives as listed below:

PHASE A: Assessment of Department-Level Compliance

To gain an enterprise-level understanding, we assessed management, policies, and guidance for the overall Treasury-wide information security program per requirements defined in FISMA and DHS *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics Version 1.2*, as well as Treasury guidelines developed in response to FISMA. This included program controls applicable to certification and accreditation, security configuration management, incident response and reporting, security training, plan of action and milestones, remote access, account and identity management, continuous monitoring management, contingency planning, and contractor systems.

PHASE B: Assessment of Bureau and Office Level Compliance

To gain a bureau and office level understanding, we assessed the implementation of the guidance for the 11[3] bureau- and office-wide information security programs according to requirements defined in FISMA and DHS *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metric Version 1.2s*, as well as Treasury guidelines developed in response to FISMA. This included program controls applicable to certification and accreditation, security configuration management, incident response and reporting, security training, plan of action and milestones, remote access, account and identity management, continuous monitoring management, contingency planning, and contractor systems.

[3] TIGTA assessed IRS's bureau-level compliance.

PHASE C: System Level (Select NIST SP 800-53 Rev. 4 Controls)

To gain an understanding of how effectively the bureaus and offices implemented information security controls at the system level, we assessed the implementation of a limited selection of security controls from the NIST SP 800-53, Rev. 4, for a subset of Treasury information systems (see Appendix IV).

We also tested a subset of 15 information systems from a total population of 120 non-IRS major applications and general support systems as of May 29, 2015.[4] Appendix IV, *Approach to Selection of Subset of Systems*, provides additional details regarding our system selection. The subset of systems encompassed systems managed and operated by 9 of 12 Treasury bureaus, excluding IRS, OIG, and TIGTA.[5]

We based our criteria for selecting security controls within each system on the following:

- Controls that were shared across a number of information systems, such as common controls,
- Controls that were likely to change over time (i.e., volatility) and require human intervention, and
- Controls that were identified in prior audits as requiring management's attention.

Other Considerations

In performing our control evaluations, we interviewed key Treasury Office of the Chief Information Officer (OCIO) personnel who had significant information security responsibilities, as well as personnel across the non-IRS bureaus. We also evaluated Treasury's and bureaus' policies, procedures, and guidelines. Lastly, we evaluated selected security-related documents and records, including security assessment and authorization (SA&A) packages, configuration assessment results, and training records.

We performed our fieldwork at Treasury's headquarters offices in Washington, D.C., and bureau locations 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 Office of Management and Budget (OMB). NIST Special Publications provide guidelines that are considered essential to the development and implementation of agencies' security programs.[6] The following is a listing of the criteria used in the performance of the fiscal year (FY) 2015 FISMA performance audit:

NIST FIPS and/or Special Publications

[4] A subset of information systems refers to our approach of stratifying the population of non-IRS Department of the Treasury information system and selecting an information system from each Department of the Treasury bureau, excluding IRS, OIG and TIGTA, rather than selecting a random sample of information systems that might exclude a Treasury bureau. We pulled the inventory again on July 10, 2015 and noted that there were no changes to the inventory.

[5] Our rotational system selection strategy precludes selecting systems reviewed within the past two years. Both of TIGTA's systems were selected in FY 2014 and FY 2013. In FY 2013, OIG's only system was selected. Therefore, we excluded those bureau's systems from our sample selection in FY 2015.

[6] Note (per *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics Version 1.2*): While agencies are required to follow NIST standards and guidance in accordance with OMB policy, there is flexibility within NIST's guidance documents in how agencies apply the guidance. However, NIST Special Publication 800-53 is mandatory because FIPS 200 specifically requires it. 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 FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- NIST FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance- Based Model*
- NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*
- NIST SP 800-60, Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*
- NIST SP 800-70, Rev. 2, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*

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 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*
- OMB Memorandum 15-01, *Fiscal Year 2014 – 2015 Guidance on Improving Federal Information Security and Privacy Management Practices*

Department of Homeland Security

- *DHS FY 2015 Inspector General Federal Information Security Management Act Reporting Metrics Version 1.2*

Treasury Policy Directives

- Treasury Directive Publication (TD P) 15-71, Department of the Treasury Security Manual
- TD P 85-01, Volume I, *Treasury Information Technology Security Program*

APPENDIX II – STATUS OF PRIOR-YEAR FINDINGS

In Fiscal Year (FY) 2015, FY 2012 and FY 2011 we conducted a FISMA Evaluation as a 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 are closed. 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 closed the findings. If there was evidence that the recommendations had been only partially implemented or not implemented at all, we determined the finding to be open.

Prior Year Findings – 2014 Evaluation

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #1 –Bureau of the Fiscal Service (Fiscal Service) Logical account management activities, such as access authorizations, were not in place or not consistently performed.	For a selected Fiscal Service system, Fiscal Service management did not retain supporting documentation of access approval for 1 of 25 administrative accounts. For this selected system, Fiscal Service did not have an effective process to retain evidence of access approval.	We recommend that Fiscal Service management, for the selected system, implement a new process to ensure that all administrative accounts are approved and that evidence of access approval is retained.	**Open** We noted that Fiscal Service has developed a project plan and has set a milestone to create and implement administrative account approval processes for the selected system by June 30, 2016.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #1 –Bureau of the Fiscal Service (Fiscal Service) Logical account management activities, such as access authorizations, were not in place or not consistently performed.	For a selected Fiscal Service System, 9 of 25 new user accounts created were approved by one of the Information System Security Officers (ISSO) prior to the ISSO's official appointment on February 4, 2014, which did not adhere to the system's System Security Plan (SSP). The SSP stipulated that the ISSO approve new users prior to being added to the system. Fiscal Service management indicated when one of the system's ISSOs retired expectantly, they informally designated a new ISSO and gave that individual permission to authorize access to the system.	We recommend that Fiscal Service Management: 1 For the selected system, implement a new process to ensure that all administrative accounts are approved and that evidence of access approval is retained. 2 For the selected system, ensure only authorized approvers grant new user account access. 3 For the selected system, reapprove all existing users under the new process to ensure their access is appropriate.	**Implemented/Closed** We obtained and inspected the SSP and noted that there was a new process to ensure all administrative accounts are approved and that the evidence of the approval is retrained. In addition, we obtained and inspected a list of the selected system's users and sampled 25 new users. We determined that all sampled 25 new users were properly authorized in accordance with the selected system's SSP. We determined that all existing users were approved and their access was appropriate.
Prior Year FY 2014 Finding #1 – Financial Crimes Enforcement Network (FinCEN) Logical account management activities were not in place or not consistently performed.	For a selected FinCEN System, the service desk did not document or retain records for 1 of 21 new user access authorizations to the system selected. FinCEN Management explained that the user account with an access form was created in the system prior to implementation to production, and the account was carried over as a part of management oversight.	We recommend that FinCEN management, for the selected system, ensure access forms are complete, properly reviewed prior to granting access, and centrally retained by the service desk	**Implemented/Closed** We obtained and inspected the selected system's user listing and noted that there were no new users added within the FISMA year. Therefore, we utilized the current FISMA years test work around new users for the FY 2015 selected system and noted that all sampled users were appropriately granted access via the appropriate access forms.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #1 – Office of the Comptroller of the Currency (OCC) Logical account management activities were not in place or not consistently performed.	For a selected OCC System, the Information System Owner inappropriately approved and modified their own elevated role request. OCC management indicated that the system's account management policies and procedures have not been fully developed to address segregation of duties.	We recommend that OCC management: 1 For the selected system, fully document account management policies and procedures to address the segregation of duties for privileged users to not approve or modify their own access requests. 2 For the selected system, ensure that segregation of duties controls are implemented, disallowing users to approve and modify their own access requests.	**Implemented/Closed** We obtained and inspected the updated User Management Process, Version 1, dated October 8, 2014, for the selected system and noted it addresses that the system has a work flow built in to address separation of duties for system administrators requesting their own role change. In addition, we obtained and inspected a Tasks Queue Screenshot from the selected system and noted that a user cannot modify their own access requests.
Prior Year FY 2014 Finding #2 – Bureau of Engraving of Printing (BEP) Security incidents were not reported correctly	BEP reported 2 of 15 CAT 1 incidents outside of the US-CERT's requirement of one hour. One incident was reported almost 2 hours after initial identification, and the other was reported 41 hours after the initial identification. This oversight was due to the lack of training and awareness of BEP Incident Response Capability Procedures.	We recommend that BEP management: 1 Provide training to the BEP CSIRC team regarding BEPs incident response policies and procedures to ensure the timely reporting of incidents. 2 Ensure that BEP CSIRC reports all CAT 1 incidents to TCSIRC within one (1) hour of discovery/detection.	**Implemented/Closed** We obtained and inspected the evidence of training of the BEP CSIRC team on BEP's incident response policies and procedures. Additionally, we selected a sample of 15 BEP incidents and noted that BEP reported 15 of 15 incidents to TCSIRC within the required reporting time frame

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #2 – Departmental Office (DO) Security incidents were not reported correctly.	DO reported 4 of the 15 CAT 1 incidents outside of the US-CERT's requirement of one hour. Two of the incidents were reported 4.25 hours and 12.5 hours after initial identification. One of the incidents was reported 8 days after initial identification. Finally, one of 15 security incidents involved a lost Blackberry phone and was not properly categorized as a CAT 1 Unauthorized Access/Physical Loss, after steps to wipe the Blackberry were taken by CSIRC personnel. DO CSIRC employees were not fully aware of the process and procedures surrounding incident response policies and procedures. Furthermore, not all DO CSIRC employees were aware that lost smart phones (e.g., iPhones or Blackberry) had to be reported within an hour as a CAT 1 incident.	We recommend that DO management: 1 Provide training to the DO CSIRC team on DO's incident response policies and procedures. 2 Ensure that DO CSIRC reports all incidents to TCSIRC in compliance with their standard operating procedures	**Implemented/Closed** We obtained and inspected the training deck and sign-in sheet of the training that was provided to the DO CSIRC team and noted that management provided training on DO's incident response policies and procedures. Additionally, we selected a sample of 15 DO incidents and noted that DO reported 15 of 15 incidents to TCSIRC within the required reporting time frame.
Prior Year FY 2014 Finding #2 – Office of Inspector General (OIG) Security incidents were not reported correctly.	OIG reported 1 of 9 CAT 1 incidents outside of the US-CERT's requirement of one hour. The incident was reported 23 hours and 9 minutes after initial identification. OIG management has only two designated security officers that know and have access to the TCSIRC portal to submit incidents. At the time of the incident, both designated security officers were on annual leave, and there was no backup to submit incident tickets to TCSIRC.	We recommend that OIG management ensure that there are an adequate number of available trained security officers who have access to the TCSIRC portal to report security incidents.	**Implemented/Closed** OIG trained three (3) additional resources on the process of submitting an incident ticket. We obtained and inspected the population of 12 incidents and noted all were appropriately report within the required timeframe.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #3 –Bureau of the Fiscal Service (Fiscal Service) Did not follow NIST guidance for SSPs.	Fiscal Service's SSP for one of the selected systems had implemented NIST SP 800-53, Rev. 4, controls for system, but the controls had not been documented in the SSP. For three other selected systems, we noted that while the SSPs had been updated, management had not documented or tested the NIST SP 800-53, Rev. 4, controls. Furthermore, one of these systems had a security assessment conducted by management in 2014 that used NIST SP 800-53, Rev. 3, controls rather than the current NIST SP-800-53, Rev. 4, controls. Fiscal Service has implemented standard system security and assessment templates based on the Fiscal Service Baseline Security Requirements (BLSRs) released January 2014, which incorporates NIST SP 800-53, Rev. 4, controls. The Security Control Matrix, which are used to document control implementation within the SSP, and assessment templates were updated in conjunction with the release of the BLSRs. While the relevant templates were updated, the subsequent updates to the system security documentation for four of the selected systems were not completed because the systems' assessment cycles were already underway.	We recommend that Fiscal Service management: 1 For the selected system, update the SSP to address and reference NIST SP 800-53, Rev. 4, controls. 2 For the selected systems, implement the NIST SP 800-53, Rev. 4, controls and then update the SSPs to reflect these new controls. 3 For the selected systems, ensure that the annual assessments reflect all of the new and updated controls in NIST SP 800-53 Rev. 4.	**Partially Implemented/Open** Recommendation #1 and #2 are closed but recommendation #3 is still open. The three selected system's SSPs were updated to address and reference NIST SP 800-53, Rev. 4, controls The three selected systems' SSP SCMs were updated to address and reference NIST SP 800-53, Rev. 4, controls One of the three selected systems completed a new SAR to reflect NIST SP 800-53, Rev. 4, controls. The second of the three selected systems completed a new SAR in August 2015 outside of the FY15 FISMA scope. The last of the three selected systems is planning on completing a new SAR to reflect NIST SP 800-53, Rev. 4, controls by June 30, 2016.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #3 – Departmental Office (DO) Did not follow NIST guidance for SSPs.	DO's SSP for the selected system did not address NIST SP 800-53, Rev. 4, controls and was used in the Authority to Operate (ATO) decision on April 28, 2014. DO management did not update or finalize their SSP due to competing priorities with other IT initiatives.	We recommend that DO management: 1 For the selected system, update the SSP to address and reference NIST SP 800-53, Rev. 4, controls and control enhancements. 2 For the selected system, ensure that the next annual assessment reflects all of the new and updated controls in NIST SP 800-53 Rev. 4.	**Implemented/Closed** We obtained inspected the selected system's SSP and noted the SSP was updated to address and reference NIST SP 800-53, Rev. 4, controls We inspected the annual assessment for the selected system and noted it reflects all of the new and updated controls in NIST SP 800-53 Rev. 4.
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 now Rev. 4 compliant; however the implementation statuses were not identified. Mint was unable to provide evidence that all Rev. 4 controls in place for the selected system were assessed**.**

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #4 – Community Development Financial Institutions (CDFI) Fund Evidence of successful completion of annual security awareness training was not retained for some users	CDFI Fund management did not ensure proper completion of annual Security Awareness Training for 8 of the 25 users selected. It was noted that all eight users were contractors who were not in the CDFI Fund's contractor database. Current CDFI Fund security awareness training standard operating procedures (SOPs) did not require the OCIO and Contracting Officer's Representatives (CORs) to coordinate to ensure the contractor database maintained a current listing of all active CDFI Fund contractors. Contractors who are not in the contractor database would not receive reminders to complete their annual security awareness training.	We recommend that CDFI Fund management: 1 Update the security awareness training SOPs to require periodic review of active contractor accounts in the contractor database to ensure the information is current and complete. 2 Ensure that all contractors complete the annual Security Awareness training.	**Implemented/Closed** We obtained and inspected the updated policy and noted it required periodic review of all system accounts on an annual basis. We also obtained and inspected a sample of 25 users and noted that 16 of 17 employees and 8 of 8 contractors had completed their annual security awareness training, which exceeds the 90 percent NIST/Treasury requirement.
Prior Year FY 2014 Finding #4 – Departmental Office (DO) Evidence of successful completion of annual security awareness training was not retained for some users	DO management was unable to provide evidence of successful completion of the annual Security Awareness Training for 9 of the 25 users selected. It was noted that eight DO employees did not complete their training as required. In addition, one individual was an employee of Government Accountability Office (GAO), and DO could not provide evidence of the user's successful completion of security training. DO management was unable to get non-compliant users to respond to requests regarding the requirement to complete training on an annual basis. Additionally, users with training from other bureaus did not provide their security awareness training artifacts for retention purposes.	We recommend that DO management ensure that users are completing the annual security awareness training and retain evidence of their user's successful completion of the annual training.	**Implemented/Closed** We selected a sample of 25 DO users and noted that 25 out of the 25 employees had completed security awareness training.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #4 – Mint Evidence of successful completion of annual security awareness training was not retained for some users	Mint management was unable to provide evidence of successful completion of the annual Security Awareness Training for 4 of the 25 users selected. It was noted that three Mint employees did not complete their training as required. In addition, one individual was a detailee from IRS, and Mint management did not obtain this user's security awareness certificate. Mint management was unable to get non-compliant users to respond to requests regarding the requirement to complete training on an annual basis. Additionally, users with training from other bureaus did not provide their security awareness training artifacts for retention purposes.	We recommend that Mint management: 1 Ensure that all detailees provide evidence of their successful completion of the annual Security Awareness Training to the Mint. 2 Review and increase the frequency of notifying users not compliant with annual security training requirements.	**Implemented/Closed** We noted that the current FISMA year's Security Training test passed with a 100% completion rate for the samples selected. Additionally, we noted Mint increased the frequency of notifying users by emailing multiple reminders to all Mint employees, contractors and detailees regarding the deadline for completing the cyber-security related training.
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 has not finished completing its corrective action We noted that the enterprise-wide POA&M due date to update the policies has been changed to December 31, 2015.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #5 –FinCEN Bureau IT security and configuration management policies had not been updated or reviewed to address NIST and Treasury requirements	FinCEN's configuration management policy references NIST SP 800-53, Rev. 2, and NIST SP 800-70, Rev. 1. Management did not perform a timely review and did not sufficiently update the Configuration Management Policy to reference the most current NIST SP 800-53, Rev. 4, and NIST SP 800-70 Rev. 2 publications. The Configuration Management Policy was last updated on December 19, 2012. The lack of an update to include the current NIST publications to the Configuration Management Policy was a FinCEN management oversight.	We recommend that FinCEN management: 1 Perform a routine review of the Configuration Management policy document and ensure the Configuration Management policy includes the latest NIST requirements. 2 Ensure FinCEN policies and procedures are periodically reviewed and updated for significant changes.	**Implemented/Closed** We obtained and inspected the updated Information Systems Security Policy (ISSP) for Configuration Management, dated December 19, 2014, and noted that includes the current NIST requirements for Configuration Management. Additionally, we noted that all other FinCEN ISSPs were also updated.
Prior Year FY 2014 Finding #6 – Mint Did not update or review their contingency plan, or finalize their contingency plan test results	Contingency plan documentation for a selected Mint system had not been updated or reviewed since January 2009. Mint provided a 2014 disaster recovery exercise lessons-learned report, from February 2014; however, we noted this was still a draft version and had not been signed off by key contingency personnel.	We recommend that Mint management: 1 For the selected system, update the Contingency Plan. 2 For the selected system, ensure key contingency personnel sign-off annually on the contingency plan review and contingency plan test and exercise in a timely fashion after its completion.	**Open** Mint provided a bureau-wide contingency plan and contingency plan test plan and exercise signature page, but the documents were not system-specific.
Prior Year FY 2014 Finding #7 – Departmental Office (DO) POA&Ms were not tracked in accordance with NIST and Treasury requirements at DO	We noted that DO management failed to track the POA&Ms for one of the selected systems in accordance with OMB and Treasury policies. DO management failure to track their POA&Ms for the selected system was due to competing priorities with other IT initiatives. This was a self-reported finding and documented within the system's POA&M, with an estimated completion date of September 30, 2014.	Based on the planned corrective actions for DO, we are not making a recommendation.	**Implemented/Closed** We inspected the POA&M listing and noted that POA&Ms for the selected system were being tracked in accordance with NIST and Treasury requirements.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #8 – OIG	OIG management did not conduct a USGCB baseline review for Windows 7 components and document deviations. OIG management was not aware that a USGCB baseline review for Windows 7 was required to be conducted and deviations documented.	We recommend that OIG management conduct a USGCB baseline review for Windows 7 and document deviations.	**Implemented/Closed** We obtained and inspected the USGCB deviation documentation and noted there was a baseline review and deviations were documented.

Prior Year Findings – 2013 Evaluation

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2013 Finding #1 – Departmental Office (DO) Logical account management activities were not in place or not consistently performed.	For a selected DO system, management was unable to provide us with user access agreements for 4 of the 25 selected active administrator accounts assigned to contractor personnel. In addition, DO management was unable to secure from the system vendor sufficient supporting documentation evidencing the administrators' account creation dates. At the beginning of a new contract, management gave verbal approval to authorize the initial contractors. Later, when the on-boarding process was formalized, it did not include validation of all contractors who received the initial verbal authorization. Without account creation dates, we could not verify that four accounts for which no formal authorization was recorded were created before the on-boarding process was finalized. As a result, there was insufficient evidence that user account authorization was in place and operating effectively.	We recommend that DO management: 1 For the selected system, implement a process or mechanism to track the administrators' account information, including account creation date. 2 For the selected system, ensure that all users are authorized and maintain evidence of the authorization of users.	**Implemented/Closed** We obtained and inspected the Standard Operating Procedures for the selected system's Security Roles and noted that the document included a process to track administrators' accounts information, including creation date. We obtained and inspected a listing of administrator accounts with account creation dates and selected a sample of 5 users and noted that all approved authorization forms were provided for each user.
Prior Year FY 2013 Finding #1 – Treasury Inspector General for Tax Administration (TIGTA) Logical account management activities were not in place or not 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.	**Open** TIGTA has not finished completing its corrective action. We obtained and inspected POA&Ms for Access Control Policy and Account Management for the system's POAMs (Items 77 and 80) and noted they are still open and have a revised due date of January 2016.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2013 Finding #2 –Bureau of the Fiscal Service (Fiscal Service) Security incidents were not reported correctly.	Fiscal Service reported 3 of 15 CAT 1 incidents outside of the US-CERT guidance of one hour. Two of the incidents were reported 85 to 111 minutes after initial identification. One of the incidents was reported 21 hours after the initial identification. Fiscal Service management explained the assessment process for an incident can sometimes exceed the 1-hour timeframe required for a CAT 1 incidents, although management is actively working the incident. Management plans to revise their current procedure to account for incidents that may require additional time for research and analysis.	We recommend that Fiscal Service management: 1 Update Bureau of the Fiscal Service Incident Handling and Response Standard Operating Procedures to account for the additional processes performed by the Enterprise Security Services – Security Divisions. 2 Ensure that Fiscal Service Security reports all CAT 1 incidents to TCSIRC in compliance with their revised standard operating procedures. In addition, provide additional training to the Incident Responder team once the incident response standard operating procedures are revised.	**Implemented/Closed** We obtained and inspected the updated Incident Handling and Response SOPs. Additionally, we selected a sample of 15 Fiscal Service incidents and noted that Fiscal Service reported 15 of 15 incidents to TCSIRC within the required reporting time frame
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.	**Open** TIGTA has not finished completing its corrective action. We obtained and inspected a screen shot of the selected system's POA&Ms and noted that the POA&M item for CP for the system (Item 78) is still open and the revised due date is December 31, 2015.

Prior Year Findings – 2012 Performance Audit

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #1 – Bureau of the Public Debt (BPD) Logical account management activities were not in place or not consistently performed.	For the two selected BPD systems, BPD management could not provide sufficient supporting documentation evidencing the users' last log-on date or time. As a result, we were unable to test the operating effectiveness of the controls over whether inactive users are disabled.	We recommend that BPD management: 1 For both selected systems, develop or acquire additional system capability that generates user lists with last log-on dates so that inactive users are automatically disabled in a timely manner. 2 For both selected systems, in the absence of a long-term system capability solution, perform manual monthly reviews of all system user accounts and disable or delete accounts that no longer need access.	**Implemented/Closed** FMS and BPD consolidated into one organization, Fiscal Service, in October 2012. We obtained and inspected the active user listing for both systems and noted that the listing includes the last access date. We determined that inactive users are disabled in accordance with policies and procedures for both systems.
Prior Year FY 2012 Finding #5-Departmental Offices (DO) Plans of Action and Milestones (POA&Ms) were not tracked in accordance with NIST and Treasury requirements at DO.	We noted that a selected DO system had multiple identified weaknesses identified in the June 2012 continuous monitoring test report that were not documented in the system POA&M. DO bureau policy requires that POA&Ms be inputted 30 days after weaknesses are initially identified. The lack of these findings being added to the POA&M was an oversight by DO management when updating the system POA&M.	We recommend that DO management: 1 Update the selected system POA&M with the findings and recommendations reported in the system continuous monitoring test report. 2 Ensure the continuous monitoring test results and recommendations are captured within the selected system POA&M within the 30-day required period.	**Implemented/Closed** We obtained and inspected the selected system's POA&Ms and noted DO updated the POA&M to include all the findings and remediation's documented in the selected system's Continuous Monitoring Test Report. In addition, we noted there was no continuous monitoring test done this year due to moving of facilities, so they were not able to update the POA&M with any new results.

Prior Year Findings – 2011 Performance Audit

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2011 Finding #1 – Treasury Inspector General for Tax Administration (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.	**Implemented/Untested** We obtained and inspected the updated policies, procedures, and supplemental guidance and noted they provided sufficient guidance over account management activities. However, we noted that TIGTA management updated their Account Management Policies and Procedures in June of 2015, resulting in a testing window of June 15 to June 30. As a result, we were unable to test that the selected system's Account Management controls have been appropriately implemented and were operating effectively for the entire FISMA period (July 1, 2014 – June 30, 2015). Therefore, the finding has been addressed from a policy perspective; however, it has not been tested to confirm effective implementation.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2011 Finding #1– Financial Management Service (FMS) Logical account management activities were not fully documented or consistently performed.	For a sampled FMS payment management system, 12 user accounts out of 2,950 inappropriately remained active following 90 days of inactivity. Additionally, 920 user accounts out of 2,950 did not have a last login date recorded, suggesting these accounts may never have been used by the account owner. We noted a similar finding in a FY 2010 financial statement audit for the sampled system, but FMS's corrective actions to implement a fully automated solution to disable inactive accounts were not fully effective. FMS attributed the noted conditions to human error during the transition to an automated solution. Prior to and after the transition to a fully automated solution, FMS did not monitor if the automated solution was working as intended.	We recommend that FMS management: 1 Continue to monitor the automated solution to disable user accounts after 90 days of inactivity in order to confirm the automated solution is working in all cases. 2 Perform a manual monthly review of all user accounts, and disable or delete (as appropriate) accounts that have not logged into the system within the prior 90 days until the manual, monthly review demonstrates that the automated solution is working for three consecutive months.	**Implemented/Closed** FMS and BPD consolidated into one organization, Fiscal Service, in October 2012. Note: Fiscal Service current policies require that information system accounts be disabled after 120 day of inactivity, not 90 days. Fiscal Service updated the system to automatically disable accounts after 120 since their last login. We noted that management conducted a manual monthly review for the first three consecutive months to ensure the automated solution was working. We obtained and inspected the user list for the selected system and noted that there were no enabled accounts past 120 days of inactivity.

Finding #	Prior-Year Condition	Recommendation(s)	Status
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.	**Open.** TIGTA has not finished completing its corrective action. We obtained and inspected a screenshot of the selected system's POA&Ms and noted that the POA&M items related to the system's CP (POA&M ID 87, 88 & 114) have a revised completion date of December 2014. We further noted a justification for why the remediation was not completed on time was provided in the "Status Comments" field.
Prior Year FY 2011 Finding #10 – TIGTA Risk management program was not consistent with NIST SP 800-37, Rev. 1.	TIGTA was aware of the requirement to comply with NIST SP 800-37, Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, by February 2011, but had not updated the risk management program at the time of the FY 2011 FISMA audit. As NIST SP 800-37 Rev 1 was issued in February 2010, OMB requires federal agencies to adopt this NIST guidance within 1 year of issuance. We did not determine a cause as the weakness was self-reported. TIGTA created a POA&M item to address identified gaps and developed corrective actions to become compliant, with a completion date of August 2014. An insufficient risk management program can lead to ineffective risk-based decision-making and untimely implementation of system-level controls.	Based on TIGTA's planned corrective actions, we are not making a recommendation.	**Implemented/Closed** We obtained and inspected the updated risk management policies, procedure, and supplemental guidance and noted it appears to be consistent with NIST guidance.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2011 Finding #12 – TIGTA Improper system configuration programs.	The sampled TIGTA system lacked formal documentation in certain areas of configuration management. TIGTA management identified this weakness in a 2010 security assessment and created POA&M remediation actions to address the weaknesses identified with a completion date of May 2012.	Based on TIGTA's planned corrective actions, we are not making a recommendation.	**Implemented/Closed** We obtained and inspected configuration documentation and noted the documentation adequately addresses the selected system's configuration management program.

APPENDIX III – DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS's FISMA 2015 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 2015 questions for Inspectors General. We prepared responses to DHS questions based on an assessment of 15 information systems across 12 Treasury components, excluding the IRS. We determined the overall status of each DHS question based on the magnitude of the aggregated findings under each category with OIG and TIGTA acceptance. 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 changed the overall from a "yes" to a "no." The information provided by TIGTA has not been subjected to KPMG audit procedures and, accordingly, we express no conclusion on it.

1: Continuous Monitoring Management		
Status of Continuous Monitoring Management Program [check one: Yes or No]		**1.1** Utilizing the ISCM maturity model definitions, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.
	Ad Hoc (Level 1)*	**1.1.1.** Please provide the D/A ISCM maturity level for the People domain.
	Ad Hoc (Level 1)*	**1.1.2.** Please provide the D/A ISCM maturity level for the Processes domain.
	Ad Hoc (Level 1)*	**1.1.3.** Please provide the D/A ISCM maturity level for the Technology domain.
	Ad Hoc (Level 1)*	**1.1.4.** Please provide the D/A ISCM maturity level for the ISCM Program Overall.
	N/A†	**1.2.** Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model above.

Note *: In FY 2015, CyberScope included the Inspector General (IG) Information Security Continuous Monitoring (ISCM) maturity model to summarize the status on a 5-level scale from lowest to highest: Ad Hoc (Level 1), Defined (Level 2), Consistently Implemented (Level 3), Managed and Measurable (Level 4), and Optimized (Level 5).

2: Configuration Management		
Status of Configuration Management Program [check one: Yes or No]	No	**2.1** Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

† No additional information on the effectiveness.

2: Configuration Management		
	Yes	**2.1.1.** Documented policies and procedures for configuration management.
	No	**2.1.2.** Defined standard baseline configurations. **Comments – Treasury OIG:** DO has a self-identified weakness over baseline configurations for one of the selected systems. (See Self-Identified Weakness Section: POA&M #576 and #6149)
	No	**2.1.3.** Assessments of compliance with baseline configurations. **Comments – Treasury OIG:** Fiscal Service had a self-identified weakness over continuous monitoring testing was not conducted during the assessment period for one the selected systems. (See Self-Identified Weakness Section: POA&M #8393) **Comments – TIGTA**: The IRS has not deployed automated mechanisms to centrally manage, apply, and verify baseline configuration settings and produce FISMA compliance reports using the NIST-defined Security Content Automation Protocol format for all of its information technology assets. The IRS is awaiting the outcome of the DHS's Continuous Diagnostics and Mitigation program Task Order #2 to provide the toolset to meet the program requirements.
	No*	**2.1.4.** Process for timely (as specified in organization policy or standards) remediation of scan result deviations. **Comments – TIGTA**: The IRS has not yet fully implemented configuration baseline scanning tools and processes on all systems to ensure timely remediation of scan result deviations.
	Yes	**2.1.5.** For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented.
	No*	**2.1.6.** Documented proposed or actual changes to the hardware and software configurations. **Comments – TIGTA**: The IRS has not yet fully implemented configuration and change management controls to ensure that proposed or actual changes to hardware and software configurations are documented and controlled.
	No	**2.1.7.** Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI-2). **Comments – Treasury OIG:** DO has a self-identified weakness over vulnerability scanning for one of the four selected systems. (See Self-Identified Weakness Section: POA&M #6736 and #7314) **Comments – TIGTA**: The IRS has not implemented software assessment (scanning) on all systems.

* Based on TIGTA's Findings over the IRS information systems, this response resulted in a "no."

2: Configuration Management		
	No	**2.1.8.** Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2). **Comments – Treasury OIG:** DO has a self-identified weakness over configuration management and timely patching for two of the four selected systems. (See Self-Identified Weakness Section: POA&M #575, #578, #6861, #7788, #8631, and #8634) OCC has a self-identified weakness over configuration settings for the selected system. (See Self-Identified Weakness Section: POA&M #3741) **Comments – TIGTA**: The IRS has not yet fully implemented configuration-related vulnerability scanning tools and processes on all systems to ensure timely remediation of scan result deviations.
	No*	**2.1.9.** Patch management process is fully developed, as specified in organization policy or standards (NIST SP 800-53: CM-3, SI-2). **Comments – TIGTA**: The IRS has not implemented a Service-wide process to ensure timely installation of software patches on all platforms.
		2.2. Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above. **Comments – Treasury OIG:** DO has a self-identified weakness over audit logging capabilities for two of the four selected systems. (See Self-Identified Weakness Section: POA&M #7412, #7413, and #7645) Fiscal Service has a self-identified weakness over audit logging capabilities for one of the selected systems. (See Self-Identified Weakness Section: POA&M #3140 and #3141) OCC has a self-identified weakness over audit logging capabilities for the selected system. (See Self-Identified Weakness Section: POA&M #47)
	No*	**2.3.** Does the organization have an enterprise deviation handling process and is it integrated with the automated scanning capability **Comments – TIGTA**: The IRS does not have an enterprise deviation handling process that is integrated with the automated capability for all of its information technology assets. A number of its assessment activities involve manual processes.
	No*	**2.3.1.** Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented. **Comments – TIGTA**: The IRS has established a process for accepting the risk introduced by deviations, but it is not integrated with the automated capability.

* Based on TIGTA's Findings over the IRS information systems, this response resulted in a "no."

3: Identity and Access Management		
Status of Identity and Access Management Program [check one: Yes or No]	No	**3.1** Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?
	Yes	**3.1.1.** Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1)
	No*	**3.1.2.** Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2). **Comments – TIGTA**: The IRS cannot yet uniquely identify all users who access its systems in compliance with HSPD-12.
	No	**3.1.3.** Organization has planned for implementation of PIV for logical access in accordance with government policies **(**HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). **Comments – Treasury OIG:** DO has a self-identified weaknesses over multi-factor authentication for two of the four selected systems. (See Self-Identified Weakness Section: POA&M#6151, 6368, #7328) Mint has a self-identified weakness over multi-factor authentication for its selected system. (See Self-Identified Weakness Section: POA&M #111) **Comments – TIGTA**: The IRS's plans did not fully address existing challenges relating to privileged user access and its legacy system environment to ensure success in achieving full and timely compliance with HSPD-12 for logical access.
	No*	**3.1.4.** Organization has planned for implementation of PIV for physical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). **Comments – TIGTA**: The IRS's plans did not fully address existing challenges (including funding challenges) to achieving full and timely compliance with HSPD-12 for physical access.

* Based on TIGTA's Findings over the IRS information systems, this response resulted in a "no."

3: Identity and Access Management		
	No	**3.1.5.** Ensures that the users are granted access based on needs and separation-of-duties principles. **Comments – Treasury OIG:** DO had accounts that were created prior to obtaining appropriate approvals. Mint and TIGTA were unable to provide evidence that users' access was granted access based on needs. (See Finding #1 and Prior Year FY 2013 Finding #1) **Comments – TIGTA**: During FY 2015, the Government Accountability Office (GAO) identified users that had been granted more access than needed and instances in which the separation-of-duties principle was not enforced.
	No*	**3.1.6.** Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. IP phones, faxes, printers). **Comments – TIGTA**: The IRS is still in the process of implementing technical solutions and introducing automated tools to achieve full asset discovery and asset management in accordance with policy.
	No	**3.1.7.** Ensures that accounts are terminated or deactivated once access is no longer required. **Comments – Treasury OIG:** CDFI Fund and DO did not deactivate accounts after 90 days of inactivity. Fiscal Service did not deactivate accounts after 120 days of inactivity. (See Finding #1) **Comments – TIGTA**: During FY 2015, the TIGTA and the GAO identified systems that do not have controls in place to ensure that accounts are terminated or deactivated once access is no longer needed.
	No*	**3.1.8.** Identifies and controls use of shared accounts. **Comments – TIGTA**: During FY 2015, the TIGTA and the GAO identified improper use of shared accounts; for example, use of generic administrator accounts and passwords.

* Based on TIGTA's Findings over the IRS information systems, this response resulted in a "no."

3: Identity and Access Management		
		3.2. Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was not noted in the questions above. **Comments – Treasury OIG:** DO has service accounts that were not appropriately identified as such. Fiscal Service was unable to provide documentation evidencing administrators account creation dates. TIGTA was unable to provide documentation evidencing the users' last log-on date or time. (See Finding #1, Prior Year FY 2014 Finding #1 and Prior Year FY 2013 Finding #1) DO has a self-identified weakness over lack of quarterly audits and automated audit account management functions for one of the four selected systems. (See Self-Identified Weakness Section: POA&M #584) **Comments – TIGTA**: In mid-June 2015, the Federal Chief Information Officer launched a 30-day Cybersecurity Sprint instructing Federal agencies to take a number of steps to further protect Federal information and assets and improve the resilience of Federal networks. As part of the Cybersecurity Sprint, agencies were instructed to dramatically accelerate the implementation of personal identity verification card use, especially for privileged users. In response to the Cybersecurity Sprint, the IRS developed a plan in July 2015 to accelerate mandatory personal identity verification card use and begin to address existing challenges related to privileged users and its legacy system environment.

4: Incident Response and Reporting		
Status of Incident Response and Reporting Program [check one: Yes or No]	Yes	**4.1** Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**4.1.1.** Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1).
	Yes	**4.1.2.** Comprehensive analysis, validation, and documentation of incidents.
	Yes	**4.1.3.** When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19).
	Yes	**4.1.4.** When applicable, reports to law enforcement and the Inspector General within established time frames.
	Yes	**4.1.5.** Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19).
	Yes	**4.1.6.** Is capable of correlating incidents.

4: Incident Response and Reporting		
	Yes	**4.1.7.** Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; and OMB M-07-16, M-06-19).
	N/A[†]	**4.2.** Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.

5: Risk Management		
Status of Risk Management Program [check one: Yes or No]	Yes	**5.1** Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**5.1.1.** Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1.
	Yes	**5.1.2.** Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1.
	Yes	**5.1.3.** Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1.
	Yes	**5.1.4.** Has an up-to-date system inventory.
	Yes	**5.1.5.** Categorizes information systems in accordance with government policies.
	Yes	**5.1.6.** Selects an appropriately tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.
	No	**5.1.7.** Implements the approved set of tailored baseline security controls specified in metric 5.1.6. **Comments – Treasury OIG:** CDFI Fund, Fiscal Service, Mint, and OCC did not implement the NIST SP 800-53, Rev. 4, security controls for some of their SSPs and ensure completeness in accordance with NIST guidance. (See Finding #2 and Prior Year FY 2014 Finding #3)
	No	**5.1.8.** Assesses the security controls using appropriate assessment procedures to determine 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 system. **Comments – Treasury OIG:** CDFI Fund, Fiscal Service, Mint, and OCC did not implement the NIST SP 800-53, Rev. 4, security controls for some of their SSPs and ensure completeness in accordance with NIST guidance. (See Finding #2 and Prior Year FY 2014 Finding #3)

[†] No additional information on the effectiveness.

5: Risk Management		
	Yes	**5.1.9.** Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
	Yes	**5.1.10.** Information-system-specific risks (tactical), mission/business-specific risks and organizational-level (strategic) risks are communicated to appropriate levels of the organization.
	Yes	**5.1.11.** Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).
	Yes	**5.1.12.** Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks.
	Yes	**5.1.13.** Security authorization package contains system security plan, security assessment report, POA&M, and accreditation boundary in accordance with government policies (NIST SP 800-18, SP 800-37).
	Yes	**5.1.14.** The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.
	No	**5.1.15** For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems **Comments – Treasury OIG:** Mint's contract with their third-party cloud service provider did not address FedRAMP requirements and the CSP did provide FISMA-related artifacts to demonstrate FISMA compliance. (See Finding #5)
		5.2. Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above. **Comments – Treasury OIG:** TTB had not updated or reviewed their bureau policies to address NIST and Treasury requirements. (See Finding #3) BEP had not updated or reviewed their bureau policies to address NIST and Treasury requirements. (Prior Year FY 2014 Finding #5, and Self-Identified Weakness Section POA&M # R4001)

6: Security Training		
Status of Security Training Program [check one: Yes or No]	Yes	**6.1** Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**6.1.1.** Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1).

6: Security Training		
	Yes	**6.1.2.** Documented policies and procedures for specialized training for users with significant information security responsibilities.
	Yes	**6.1.3.** Security training content based on the organization and roles, as specified in organization policy or standards.
	Yes	**6.1.4.** Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training.
	No*	**6.1.5.** Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training. **Comments – TIGTA**: The IRS does not identify and track the status of specialized training for all of its contractor employees with significant information security responsibilities that require specialized training.
	Yes	**6.1.6.** Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53).
	N/A†	**6.2.** Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.

7: POA&M		
Status of POA&M Program [check one: Yes or No]	Yes	**7.1** Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**7.1.1.** Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.
	Yes	**7.1.2.** Tracks, prioritizes, and remediates weaknesses.

* Based on TIGTA's Findings over the IRS information systems, this response resulted in a "no."
† No additional information on the effectiveness.

7: POA&M		
	No	**7.1.3.** Ensures remediation plans are effective for correcting weaknesses. **Comments – Treasury OIG:** DO did not adequately document the remedial actions taken to correct the weaknesses or deficiencies for one of the four selected systems. (See Finding #4) **Comments – TIGTA**: The IRS did not always ensure that weaknesses were corrected prior to POA&M closure. The 10 systems we evaluated closed a total of 43 POA&Ms during FY 2015. Of the 43 POA&M closures, 22 were closed without sufficient evidence that the weakness was corrected. However, the IRS's POA&M validation processes did not fail the closure of 13 of the 22. The IRS confirmed that five of the 13 POA&Ms had not been corrected, and it could not provide sufficient evidence to support the closure of an additional three. The IRS subsequently uploaded artifacts that justified closure for the remaining five POA&Ms.
	No	**7.1.4.** Establishes and adheres to milestone remediation dates and provides adequate justification for missed remediation dates. **Comments – Treasury OIG:** FinCEN did not adhere to milestone remediation dates or provides adequate justification for missed remediation dates for the selected system. DO did not adhere to milestone remediation dates or provides adequate justification for missed remediation dates for two of the four selected systems. (See Finding #4)
	Yes	**7.1.5.** Ensures resources and ownership are provided for correcting weaknesses.
	Yes	**7.1.6.** POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25).
	Yes	**7.1.7.** Costs associated with remediating weaknesses are identified in terms of dollars (NIST SP 800-53, Rev. 3: PM-3; OMB M-04-25).
	Yes	**7.1.8.** Programs officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53: CA-5; and OMB M-04-25).
	N/A[†]	**7.2.** Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above.

[†] No additional information on the effectiveness.

8: Remote Access Management		
Status of Remote Access Management Program [check one: Yes or No]	Yes	**8.1** Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**8.1.1.** Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17).
	Yes	**8.1.2.** Protects against unauthorized connections or subversion of authorized connections.
	No*	**8.1.3.** Users are uniquely identified and authenticated for all access (NIST 800-46, Section 4.2, Section 5.1). **Comments – TIGTA**: The IRS had not fully implemented unique user identification and authentication that complies with HSPD-12. In addition, system administrators of the virtual private network infrastructure and server components do not use NIST-compliant multifactor authentication for local or network access to privileged accounts.
	Yes	**8.1.4.** Telecommuting policy is fully developed (NIST 800-46, Section 5.1).
	No*	**8.1.5.** Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. **Comments – TIGTA**: The IRS had not fully implemented remote electronic authentication that complies with HSPD-12.
	Yes	**8.1.6.** Defines and implements encryption requirements for information transmitted across public networks.
	Yes	**8.1.7.** Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.
	Yes	**8.1.8.** Lost or stolen devices are disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).
	Yes	**8.1.9.** Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4).
	Yes	**8.1.10.** Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1, NIST SP 800-53, PS-6).
	N/A†	**8.2.** Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.
	Yes	**8.3.** Does the organization have a policy to detect and remove unauthorized (rogue) connections?

* Based on TIGTA's Findings over the IRS information systems, this response resulted in a "no."
† No additional information on the effectiveness.

9: Contingency Planning		
Status of Contingency Planning Program [check one: Yes or No]	No	**9.1** Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**9.1.1.** Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1).
	Yes	**9.1.2.** The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan (NIST SP 800-34).
	No	**9.1.3.** Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures (NIST SP 800-34). **Comments – Treasury OIG:** Mint did not fully implement contingency planning and testing controls. TIGTA did not fully implement contingency planning and testing controls for one system and one prior year system did not have a new operating system integrated into its contingency plan. (See Prior Year FY 2014 Finding #6, Prior Year FY 2013 Finding #4 and Prior Year FY 2011 Finding #8)
	No	**9.1.4.** Testing of system-specific contingency plans. **Comments – Treasury OIG:** Mint conducted a disaster recovery exercise, but it was still in draft and had not been signed off by the contingency planning personnel. TIGTA did not perform contingency plan testing for the selected system. (See Prior Year FY 2014 Finding #6 and Prior Year FY 2013 Finding #4)
	Yes	**9.1.5.** The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).
	No	**9.1.6.** Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53). **Comments – Treasury OIG:** TIGTA did not fully implement contingency planning and testing controls. (See Prior Year FY 2013 Finding #4 and Prior Year FY 2011 Finding #8)
	No	**9.1.7.** Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans. **Comments – Treasury OIG:** Mint conducted a disaster recovery exercise, but it was still in draft and had not been signed off by the contingency planning personnel. TIGTA did not perform contingency plan testing for the selected system. (See Prior Year FY 2014 Finding #6 and Prior Year FY 2013 Finding #4) DO had a self-identified weakness over contingency plan testing for one the selected systems. (See Self-Identified Weakness Section: POA&M #3508)

9: Contingency Planning		
	No	**9.1.8.** After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34). **Comments – Treasury OIG:** Mint conducted a disaster recovery exercise, but it was still in draft and had not been signed off by the contingency planning personnel. TIGTA did not perform contingency plan testing for the selected system. (See Prior Year FY 2014 Finding #6 and Prior Year FY 2013 Finding #4)
	No	**9.1.9.** Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for system that require them (FCD1, NIST SP 800-34, NIST SP 800-53). **Comments – Treasury OIG:** DO had a self-identified weakness over the disaster recovery was not operational at the time of the assessment for one the selected systems. (See POA&M #3506)
	Yes	**9.1.10.** Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).
	Yes	**9.1.11.** Contingency planning that considers supply chain threats.
	N/A[†]	**9.2.** Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.

10: Contractor Systems		
Status of Contractor Systems [check one: Yes or No]	Yes	**10.1** Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes?
	Yes	**10.1.1.** Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities (including other government agencies), including organization systems and services residing in a public, hybrid, or private cloud.
	Yes	**10.1.2.** The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with FISMA requirements, OMB policy, and applicable NIST guidelines (NIST SP 800-53: CA-2).
	Yes	**10.1.3.** A complete inventory of systems operated on the organization's behalf by contractors or other entities, (including other government agencies), including organization systems and services residing in a public, hybrid, or private cloud.

[†] No additional information on the effectiveness.

10: Contractor Systems		
	Yes	**10.1.4.** The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5).
	No*	**10.1.5.** The Organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates. **Comments – TIGTA**: The IRS did not have sufficient processes to ensure that interfaces between IRS and contractor systems have appropriate agreements.
	Yes	**10.1.6.** The inventory of contractor systems is updated at least annually.
	N/A†	**10.2.** Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.

* Based on TIGTA's Findings over the IRS information systems, this response resulted in a "no."
† No additional information on the effectiveness.

APPENDIX IV – APPROACH TO SELECTION OF SUBSET OF SYSTEMS

In fiscal year (FY) 2015, a risk-based approach was employed to determine the subset of Department of the Treasury (Treasury) information systems for the FISMA audit. The universe for this subset only included major business applications and general support systems with a security classification of "moderate" or "high." We used the system inventory contained within the Treasury FISMA management tracking tool as the population for this subset. However, we did not validate the completeness and accuracy of the inventory in the Treasury FISMA management tracking tool.

Based on historical trends in Treasury's systems inventory and past reviews, we used a subset size of 25 from the total population of Treasury major applications and general support systems with a security classification of "Moderate" or "High." Based on their lower risk, we elected not to incorporate any systems with a FIPS 199 System Impact Level of "Low" into the population of applications to be selected. We then applied the weighting of IRS systems to non-IRS bureau systems to the total subset size in order to determine the IRS and non-IRS bureau subset sizes.

To select the subset, we stratified the full population of Treasury major applications and general support systems by bureau and by FIPS 199 system impact level. We used a risk-based approach to select systems out of each stratum. We considered the following factors to select system:

- Total number of systems per bureau.
- Systems at smaller bureaus not historically included in FISMA audits or evaluations.
- Number of systems at each bureau with a FIPS system impact level of "High."
- Location of the system.
- Whether the system is going to be decommissioned prior to December 31, 2015.
- Whether the system was identified in a previous FISMA audits or evaluations within the past two years.

Lastly, the total number of financial systems selected did not exceed the percentage of Treasury's population of financial systems.

Based on our analysis of Treasury's inventory of information systems as of May 29, 2015, we noted a total of 190 major applications and general support systems with a security classification of moderate or high are contained within the Treasury-wide inventory. The following table provides our analysis of the composition of Treasury's inventory of major applications and general support systems.

	Total	**IRS Financial Systems**	**IRS Non-Financial Systems**	**Non-IRS Financial Systems**	**Non-IRS Non-Financial Systems**
Major Applications	132	2	43	36	51
General Support Systems	58	0	25	1	32
Total	190	2	68	37	83

From the analysis above, it was determined that IRS systems make up 37% of the total population of Major Applications and General Support systems and Non-IRS systems make up 63%. When the IRS to Non-IRS weighting is applied to subset size of 25 from the total population, the resulting sizes for the IRS and Non-IRS subsets are 10 and 15, respectively.

We determined that Major Applications account for 73% of the population of the Non-IRS population and General Support Systems account for 27%. We further determined that systems designated as "Financial" in the Treasury FISMA management tracking tool, account for 31% of all Non-IRS Major Applications and General Support Systems. Lastly, we determined that 28% of the Non-IRS Major Applications and General Support Systems are assigned a FIPS 199 System Impact Level of "High," while 72% are assigned a FIPS 199 System Impact Level of "Moderate."

Based on these factors, we determined the following proposed composition for the subset of Non-IRS Major Applications and General Support Systems for the FY 2015 FISMA audit:

Total Selected	15
Total Major Applications	11
Total General Support Systems	4
Total Systems with a FIPS 199 System Impact Level of "High"	4
Total Systems with a FIPS 199 System Impact Level of "Moderate"	11
Total Systems with a FIPS 199 System Impact Level of "Low"	0
Total Systems Designated as Financial	5

We further stratified the number of information systems by each bureau to determine the total percentage of information systems at each Non-IRS bureau, based on the total population of the 120 Non-IRS information systems. We used this information as a baseline to determine the total number of systems to select at each bureau or office:

Bureau	Total Systems	Percentage of Total Non-IRS Population	Total Number of Non-IRS Systems to be Select
BEP	6	5%	1
Fiscal Service	46	38%	5
CDFI Fund	3	2%	1 (See Note 1)
DO	33	28%	4
FinCEN	6	5%	1
Mint	13	11%	1
OCC	7	6%	1
OIG	1	1%	0 (See Note 2)
TIGTA	2	2%	0 (See Note 3)
TTB	3	2%	1 (See Note 1)
Total	120	100%	15

(**Note 1:** Using this methodology initially did not yield a system being selected at these agencies. However, using our risk-based methodology, we elected to select one system for each of these agencies and decrease the number of systems for Fiscal Service.)
(**Note 2:** Our rotational system selection strategy precludes selecting systems reviewed within the past two years. In FY 2013, OIG's only system was selected. Therefore, we excluded that system from our sample selection in FY 2015.)
(Note 3: Our rotational system selection strategy precludes selecting systems reviewed within the past two years. TIGTA has two systems and one of each were selected in FY 2014 and FY 2013. Therefore, we excluded these systems from our sample selection in FY 2015.)

APPENDIX V – GLOSSARY OF TERMS

Acronym	Definition
AC	Access Control
ACIOCS	Associate Chief Information Officer for Cyber Security
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
CA	Security Assessment and Authorization
CAT	Category
CDFI	Community Development Financial Institutions
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CM	Configuration Management
COR	Contracting Officer Representative
CP	Contingency Plan
CSIRC	Computer Security Incident Response Center
CSP	Cloud Service Provider
CSS	Cyber Security Sub-Council
DHS	Department of Homeland Security
DO	Departmental Offices
DRP	Disaster Recovery Plan
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
FMS	Financial Management Service
FY	Fiscal Year
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
IG	Inspector General
IR	Incident Response
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring

Acronym	Definition
ISSO	Information Systems Security Officer
IT	Information Technology
KPMG	KPMG LLP
Mint	United States Mint
MOU	Memorandum of Understanding
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
PL	Planning
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
Rev.	Revision
SA	System and Services Acquisition
SA&A	Security Assessment and Authorization
SC	System and Communication Protection
SIGTARP	Special Inspector General for the Troubled Asset Relief Program
SOP	Standard Operating Procedures
SP	Special Publication
STIG	Security Technical Implementation Guide
SSP	System Security Plan
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
USGCB	United States Government Configuration Baseline

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 2

Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2015
September 25, 2015

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 2015

September 25, 2015

Reference Number: 2015-20-092

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

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION – FEDERAL INFORMATION SECURITY MODERNIZATION ACT REPORT FOR FISCAL YEAR 2015

Highlights

Final Report issued on September 25, 2015

Highlights of Reference Number: 2015-20-092 to the Department of the Treasury, Office of the Inspector General, Assistant Inspector General for Audit.

IMPACT ON TAXPAYERS

The Federal Information Security Management Act of 2002, and its recent amendment, the Federal Information Security Modernization Act (FISMA) of 2014, were enacted to strengthen the security of information and systems within Federal Government agencies. The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. As custodians of taxpayer information, the IRS 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 2015.

WHAT TIGTA FOUND

The IRS's Information Security Program generally complied with the FISMA requirements. Three program areas met all FISMA performance attributes specified by the Department of Homeland Security: *Risk Management*, *Incident Response and Reporting*, and *Contingency Planning*. Four other security program areas met all attributes with the exception of two or fewer program attributes that were not met: *Security Training*, *Plan of Action and Milestones*, *Remote Access Management*, and *Contractor Systems*.

However, three security program areas failed to meet FISMA requirements overall due to not meeting many of the performance attributes specified by the Department of Homeland Security: *Continuous Monitoring Management*, *Configuration Management*, and *Identity and Access Management*.

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 issued by the Department of Homeland Security for the applicable FISMA evaluation period.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 25, 2015

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 2015 (Audit # 201520001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Modernization Act[1] evaluation of the Internal Revenue Service for Fiscal Year 2015. 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 evaluations to the Office of Management and Budget.

This report was forwarded to the Treasury Inspector General for consolidation into a report issued to the Department of the Treasury, Chief Information Officer. Copies of this report are also being sent to the Internal Revenue Service managers affected by the report results.

If you have any questions, please contact me or Danny Verneuille, Acting 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

Background ..... Page 1

Results of Review ..... Page 3

The Information Security Program Generally Complied With the Federal Information Security Modernization Act ..... Page 4

Significant Improvements Are Needed in Continuous Monitoring Management, Configuration Management, and Identity and Access Management ..... Page 4

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 18

Appendix II – Major Contributors to This Report ..... Page 19

Appendix III – Report Distribution List ..... Page 20

Appendix IV – Treasury Inspector General for Tax Administration Information Technology Security-Related Reports Issued During the Fiscal Year 2015 Evaluation Period ..... Page 21

Abbreviations

DHS	Department of Homeland Security
FCD1	Federal Continuity Directive 1
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAO	Government Accountability Office
HSPD-12	Homeland Security Presidential Directive-12
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SP	Special Publication
TIGTA	Treasury Inspector General for Tax Administration
US-CERT	United States Computer Emergency Response Team
USGCB	United States Government Configuration Baseline

Background

The Federal Information Security Management Act of 2002[2] was enacted to strengthen the security of information and information systems within Federal agencies. The Act 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 entity. To ensure uniformity in this process, the Act requires the National Institute of Standards and Technology (NIST) to prescribe standards and guidelines pertaining to Federal information systems.

The Federal Information Security Modernization Act of 2014 intends to improve security by transitioning agencies away from paperwork requirements toward a more automated and continuous security posture.

After 12 years, an amendment to the Federal Information Security Management Act of 2002 was signed into law, called the Federal Information Security Modernization Act of 2014 (FISMA).[3] It provides several modifications to the Federal Information Security Management Act of 2002 that modernize Federal security practices to current security concerns. Specifically, it:

- Reasserts the authority of the Director of the Office of Management and Budget (OMB) with oversight, while authorizing the Secretary of the Department of Homeland Security (DHS) to administer the implementation of security policies and practices for Federal information systems.
- Requires agencies to notify Congress of major security incidents within seven days. The OMB will be responsible for developing guidance on what constitutes a major incident.
- Places more responsibility on agencies for budgetary planning for security management, ensuring that senior officials accomplish information security tasks, and ensuring that all personnel are responsible for complying with agency information security programs.
- Changes the reporting guidance focusing on threats, vulnerabilities, incidents, the compliance status of systems at the time of major incidents, and data on incidents involving Personally Identifiable Information.

[2] Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.
[3] 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.

- Calls for the revision of OMB Circular A-130[4] to eliminate inefficient or wasteful reporting.
- Provides for the use of automated tools in agencies' information security programs, including periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents.

These changes are intended to improve security by transitioning agencies away from paperwork requirements (*e.g.*, "check-the-box" style of approaches to compliance) toward a more automated and continuous security posture.

Under the new FISMA legislation, agency heads continue to be responsible for submitting an annual report on the adequacy and effectiveness of their information security policies, procedures, and practices to the OMB Director, the Comptroller General of the United States, and selected congressional committees. In addition, agencies continue to be responsible to have an annual independent evaluation of their information security program and practices to determine the effectiveness of such program and practices. Each independent evaluation must include:

- Testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems.
- An assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

For agencies with an Inspector General appointed under the Inspector General Act of 1978,[5] the annual independent evaluation shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency.

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 (OIG). TIGTA is responsible for oversight of the Internal Revenue Service (IRS), while Treasury OIG is responsible for all other Treasury bureaus. Because of this arrangement, each Inspector General conducts FISMA evaluations on its bureaus and submits separate FISMA reports. However, the OMB requires and expects only one FISMA report to be issued for each department, so coordination is required among both Inspectors General to satisfy this requirement. As a result, TIGTA will issue its final report with the results of its evaluation of the IRS to the Treasury OIG, which will then combine the results for all the Treasury bureaus into one report for the OMB.

This review was performed at, and with information obtained from, the IRS Information Technology organization's Office of Cybersecurity in New Carrollton, Maryland, during the

[4] OMB, OMB Circular No. A-130 (Revised), *Management of Federal Information Resources* (Nov. 2000).
[5] 5 U.S.C. app. 3 (amended 2008).

period April through August 2015. This report covers the period from July 1, 2014, through June 30, 2015. 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 IRS collects and maintains a significant amount of personal and financial information on each taxpayer. As custodians of taxpayer information, the IRS is responsible for implementing appropriate security controls to protect the confidentiality of this sensitive information against unauthorized access or loss in accordance with FISMA requirements.

The OMB uses annual FISMA metrics to assess the implementation of agency information security capabilities and to measure overall program effectiveness in reducing risks. For Inspectors' General use in assessing Federal agency information security programs, the DHS issued the *Fiscal Year (FY) 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics* on June 19, 2015, which contained 10 information security program areas for Inspectors General to assess.

1. Continuous Monitoring Management.
2. Configuration Management.
3. Identity and Access Management.
4. Incident Response and Reporting.
5. Risk Management.
6. Security Training.
7. Plan of Action and Milestones (POA&M).
8. Remote Access Management.
9. Contingency Planning.
10. Contractor Systems.

With the exception of the Continuous Monitoring Management program area, the assessment consisted of two parts: 1) determining if a program was in place for the area and 2) evaluating a combined 83 attributes of those programs. For Continuous Monitoring Management, the Inspectors General were asked to assess the maturity level of this security program area using a maturity model approach. Using the attributes contained within the model, maturity levels from one to five were to be assigned to each of the domains of people, processes, and technology, and the lowest measure assigned to these domains would be given as the overall maturity level for this program. The Information Technology Committee of the Council of Inspectors General on Integrity and Efficiency, in coordination with the DHS, OMB, NIST, and other key stakeholders, developed this maturity model and plans to develop additional maturity models for other FISMA program areas in the coming years.

The Information Security Program Generally Complied With the Federal Information Security Modernization Act

The IRS has established an information security program and related practices in all 10 FISMA program areas. Three of the 10 program areas met all performance attributes specified by the DHS: *Incident Response and Reporting*, *Risk Management*, and *Contingency Planning*. Four other program areas were not fully effective due to two or fewer program attributes that were not met, as follows:

- *Security Training*

  The IRS does not identify and track the status of specialized training for all of its contractor employees with significant information security responsibilities that require specialized training.

- *POA&M*

  The IRS did not always ensure that weaknesses were corrected prior to POA&M closure.

- *Remote Access Management*

  The IRS has not fully implemented unique user identification and authentication or remote electronic authentication that complies with Homeland Security Presidential Directive-12 (HSPD-12) requirements.

- *Contractor Systems*

  The IRS did not have sufficient processes to ensure that interfaces between IRS and contractor systems have appropriate agreements.

Significant Improvements Are Needed in Continuous Monitoring Management, Configuration Management, and Identity and Access Management

Significant improvements are needed in three program areas that failed to meet FISMA requirements overall. These program areas were missing many performance attributes specified by the DHS for meeting FISMA requirements.

- *Continuous Monitoring Management*

  The Continuous Monitoring Management program is at a maturity level of one on a scale of one to five. The IRS is still in the process of implementing its Information Security Continuous Monitoring (ISCM) program required by the OMB to automate asset management and maintain secure configuration of these assets in real time. In July 2014, the Department of the Treasury decided to adopt a uniform approach to ISCM across the Department and to use the toolset selected by the DHS to meet the program requirements.

The DHS is in the process of procuring a standard set of cybersecurity tools and services for use by Federal agencies (expected to be completed in August 2015). This toolset will include sensors that perform automated searches for known cyber flaws and send the results to dashboards that inform system managers in real time of cyber risks that need remediation. When implemented, ISCM is intended to provide security automation in 11 domains: Vulnerability Management, Patch Management, Event Management, Incident Management, Malware Detection, Asset Management, Configuration Management, Network Management, License Management, Information Management, and Software Assurance.

- *Configuration Management*

  The Configuration Management program did not meet a majority of the attributes specified by the DHS. Although the IRS has tools and processes that discover assets, evaluate configuration policy, and scan the enterprise to detect vulnerabilities, these processes have not been fully implemented Service-wide, and the IRS still relies on many tedious manual procedures. In addition, the IRS is still working to expand a standard automated process to deploy operating system patches Service-wide. Eventually, the IRS's Configuration Management program will benefit from the implementation of ISCM, which intends to automate configuration management in real time for the universe of the IRS's assets.

- *Identity and Access Management*

  The Identity and Access Management program did not meet a majority of the attributes specified by the DHS, largely due to the IRS not achieving Governmentwide set goals for implementing logical (system) and physical access to facilities in compliance with HSPD-12 requirements. The HSPD-12 requires Federal agencies to issue personal identity verification cards to employees and contractors for accessing agency systems and facilities. The IRS had not resolved existing challenges to achieving full compliance with HSPD-12.

  In mid-June 2015, the Federal Chief Information Officer launched a 30-day Cybersecurity Sprint, instructing Federal agencies to take a number of steps to further protect Federal information and assets and improve the resilience of Federal networks. As part of the Cybersecurity Sprint, agencies were instructed to dramatically accelerate the implementation of personal identity verification card use, especially for privileged users. In response to the Cybersecurity Sprint, the IRS developed a plan in July 2015 to accelerate mandatory personal identity verification card use and begin to address existing challenges related to privileged users and its legacy system environment.

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.

Figure 1 presents TIGTA's detailed results for the 10 security program areas in response to the DHS's *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*.[6] TIGTA's results will be consolidated with the Treasury OIG's results of non-IRS bureaus and uploaded into the DHS's CyberScope[7] for the OMB's use in developing its annual report to Congress on the Federal Government's progress in meeting key security performance measures.

Figure 1: TIGTA's Responses to the DHS's FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics

1: Continuous Monitoring Management

Status of Continuous Monitoring Management Program [provide maturity level 1 – 5]	1	**1.1.** Utilizing the ISCM maturity model definitions, in conjunction with the attributes outlined in Appendix A, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall. **TIGTA Comments:** The IRS has not yet implemented its ISCM program but stated that it is fully participating in the DHS's Continuous Diagnostics and Mitigation Program to comply with the OMB M-14-03 mandate and is in the process of determining its final toolset to meet the program requirements.
	1	People
	1	Processes
	1	Technology

2: Configuration Management

Status of Configuration Management Program [check one: Yes or No]	**No**	**2.1.** Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**2.1.1.** Documented policies and procedures for configuration management.
	Yes	**2.1.2.** Defined standard baseline configurations.

[6] Many abbreviations in this matrix are used as presented in the original document and are not defined therein. However, we have provided the definitions in the Abbreviations page after the Table of Contents of this report.
[7] An online data collection tool administered by the DHS to collect performance data for FISMA compliance reporting.

	No	**2.1.3.** Assessments of compliance with baseline configurations. **TIGTA Comments:** The IRS has not deployed automated mechanisms to centrally manage, apply, and verify baseline configuration settings and produce FISMA compliance reports using the NIST-defined Security Content Automation Protocol format for all of its information technology assets. The IRS is awaiting the outcome of the DHS's Continuous Diagnostics and Mitigation program Task Order #2 to provide the toolset to meet the program requirements.
	No	**2.1.4.** Process for timely (as specified in organization policy or standards) remediation of scan result deviations. **TIGTA Comments:** The IRS has not yet fully implemented configuration baseline scanning tools and processes on all systems to ensure timely remediation of scan result deviations.
	Yes	**2.1.5.** For Windows-based components, USGCB secure configuration settings are fully implemented and any deviations from USGCB baseline settings are fully documented.
	No	**2.1.6.** Documented proposed or actual changes to the hardware and software configurations. **TIGTA Comments:** The IRS has not yet fully implemented configuration and change management controls to ensure that proposed or actual changes to hardware and software configurations are documented and controlled.
	No	**2.1.7.** Implemented software assessing (scanning) capabilities. (NIST SP 800-53: RA-5, SI-2) **TIGTA Comments:** The IRS has not implemented software assessment (scanning) on all systems.
	No	**2.1.8.** Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards. (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2) **TIGTA Comments:** The IRS has not yet fully implemented configuration-related vulnerability scanning tools and processes on all systems to ensure timely remediation of scan result deviations.
	No	**2.1.9.** Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2) **TIGTA Comments:** The IRS has not implemented a Service-wide process to ensure timely installation of software patches on all platforms.
		2.2. Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above.

	No	**2.3.** Does the organization have an enterprise deviation handling process and is it integrated with the automated capability? **TIGTA Comments:** The IRS does not have an enterprise deviation handling process that is integrated with the automated capability for all of its information technology assets. A number of its assessment activities involve manual processes.
	No	**2.3.1.** Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented. **TIGTA Comments:** The IRS has established a process for accepting the risk introduced by deviations, but it is not integrated with the automated capability.

3: Identity and Access Management

Status of Identity and Access Management Program [check one: Yes or No]	**No**	**3.1.** Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and that identifies users and network devices? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**3.1.1.** Documented policies and procedures for account and identity management. (NIST SP 800-53: AC-1)
	No	**3.1.2.** Identifies all users, including Federal employees, contractors, and others who access organization systems. (HSPD-12, NIST SP 800-53: AC-2) **TIGTA Comments:** The IRS cannot yet uniquely identify all users who access its systems in compliance with HSPD-12.
	No	**3.1.3.** Organization has planned for implementation of personal identity verification for logical access in accordance with government policies (HSPD-12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). **TIGTA Comments:** The IRS's plans did not fully address existing challenges relating to privileged user access and its legacy system environment to ensure success in achieving full and timely compliance with HSPD-12 for logical access.

	No	**3.1.4.** Organization has planned for implementation of personal identity verification for physical access in accordance with Government policies (HSPD-12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). **TIGTA Comments:** The IRS's plans did not fully address existing challenges (including funding challenges) to achieving full and timely compliance with HSPD-12 for physical access.
	No	**3.1.5.** Ensures that the users are granted access based on needs and separation-of-duties principles. **TIGTA Comments:** During FY 2015, the Government Accountability Office (GAO) identified users that had been granted more access than needed and instances in which the separation-of-duties principle was not enforced.
	No	**3.1.6.** Distinguishes hardware assets that have user accounts (*e.g.*, desktops, laptops, servers) from those without user accounts (*e.g.*, Internet Protocol phones, faxes, printers). **TIGTA Comments:** The IRS is still in the process of implementing technical solutions and introducing automated tools to achieve full asset discovery and asset management in accordance with policy.
	No	**3.1.7.** Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy. **TIGTA Comments:** During FY 2015, the TIGTA and the GAO identified systems that do not have controls in place to ensure that accounts are terminated or deactivated once access is no longer needed.
	No	**3.1.8.** Identifies and controls use of shared accounts. **TIGTA Comments:** During FY 2015, the TIGTA and the GAO identified improper use of shared accounts; for example, use of generic administrator accounts and passwords.
		3.2. Please provide any additional information on the effectiveness of the organization's Identity and Access Management that was not noted in the questions above. **TIGTA Comments:** In mid-June 2015, the Federal Chief Information Officer launched a 30-day Cybersecurity Sprint instructing Federal agencies to take a number of steps to further protect Federal information and assets and improve the resilience of Federal networks. As part of the Cybersecurity Sprint, agencies were instructed to dramatically accelerate the implementation of personal identity verification card use, especially for privileged users. In response to the Cybersecurity Sprint, the IRS developed a plan in July 2015 to accelerate mandatory personal identity verification card use and begin to address existing challenges related to privileged users and its legacy system environment.

4: Incident Response and Reporting

Status of Incident Response and Reporting Program [check one: Yes or No]	Yes	**4.1.** Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**4.1.1.** Documented policies and procedures for detecting, responding to, and reporting incidents. (NIST SP 800-53: IR-1)
	Yes	**4.1.2.** Comprehensive analysis, validation, and documentation of incidents.
	Yes	**4.1.3.** When applicable, reports to US-CERT within established time frames. (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19)[8]
	Yes	**4.1.4.** When applicable, reports to law enforcement and the agency Inspector General within established time frames. (NIST SP 800-61)
	Yes	**4.1.5.** Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage. (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19)
	Yes	**4.1.6.** Is capable of correlating incidents.
	Yes	**4.1.7.** Has sufficient incident monitoring and detection coverage in accordance with Government policies. (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19)
		4.2. Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.

5: Risk Management

Status of Risk Management Program [check one: Yes or No]	Yes	**5.1.** Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**5.1.1.** Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev.1.

[8] NIST, NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide* (Aug. 2012); OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 2006); OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 2007).

	Yes	**5.1.2.** Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1.
	Yes	**5.1.3.** Addresses risk from an information system perspective and is guided by the risk decisions from the organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1.
	Yes	**5.1.4.** Has an up-to-date system inventory.
	Yes	**5.1.5.** Categorizes information systems in accordance with Government policies.
	Yes	**5.1.6.** Selects an appropriately tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.
	Yes	**5.1.7.** Implements the approved set of tailored baseline security controls specified in metric 5.1.6.
	Yes	**5.1.8.** Assesses the security controls using appropriate assessment procedures to determine 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 system.
	Yes	**5.1.9.** Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
	Yes	**5.1.10.** Information system–specific risks (tactical), mission/business–specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.
	Yes	**5.1.11.** Senior officials are briefed on threat activity on a regular basis by appropriate personnel (*e.g.*, Chief Information Security Officer).
	Yes	**5.1.12.** Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system–related security risks.
	Yes	**5.1.13.** Security authorization package contains system security plan, security assessment report, POA&M, and accreditation boundaries in accordance with Government policies for organization information systems. (NIST SP 800-18, 800-37)
	Yes	**5.1.14.** The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.

	Yes	**5.1.15.** For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems.
		5.2. Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above.

6: Security Training

Status of Security Training Program [check one: Yes or No]	Yes	**6.1.** Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**6.1.1.** Documented policies and procedures for security awareness training. (NIST SP 800-53: AT-1)
	Yes	**6.1.2.** Documented policies and procedures for specialized training for users with significant information security responsibilities.
	Yes	**6.1.3.** Security training content based on the organization and roles, as specified in organization policy or standards.
	Yes	**6.1.4.** Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training.
	No	**6.1.5.** Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training. **TIGTA Comments:** The IRS does not identify and track the status of specialized training for all of its contractor employees with significant information security responsibilities that require specialized training.
	Yes	**6.1.6.** Training material for security awareness training contains appropriate content for the organization. (NIST SP 800-50, 800-53)
		6.2. Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.

7: Plan of Action & Milestones (POA&M)

Status of POA&M Program [check one: Yes or No]	Yes	**7.1.** Has the organization established a POA&M Program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**7.1.1.** Documented policies and procedures for managing information technology security weaknesses discovered during security control assessments and that require remediation.
	Yes	**7.1.2.** Tracks, prioritizes, and remediates weaknesses.
	No	**7.1.3.** Ensures that remediation plans are effective for correcting weaknesses. **TIGTA Comments:** The IRS did not always ensure that weaknesses were corrected prior to POA&M closure. The 10 systems we evaluated closed a total of 43 POA&Ms during FY 2015. Of the 43 POA&M closures, 22 were closed without sufficient evidence that the weakness was corrected. However, the IRS's POA&M validation processes did not fail the closure of 13 of the 22. The IRS confirmed that five of the 13 POA&Ms had not been corrected, and it could not provide sufficient evidence to support the closure of an additional three. The IRS subsequently uploaded artifacts that justified closure for the remaining five POA&Ms.
	Yes	**7.1.4.** Establishes and adheres to milestone remediation dates and provides adequate justification for missed remediation dates.
	Yes	**7.1.5.** Ensures resources and ownership are provided for correcting weaknesses.
	Yes	**7.1.6.** POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weaknesses due to a risk-based decision to not implement a security control). (OMB M-04-25)
	Yes	**7.1.7.** Costs associated with remediating weaknesses are identified in terms of dollars. (NIST SP 800-53: PM-3; OMB M-04-25)
	Yes	**7.1.8.** Program officials report progress on remediation to the Chief Information Officer on a regular basis, at least quarterly, and the Chief Information Officer centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly. (NIST SP 800-53: CA-5; OMB M-04-25)
		7.2. Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above.

8: Remote Access Management

Status of Remote Access Management Program [check one: Yes or No]	Yes	**8.1.** Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**8.1.1.** Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access. (NIST SP 800-53: AC-1, AC-17)
	Yes	**8.1.2.** Protects against unauthorized connections or subversion of authorized connections.
	No	**8.1.3.** Users are uniquely identified and authenticated for all access. (NIST SP 800-46, Section 4.2, Section 5.1) **TIGTA Comments:** The IRS had not fully implemented unique user identification and authentication that complies with HSPD-12. In addition, system administrators of the virtual private network infrastructure and server components do not use NIST-compliant multifactor authentication for local or network access to privileged accounts.
	Yes	**8.1.4.** Telecommuting policy is fully developed. (NIST SP 800-46, Section 5.1)
	No	**8.1.5.** Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. **TIGTA Comments:** The IRS had not fully implemented remote electronic authentication that complies with HSPD-12.
	Yes	**8.1.6.** Defines and implements encryption requirements for information transmitted across public networks.
	Yes	**8.1.7.** Remote access sessions, in accordance to OMB M-07-16, are timed out after 30 minutes of inactivity, after which reauthentication is required.
	Yes	**8.1.8.** Lost or stolen devices are disabled and appropriately reported. (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines)
	Yes	**8.1.9.** Remote access rules of behavior are adequate in accordance with Government policies. (NIST SP 800-53: PL-4)
	Yes	**8.1.10.** Remote access user agreements are adequate in accordance with Government policies. (NIST SP 800-46, Section 5.1; NIST SP 800-53: PS-6)
		8.2. Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.
	Yes	**8.3.** Does the organization have a policy to detect and remove unauthorized (rogue) connections?

9: Contingency Planning

Status of Contingency Planning Program [check one: Yes or No]	Yes	**9.1.** Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**9.1.1.** Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster. (NIST SP 800-53: CP-1)
	Yes	**9.1.2.** The organization has incorporated the results of its system's Business Impact Analysis and Business Process Analysis into the analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan. (NIST SP 800-34)
	Yes	**9.1.3.** Development and documentation of division, component, and information technology infrastructure recovery strategies, plans, and procedures. (NIST SP 800-34)
	Yes	**9.1.4.** Testing of system-specific contingency plans.
	Yes	**9.1.5.** The documented business continuity and disaster recovery plans are in place and can be implemented when necessary. (FCD1, NIST SP 800-34)
	Yes	**9.1.6.** Development of test, training, and exercise programs. (FCD1, NIST SP 800-34, NIST SP 800-53)
	Yes	**9.1.7.** Testing or exercising of business continuity and disaster recovery plans to determine effectiveness and to maintain current plans.
	Yes	**9.1.8.** After-action report that addresses issues identified during contingency/disaster recovery exercises. (FCD1, NIST SP 800-34)
	Yes	**9.1.9.** Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for systems that require them. (FCD1, NIST SP 800-34, NIST SP 800-53)
	Yes	**9.1.10.** Backups of information that are performed in a timely manner. (FCD1, NIST SP 800-34, NIST SP 800-53)
	Yes	**9.1.11.** Contingency planning that considers supply chain threats.
		9.2. Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.

10: Contractor Systems

Status of Contractor Systems Program [check one: Yes or No]	Yes	**10.1.** Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**10.1.1.** Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities (including other Government agencies), including organization systems and services residing in a public cloud, hybrid, or private cloud.
	Yes	**10.1.2.** The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines. (NIST SP 800-53: CA-2)
	Yes	**10.1.3.** A complete inventory of systems operated on the organization's behalf by contractors or other entities (including other Government agencies), including organization systems and services residing in a public cloud, hybrid, or private cloud.
	Yes	**10.1.4.** The inventory identifies interfaces between these systems and organization-operated systems. (NIST SP 800-53: PM-5)
	No	**10.1.5.** The organization requires appropriate agreements (*e.g.*, Memorandums of Understanding, Interconnection Security Agreements, contracts, *etc.*) for interfaces between these systems and those that it owns and operates. **TIGTA Comments:** The IRS did not have sufficient processes to ensure that interfaces between IRS and contractor systems have appropriate agreements.
	Yes	**10.1.6.** The inventory of contractor systems is updated at least annually.
		10.2. Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of this independent evaluation was to assess the effectiveness of the IRS's information technology security program and practices and their compliance with FISMA requirements for the period July 1, 2014, to June 30, 2015. To accomplish our objective, we responded to the questions provided in the DHS *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, issued on June 19, 2015. The questions related to the following 10 security program areas:

1. Continuous Monitoring Management.
2. Configuration Management.
3. Identity and Access Management.
4. Incident Response and Reporting.
5. Risk Management.
6. Security Training.
7. Plan of Action and Milestones.
8. Remote Access Management.
9. Contingency Planning.
10. Contractor Systems.

We based our evaluation work, in part, on a representative subset of 10 major IRS information systems. We used the system inventory contained within the Treasury FISMA Information Management System of major applications and general support systems with a security classification of "Moderate" or "High" as the population for this subset.

We also considered the results of TIGTA audits completed during the FY 2015 FISMA evaluation period, as listed in Appendix IV, as well as audit reports from the GAO that contained results applicable to the FISMA questions.

Appendix II

Major Contributors to This Report

Danny Verneuille, Acting 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
Mary Jankowski, Senior Auditor
Esther Wilson, Senior Auditor
Chinita Coates, Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
Chief Technology Officer OS:CTO
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Director, Office of Audit Coordination OS:PPAC:AC
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
- Business Planning and Risk Management OS:CTO:SP:BPRM
- Cybersecurity OS:CTO:C

Appendix IV

Treasury Inspector General for Tax Administration Information Technology Security-Related Reports Issued During the Fiscal Year 2015 Evaluation Period

1. TIGTA, Ref. No. 2014-20-071, *Information Technology: Improvements Are Needed to Successfully Plan and Deliver the New Taxpayer Advocate Service Integrated System* (Sept. 2014).
2. TIGTA, Ref. No. 2014-20-094, *While the Financial Institution Registration System Deployed on Time, Improved Controls Are Needed* (Sept. 2014).
3. TIGTA, Ref. No. 2014-20-063, *Customer Account Data Engine 2 Database Validation Is Progressing; However, Data Coverage, Data Defect Reporting, and Documentation Need Improvement* (Sept. 2014).
4. TIGTA, Ref. No. 2014-20-088, *The Information Reporting and Document Matching Case Management System Could Not Be Deployed* (Sept. 2014).
5. TIGTA, Ref. No. 2014-20-042, *The Internal Revenue Service Should Improve Server Software Asset Management and Reduce Costs* (Sept. 2014).
6. TIGTA, Ref. No. 2014-20-087, *While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget* (Sept. 2014).
7. TIGTA, Ref. No. 2014-20-092, *The Internal Revenue Service Does Not Adequately Manage Information Technology Security Risk-Based Decisions* (Sept. 2014).
8. TIGTA, Ref. No. 2014-20-083, *The Internal Revenue Service Should Implement an Efficient Internal Information Security Continuous Monitoring Program That Meets Its Security Needs* (Sept. 2014).
9. TIGTA, Ref. No. 2014-20-059, *The Office of Safeguards Should Improve Management Oversight and Internal Controls to Ensure the Effective Protection of Federal Tax Information* (Sept. 2014).
10. TIGTA, Ref. No. 2014-20-069, *Progress Has Been Made; However, Significant Work Remains to Achieve Full Implementation of Homeland Security Presidential Directive 12* (Sept. 2014).
11. TIGTA, Ref. No. 2015-20-031, *Planning Decisions for Customer Account Data Engine 2 Transition State 2 Should Be Effectively Linked to Actions Needed to Address the Internal Revenue Service's Financial Material Weakness* (May 2015).

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