Evaluation Report

OIG-CA-15-004

INFORMATION TECHNOLOGY: Department of the Treasury Federal Information Security Management Act Fiscal Year 2014 Evaluation

November 6, 2014

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 6, 2014

MEMORANDUM FOR NANI COLORETTI
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: Evaluation Report – *Department of the Treasury Federal Information Security Management Act Fiscal Year 2014 Evaluation*

We are pleased to transmit the following reports:

- *Department of the Treasury Federal Information Security Management Act Fiscal Year 2014 Evaluation,* dated October 28, 2014 (Attachment 1)

- *Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2014,* dated September 23, 2014 (Attachment 2)

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to have an annual independent evaluation of their information security program and practices performed and to report evaluation 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 annual evaluation be performed by the agency Inspector General or an independent external auditor as determined by the Inspector General. To meet our FISMA requirements, we contracted with KPMG LLP (KPMG), an independent certified public accounting firm, to perform the FISMA evaluation of Treasury's unclassified systems, except for those of the Internal

Revenue Service (IRS), which was performed by the Treasury Inspector General for Tax Administration (TIGTA). KPMG conducted its evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

In its report on Treasury's non-IRS bureaus' unclassified systems, KPMG concluded that Treasury established an information security program and related practices consistent with applicable FISMA requirements, OMB policy, and National Institute of Standards and Technology standards and guidelines. Although the security program has been established, KPMG identified needed improvements within 7 of 11 security program areas as follows: identity and access management, incident and response reporting, risk management, security training, contingency planning, Plan of Actions & Milestones, and configuration management. Accordingly, KMPG made 28 recommendations to the responsible officials to address noted deficiencies.

With respect to IRS's unclassified systems, TIGTA reported that IRS established an information security program and related practices covering the 11 security program areas. However, TIGTA found that 6 of the 11 security program areas did not fully meet the performance metrics specified in the DHS guidelines as follows: continuous monitoring management, incident response and reporting, security training, remote access management, configuration management, and identity and access management.

In connection with contract oversight of KPMG, we reviewed KPMG's report and related documentation and inquired of its representatives. Our review, as differentiated from an evaluation performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*, was not intended to enable us to conclude about the effectiveness of Treasury's information security program or its compliance with FISMA. KPMG is responsible for its report and the conclusions expressed therein.

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

Attachments

cc: Michael E. McKenney
Deputy Inspector General for Audit
Treasury Inspector General for Tax Administration

Edward A. Roback
Associate Chief Information Officer for Cyber Security
Departmental Offices

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 1

Department of the Treasury
Federal Information Security Management Act
Fiscal Year 2014 Evaluation
October 28, 2014

THIS PAGE INTENTIONALLY LEFT BLANK

Department of the Treasury
Federal Information Security Management Act
Fiscal Year 2014 Evaluation

October 28, 2014

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

Department of the Treasury
Federal Information Security Management Act Fiscal Year 2014 Evaluation

Table of Contents

FISMA Evaluation Report

Appendices

KPMG LLP
1676 International Drive
McLean, VA 22102

The Honorable Eric Thorson
Inspector General, Department of the Treasury
1500 Pennsylvania Avenue NW
Room 4436
Washington, DC 20220

Re: Department of the Treasury's Federal Information Security Management Act Fiscal Year 2014 Evaluation

Dear Mr. Thorson:

This report presents the results of our independent evaluation of the Department of the Treasury's (Treasury) information security program and practices. The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies, including the Treasury, 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 (OMB). OMB has delegated its responsibility to Department of Homeland Security (DHS) for the collection of annual FISMA responses. DHS has prepared the FISMA 2014 questionnaire to collect these responses. Appendix III, *Department of the Treasury's Consolidated Response to DHS's FISMA 2014 Questions for Inspectors General,* provides the Treasury's response to the questionnaire. FISMA requires that the agency Inspector General (IG) or an independent external auditor perform the independent evaluation as determined by the IG. The Treasury Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct this independent evaluation.

We conducted our independent evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation.

The objectives for this independent evaluation were to assess Treasury's information security program and practices for the period July 1, 2013 to June 30, 2014 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 2014 Questions for Inspectors General*. Additional details regarding the scope of our independent evaluation are included in Appendix I, *Objectives, Scope & Methodology*.

Treasury has established an information security program and practices for its non-IRS bureaus' unclassified systems consistent with applicable FISMA requirements, OMB policy and guidelines, and

the National Institute of Standards and Technology (NIST) standards and guidelines. This program covers the 11 FISMA program areas.[1] However, while the security program has been implemented across Treasury for its non-IRS bureaus, we identified 8 findings within 7 of the 11 FISMA program areas that needed improvements:

1. **Identity and Access Management:** Logical account management activities, such as access authorizations, were not in place or not consistently performed by Financial Crimes Enforcement Network (FinCEN), the Bureau of the Fiscal Service (Fiscal Service) and the Office of the Comptroller of the Currency (OCC).
2. **Incident and Response Reporting:** Bureau of Engraving and Printing (BEP), Departmental Offices (DO), and OIG did not report security incidents timely or correctly according to United States Computer Emergency Readiness Team (US-CERT) and Treasury recommended guidelines.
3. **Risk Management:** DO, Fiscal Service, and the United States Mint (Mint) did not implement the NIST Special Publication (SP) 800-53, Revision 4, security controls for some of their System Security Plans (SSPs) and security assessments.
4. **Security Training:** Evidence of successful completion of annual security awareness training was not retained for some users at the Community Development Financial Institutions (CDFI) Fund, DO, and Mint.
5. **Risk Management:** Bureau information technology (IT) security and configuration management policies had not been updated or reviewed by BEP and FinCEN to address NIST and Treasury requirements.
6. **Contingency Planning:** Mint did not update or review their contingency plan, or finalize their contingency plan test results.
7. **Plan of Actions & Milestones (POA&Ms):** POA&Ms were not tracked in accordance with NIST and Treasury requirements at DO.
8. **Configuration Management:** OIG did not conduct or document a United States Government Configuration Baseline (USGCB) baseline review and document deviations.

We have made 28 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 Acting Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO) agreed with our findings and recommendations (see *Management Response*).

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

[1] The 11 FISMA program areas are: continuous monitoring management, configuration management, identity and access management, incident and response reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, contractor systems, and security capital planning.

Appendix I describes the FISMA evaluation's objectives, scope, and methodology. Appendix II, *Status of Prior-Year Findings*, summarizes Treasury's progress in addressing prior-year recommendations. Appendix III provides *Department of the Treasury's Consolidated Response to DHS's FISMA 2014 Questions for Inspectors General*. 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.

Sincerely,

KPMG LLP

October 28, 2014

BACKGROUND

Federal Information Security Management Act of 2002 (FISMA)

Title III of the E-Government Act of 2002, 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. FISMA assigns specific responsibilities to agency heads and Inspectors Generals (IGs) in complying with requirements of FISMA. FISMA is supported by the Office of Management and Budget (OMB) directives, 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. OMB has delegated some responsibility to the Department of Homeland Security (DHS) in memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*, 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. 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 2014 FISMA evaluation 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, *The Department of the Treasury's Consolidated Response to DHS's FISMA 2014 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 EVALUATION RESULTS

Treasury has established an information security program and related practices for its non-IRS bureaus' unclassified systems consistent with applicable FISMA requirements, OMB policy, and NIST guidelines. This program covers the 11 FISMA program areas outlined in the *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics* that were prepared by U.S. Department of Homeland Security Office of Cybersecurity and Communications Federal Network Resilience. The 11 program areas are continuous monitoring management, configuration management, identity and access management, incident and response reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, contractor systems, and security capital planning.[2] However, while the security program has been implemented across the Treasury for its non-IRS bureaus, we identified 8 findings within 7 of the 11 FISMA program areas that needed improvements. We have made 28 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. In a written response to this report, the Treasury Acting 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 2015 independent evaluation.

Additionally, we evaluated the prior-year findings from the fiscal year (FY) 2013 FISMA Evaluation and the FY 2012 and 2011 FISMA Evaluation as a performance audit and noted that management had closed 8 of 18 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, such as access authorizations, were not in place or not consistently performed by FinCEN, Fiscal Service, and OCC

We identified instances of noncompliance with Treasury, bureau-, and system-level logical access policies at FinCEN, Fiscal Service, and OCC. This control falls under the identity and access management FISMA program area. We noted the following:

1. Access authorization activities were not consistently performed as required by TD P 85-01 Volume I, *Treasury Information Technology Security Program*, and bureau-specific policies at FinCEN and Fiscal Service.
   - 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 actually not a "new" user, but instead a key team member whose account was created in the system prior to implementation to production, and still remains an active user of the system. *(See Recommendation #1.)*
   - 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. *(See Recommendation #2.)*
2. 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 unexpectantly, they informally designated a new ISSO and gave that individual permission to authorize access to the system. *(See Recommendations #3 and #4.)*
3. 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. *(See Recommendation #5 and #6.)*

These control deficiencies demonstrate that these bureaus did not appropriately implement policies for approving and reviewing user access. 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. In, addition, the risk of an unauthorized user gaining access to the system is increased when the ISSO has not been formally appointed.

We recommend that FinCEN management:

1. For the selected system, ensure access forms are complete, properly reviewed prior to granting access, and centrally retained by the service desk

We recommend that Fiscal Service management:

2. For the selected system, implement a new process to ensure that all administrative accounts are approved and that evidence of access approval is retained.

3. For the selected system, ensure only authorized approvers grant new user account access.

4. For the selected system, reapprove all existing users under the new process to ensure their access is appropriate.

We recommend that OCC management:

5. 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

6. For the selected system, ensure that segregation of duties controls are implemented, disallowing users to approve and modify their own access requests.

2. BEP, DO, and OIG did not report security incidents timely or correctly according to United States Computer Emergency Readiness Team (US-CERT) and Treasury recommended guidelines

Treasury bureaus are required to submit all security incidents to the TCSIRC within specified time frames categorized by incident severity. We identified that BEP, DO, and OIG reported incidents later than US-CERT and Treasury recommended guidelines. We also noted that DO reported a Category (CAT) 1[3] incident incorrectly as a CAT 6[4] incident. This control falls under the incident and response reporting FISMA program area. Specifically, we noted the following:

- 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. *(See Recommendations #7 and #8.)*
- 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, respectively, 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. *(See Recommendation #9 and #10.)*
- 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

[3] CAT 1 Unauthorized Access - In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource. The reporting requirement is within one hour of discovery/detection.
[4] CAT 6: Investigation – Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. The reporting requirement is not applicable as this category is for each agency's user to categorize a potential incident that is currently being investigated.

leave, and there was no backup to submit incident tickets to TCSIRC. *(See Recommendation #11.)*

By not reporting security incidents in a timely manner and under the correct categorization, these bureaus and offices increase the risk of unauthorized access, or denial of service attacks, posed to their information system while the incident remains unreported. Additionally, by not reporting incidents correctly, bureaus and offices can impair the TSIRC's and the US-CERT's ability to track, analyze, and act on aggregated incident data within prescribed timeframes.

We recommend that BEP management:

7. Provide training to the BEP CSIRC team regarding BEPs incident response policies and procedures to ensure the timely reporting of incidents.

8. Ensure that BEP CSIRC reports all CAT 1 incidents to TCSIRC within one (1) hour of discovery/detection.

We recommend that DO management:

9. Provide training to the DO CSIRC team on DO's incident response policies and procedures.

10. Ensure that DO CSIRC reports all incidents to TCSIRC in compliance with their standard operating procedures.

We recommend that OIG management:

11. Ensure that there are an adequate number of available trained security officers who have access to the TCSIRC portal to report security incidents.

3. DO, Fiscal Service, and Mint did not implement the NIST SP 800-53, Rev. 4, security controls for some of their SSPs and security assessments

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 one 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. Specifically, we noted that:

- 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. *(See Recommendations #12 and #13.)*
- 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. *(See Recommendation #14, #15, and #16.)*

- 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. *(See Recommendations #17 and #18.)*

Failing to document an up-to-date baseline of security controls 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 DO management:

12. For the selected system, update the SSP to address and reference NIST SP 800-53, Rev. 4, controls and control enhancements.

13. 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.

We recommend that Fiscal Service management:

14. For the selected system, update the SSP to address and reference NIST SP 800-53, Rev. 4, controls.

15. For the selected systems, implement the NIST SP 800-53, Rev. 4, controls and then update the SSPs to reflect these new controls.

16. For the selected systems, ensure that the annual assessments reflect all of the new and updated controls in NIST SP 800-53 Rev. 4.

We recommend that Mint management:

17. For the selected systems, review and update the SSP to include all relevant controls from the NIST SP 800-53, Rev. 4, final version.

18. For the selected systems, ensure Rev. 4 controls and enhancements are implemented on the system and tested promptly.

4. Evidence of successful completion of annual security awareness training was not retained for some users at CDFI Fund, DO, and Mint

NIST SP 800-53, Rev. 4, and the TD P 85-01 require that all users complete IT Security Awareness Training on an annual basis. Additionally, Treasury guidance requires that individual training records are to be retained for a period of five years. This control falls under the security training FISMA program area. Specifically, we noted the following:

- 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. *(See Recommendations #19 and #20.)*
- 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. *(See Recommendation #21.)*
- 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. *(See Recommendations #22 and #23.)*

Annual security awareness training, as required by TD P 85-01, is essential to verify that users have been made aware of system or application rules, their responsibilities, and their expected behavior. Without the ability to verify that security awareness training is being completed by every employee, management cannot ensure that employees are properly aware of the systems or application rules, their responsibilities, and their expected behavior, thereby not adequately protecting IT resources and data from being compromised.

We recommend that CDFI Fund management:

19. 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.

20. Ensure that all contractors complete the annual Security Awareness training.

We recommend that DO management:

21. Ensure that users are completing the annual security awareness training and retain evidence of their user's successful completion of the annual training.

We recommend that Mint management:

22. Ensure that all detailees provide evidence of their successful completion of the annual Security Awareness Training to the Mint.

23. Review and increase the frequency of notifying users not compliant with annual security training requirements.

5. Bureau IT security and configuration management policies had not been updated or reviewed to address NIST and Treasury requirements at BEP and FinCEN

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 following:

- 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.
- 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. *(See Recommendations #24 and #25.)*

Having policies not updated to reflect the most current NIST publications, could result in insufficient guidance to protect the confidentiality, integrity, and availability of information maintained by the bureau's systems by referencing out of date and potentially inaccurate information.

Based on the planned corrective actions for BEP, we are not making a recommendation.

We recommend that FinCEN management:

24. Perform a routine review of the Configuration Management policy document and ensure the Configuration Management policy includes the latest NIST requirements.

25. Ensure FinCEN policies and procedures are periodically reviewed and updated for significant changes.

6. Mint did not update or review their contingency plan, or finalize their contingency plan test results

The TD P 85-01 requires Treasury bureaus and offices to protect their information systems in the event of a disaster. Bureaus must create plans for system recovery and test these plans. Mint did not fully implement contingency planning (planning and testing) controls as required by TD P 85-01 Volume I, NIST SP 800-53, Rev. 4, and NIST SP 800-34 guidance. These controls fall under the contingency planning FISMA program area. 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 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. Mint was aware that the contingency plan had not been updated and the contingency plan test and exercises had not been finalized or signed-off by the contingency planning personnel. This was due to a transition in the IT contractor support in June 2013, combined with the inability to obtain proper contingency planning documentation from the IT services provider, despite ongoing attempts. *(See Recommendations #26 and #27.)*

Contingency plans and contingency plan testing, as required by NIST SP 800-53, Rev. 3, and NIST SP 800-34, are paramount in assuring that Mint information systems can remain operational with the least amount of downtime possible in emergencies. Failure to appropriately test recovery capabilities could result in the unavailability of critical Mint information and information systems in the event of a disaster.

We recommend that Mint management:

26. For the selected system, update the Contingency Plan.

27. 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.

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

Treasury has provided guidance on POA&M creation and tracking through TD P 85-01 Volume I. This policy 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 additional necessary resources. This control falls under the POA&M FISMA program area. 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.

By not recording identified information security weaknesses in POA&Ms, these weaknesses may not be addressed in a timely manner and subsequently be exploited by an attacker. Moreover, by not timely recording and updating identified system security vulnerabilities in their POA&M, Treasury bureaus' summary-level security metrics under-report the true number of known security weaknesses to the Treasury OCIO. Additionally, senior Treasury management would be unable to exercise its oversight responsibilities to adjust funding levels, human resources, and requested priorities in response to identified security weaknesses.

Based on the planned corrective actions for DO, we are not making a recommendation.

8. OIG did not conduct or document a United States Government Configuration Baseline (USGCB) baseline review and document deviations

TD P 85-01 requires that all Treasury bureaus and offices document configuration baselines. This control falls under the configuration management FISMA program area. 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. *(See Recommendation #28.)*

Managing the configuration settings of the system is an essential control element within Treasury's risk management and IT security controls framework. Without documenting the USGCB baseline deviation for Windows 7, management cannot provide sufficient control to enforce and maintain settings in the system. This will hinder OIG's attempts to validate and enforce system configuration settings, thus jeopardizing the confidentiality, integrity, and availability of the information systems maintained by the OIG environment and network.

We recommend that OIG management:

28. Conduct a USGCB baseline review for Windows 7 and document deviations.

MANAGEMENT RESPONSE TO THE REPORT

The following is the Treasury CIO's response, dated October 17, 2014, to the FY 2014 FISMA Evaluation Report.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OCT 17 2014

MEMORANDUM FOR TRAM J. DANG
DIRECTOR, INFORMATION TECHNOLOGY AUDIT

FROM: Raghav Vajjhala
Acting Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO)

SUBJECT: Management Response to Draft Evaluation Report – "Fiscal Year 2014 Evaluation of Treasury's Compliance with Federal Information Security Management Act"

Thank you for the opportunity to comment on the draft report entitled, *Fiscal Year 2014 Evaluation of Treasury's Compliance with Federal Information Security Management 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 draft and agree with all findings and recommendations. Please refer to the attachment for further details on our planned corrective actions. We appreciate your noting that some of the findings were actually issues identified by Bureaus through their own security programs.

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:

- Reached or exceeded the Department's targets for the Fiscal Year 2014 Cybersecurity Cross-Agency Priority goals: 1) monitored 98 percent of Treasury IT assets for inventory, configuration, and vulnerability management; 2) routed 99 percent of required network traffic through a Trusted Internet Connection (TIC); 3) met 99 percent of the TIC 2.0 architecture requirements; and, 4) required 44 percent of Treasury users to authenticate to network accounts using their Personal Identity Verification cards;

- Complied with OMB policy on Domain Name Server (DNS) Security by digitally signing 100 percent of external-facing second-level DNS names. This is important to reduce the ability of others to impersonate Treasury websites;

- Completed the Department's strategy for Information Security Continuous Monitoring (ISCM) in accordance with the schedule mandated by OMB requirements for Enhancing the Security of Federal Information and Information

Systems. The Office of the Chief Information Officer identified a mature, compliant approach to ISCM proposed by one Bureau and coordinated with the other Bureaus to adopt the approach Department-wide. This reduced the cost of compliance with the OMB mandate and ensured that Treasury bureaus will implement ISCM programs using a consistent framework;

- Successfully transitioned to a modernized FISMA inventory tool, achieving an integral piece of the Department's transition to Information Security Continuous Monitoring. The tool will enable analysis resulting in improved targeting of resources based on risk factors, and in turn allow Treasury to better mitigate the risks associated with transitioning from a three-year security authorization cycle to ongoing authorizations in accordance with NIST guidance; and,

- 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.

We appreciate the audit recommendations because they will help improve our security posture. If you have any questions, please contact Edward Roback, Associate CIO for Cyber Security, at 202-622-2593.

Attachment

cc: Edward A. Roback

Management Response to KPMG Recommendations

KPMG Finding 1: Logical account management activities, such as access authorizations, were not in place or not consistently performed by FinCEN, Fiscal Service, and OCC.

KPMG Recommendation 1: 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.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The FinCEN will search again for the one user's Fin-18 form. If FinCEN is unable to locate the form, FinCEN will retroactively complete a Fin-18 form to update the user's access. The target completion date is November 30, 2014.
>
> **Responsible Official:** FinCEN, Chief Information Security Officer

KPMG Recommendation 2: 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.

> **Treasury Response:** Treasury agrees with the finding and recommendation. Fiscal Service will ensure all administrative accounts for the selected system are approved and that evidence of access approval is retained. The target completion date is June 30, 2015.
>
> **Responsible Official:** Fiscal Service, Chief Information Officer

KPMG Recommendation 3: We recommend that Fiscal Service management: For the selected system, ensure only authorized approvers grant new user account access.

> **Treasury Response:** Treasury agrees with the finding and recommendation. Fiscal Service will ensure that only authorized approvers grant new user account access in accordance with the selected system's SSP. The target completion date is June 30, 2015.
>
> **Responsible Official:** Fiscal Service, Assistant Commissioner for Payment Management

KPMG Recommendation 4: We recommend that Fiscal Service management: For the selected system, reapprove all existing users under the new process to ensure their access is appropriate.

> **Treasury Response:** Treasury agrees with the finding and recommendation. Fiscal Service will complete a user recertification as scheduled for the selected system. The target completion date is June 30, 2015.
>
> **Responsible Official:** Fiscal Service, Assistant Commissioner for Payment Management

KPMG Recommendation 5: We recommend that OCC management: 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.

Treasury Response: Treasury agrees with the finding and recommendation. The OCC will ensure that policies and procedures are in alignment, and that they specifically address segregation of duties. The completion date of these actions was October 10, 2014.

Responsible Official: OCC, Director for Office of Security

KPMG Recommendation 6: We recommend that OCC management: For the selected system, ensure that segregation of duties controls is implemented, disallowing users to approve and modify their own access requests.

Treasury Response: Treasury agrees with the finding and recommendation. The OCC has implemented technical controls that enforce segregation of duties controls for this system, including controls preventing users from modifying and approving their own access requests. The completion date of these actions was September 15, 2014.

Responsible Official: OCC, Chief Information Officer

KPMG Finding 2: BEP, DO, and OIG did not report security incidents timely or correctly according to United States Computer Emergency Readiness Team (US-CERT) and Treasury recommended guidelines.

KPMG Recommendation 7: We recommend that BEP management: Provide training to the BEP CSIRC team regarding BEPs incident response policies and procedures to ensure the timely reporting of incidents.

Treasury Response: Treasury agrees with the finding and recommendation. The BEP will train the BEP CSRIC team members regarding BEP's incident response policies and procedures to ensure timely reporting of incidents. The target completion date is December 15, 2014.

Responsible Official: BEP, Chief Information Security Officer

KPMG Recommendation 8: We recommend that BEP management: Ensure that BEP CSIRC reports all CAT 1 incidents to TCSIRC within one (1) hour of discovery/detection.

Treasury Response: Treasury agrees with the finding and recommendation. The BEP will train the BEP CSRIC team members regarding BEP's incident response policies and procedures to ensure timely reporting of incidents. The target completion date is December 15, 2014.

Responsible Official: BEP, Chief Information Security Officer

KPMG Recommendation 9: We recommend that DO management: Provide training to the DO CSIRC team on DO's incident response policies and procedures.

Treasury Response: Treasury agrees with the finding and recommendation. The DO has developed and conducted Incident Response Training for Tier 1 Help Desk Analysts for role-based training. This training provided and enhanced the foundation for incident response reporting for Tier 1 Help Desk analysts and closed the associated POA&M. This was completed over a two-week period in June 2014.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 10: We recommend that DO management: Ensure that DO CSIRC reports all incidents to TCSIRC in compliance with their standard operating procedures.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The DO has developed and conducted Incident Response Training for Tier 1 Help Desk Analysts for role-based training. This training provided and enhanced the foundation for incident response reporting for Tier 1 Help Desk analysts and closed the associated POA&M. This was completed over a two-week period in June 2014.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Recommendation 11: 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.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The OIG's management will ensure that there is a trained tertiary security officer who has access to the portal to report security incidents. The target completion date is December 31, 2014.
>
> **Responsible Official:** OIG, Information Technology Director

KPMG Finding 3: DO, Fiscal Service, and Mint did not implement the NIST SP 800-53, Rev. 4, security controls for some of their SSPs and security assessments.

KPMG Recommendation 12: We recommend that DO management: For the selected system, update the SSP to address and reference NIST SP 800-53, Rev. 4, controls and control enhancements.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The DO has verified that the SSP for the selected system was updated in August 2014 to include the NIST SP 800-53, Rev.4 controls and control enhancements.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Recommendation 13: We recommend that DO management: 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.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The DO will ensure that the controls in NIST SP 800-53 Rev. 4 are tested as part of the next annual assessment due by April 2015.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Recommendation 14: We recommend that Fiscal Service management: For the selected system, update the SSP to address and reference NIST SP 800-53, Rev. 4, controls.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The Fiscal Service will incorporate NIST SP 800-53 Revision 4 updates during the selected system's next assessment cycle. The target completion date is April 30, 2015.
>
> **Responsible Official:** Fiscal Service, Chief Information Officer

KPMG Recommendation 15: We recommend that Fiscal Service management: For the selected systems, implement the NIST SP 800-53, Rev. 4, controls and then update the SSPs to reflect these new controls.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The Fiscal Service will incorporate NIST SP 800-53 Revision 4 updates during the system's next assessment cycle. The target completion date is June 30, 2015.
>
> **Responsible Official:** Fiscal Service, Assistant Commissioner for Payment Management

KPMG Recommendation 16: We recommend that Fiscal Service management: For the selected systems, ensure that the annual assessments reflect all of the new and updated controls in NIST SP 800-53 Rev. 4.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The Fiscal Service will incorporate NIST SP 800-53 Revision 4 updates during the system's next assessment cycle. The target completion date is June 30, 2015.
>
> **Responsible Official:** Fiscal Service, Assistant Commissioner for Payment Management

KPMG Recommendation 17: We recommend that Mint: For the selected systems, review and update the SSP to include all relevant controls from the NIST SP 800-53, Rev. 4, final version.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The Mint will update the existing SSP to ensure all relevant controls and enhancements from the final NIST SP 800-53 Rev. 4 are incorporated in the SSP and test the additional controls upon completion of updates. The target completion date is December 1, 2014.
>
> **Responsible Official:** Mint, Chief Information Security Officer

KPMG Recommendation 18: We recommend that Mint: For the selected systems, ensure Rev. 4 controls and enhancements are implemented on the system and tested promptly.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The Mint will update the existing SSP to ensure all relevant controls and enhancements from the final NIST SP 800-53 Rev. 4 are incorporated in the SSP and test the additional controls upon completion of updates. The target completion date is December 1, 2014.
>
> **Responsible Official:** Mint, Chief Information Security Officer

KPMG Finding 4: Evidence of successful completion of annual security awareness training was not retained for some users at CDFI Fund, DO, and Mint.

KPMG Recommendation 19: We recommend that CDFI Fund management: 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.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The CDFI Fund maintains Standard Operating Procedures (SOPs) for the onboarding of contractors. The CDFI Fund has revised these SOPs to include periodic reviews to ensure the list of contractors is current and complete. The completion date of these actions was August 23, 2014.

Responsible Official: CDFI, Fund Chief Information Officer

KPMG Recommendation 20: We recommend that CDFI Fund management: Ensure that all contractors complete the annual Security Awareness training.

Treasury Response: Treasury agrees with the finding and recommendation. The CDFI Fund will continue to ensure that all contractors complete the annual Cyber Security training. The completion date of this action was August 23, 2014.

Responsible Official: CDFI, Fund Chief Information Officer

KPMG Recommendation 21: 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.

Treasury Response: Treasury agrees with the finding and recommendation. DO will work with Human Resources to improve employee completion of Security Awareness Training throughout the year. The target completion date is June 30, 2015.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 22: We recommend that Mint management: Ensure that all detailees provide evidence of their successful completion of the annual Security Awareness Training to the Mint.

Treasury Response: Treasury agrees with the finding and recommendation. The Mint will update existing United States Mint INFOSEC Awareness and Training Policy to include processes and procedures for: 1) requesting a copy of the certificate for completion of annual security awareness training from detailees upon identification of non-completion status for United States Mint users and 2) add a Reporting Cycle section to the policy to identify and establish frequency for reporting of non-completions during the reporting period. The target completion date is December 15, 2014.

Responsible Official: Mint Chief Information Security Officer

KPMG Recommendation 23: We recommend that Mint management: Review and increase the frequency of notifying users not compliant with annual security training requirements.

Treasury Response: Treasury agrees with the finding and recommendation. The Mint will update existing United States Mint INFOSEC Awareness and Training Policy to include processes and procedures for: 1) requesting a copy of the certificate for completion of annual security awareness training from detailees upon identification of non-completion status for United States Mint users and 2) add a Reporting Cycle section to the policy to identify and establish frequency for reporting of non-completions during the reporting period. The target completion date is December 15, 2014.

Responsible Official: Mint, Chief Information Security Officer

KPMG Finding 5: Bureau IT security and configuration management policies had not been updated or reviewed to address NIST and Treasury requirements at BEP and FinCEN.

KPMG Recommendation 24: We recommend that FinCEN management: Perform a routine review of the Configuration Management policy document and ensure the Configuration Management policy includes the latest NIST requirements.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The FinCEN will update all of its cyber security policies, including the Configuration Management Policy, to include applicable references to NIST SP 800-53 revision 4 and NIST SP 800-70 Rev. 2. The target completion date is December 30, 2014.
>
> **Responsible Official:** FinCEN, Chief Information Security Officer

KPMG Recommendation 25: We recommend that FinCEN management: Ensure FinCEN policies and procedures are periodically reviewed and updated for significant changes.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The FinCEN will update all of its cyber security policies, including the Configuration Management Policy, to include applicable references to NIST SP 800-53 revision 4 and NIST SP 800-70 Rev. 2. The target completion date is December 30, 2014.
>
> **Responsible Official:** FinCEN, Chief Information Security Officer.

KPMG Finding 6: Mint did not update or review their contingency plan, or finalize their contingency plan test results.

KPMG Recommendation 26: We recommend that Mint management: For the selected system, update the Contingency Plan.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The Mint will develop a project schedule with the system owner for updating contingency plan and development of annual contingency plan test scenarios for the execution of annual exercises. The Mint will submit contingency plans to key contingency personnel for review and approval prior to execution of annual exercises; and for review and signed approval for lessons learned at the conclusion of annual contingency plan tests and exercises. The target completion date is January 30, 2015.
>
> **Responsible Official:** Mint, Chief Information Security Officer

KPMG Recommendation 27: We recommend that Mint management: 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.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The Mint will develop a project schedule with the system owner for updating contingency plan and development of annual contingency plan test scenarios for the execution of annual exercises. The Mint will submit contingency plans to key contingency personnel for review and approval prior to execution of annual exercises; and for review and signed approval for lessons learned at the conclusion of annual contingency plan tests and exercises. The target completion date is January 30, 2015.
>
> **Responsible Official:** Mint, Chief Information Security Officer

KPMG Finding 7: POA&Ms were not tracked in accordance with NIST and Treasury requirements at DO.

> **KPMG Comment:** Based on the planned corrective actions for DO, we are not making a recommendation.

KPMG Finding 8: OIG did not conduct or document a United States Government Configuration Baseline (USGCB) baseline review and document deviations.

KPMG Recommendation 28: We recommend that OIG management: Conduct a USGCB baseline review for Windows 7 and document deviations.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The OIG will conduct an USGCB baseline review for Windows 7 components and document the deviations. The target completion date is December 31, 2014.
>
> **Responsible Official:** OIG, Information Technology Director

APPENDIX I – OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives for this independent evaluation were to assess the Department of the Treasury's (Treasury's) information security program and practices for the period July 1, 2013 to June 30, 2014 as they relate to non-Internal Revenue Service (IRS) information systems. Specifically, the objectives of this evaluation were to:

- Perform the annual independent FISMA evaluation 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 our independent evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation.

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation, Presidential directives, and the DHS *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, dated December 2, 2013. We noted that the DHS FISMA reporting metrics called out the usage of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev.) 3, however, it further states that "FIPS 200 mandates the use of NIST SP 800-53, as amended." NIST released SP 800-53 Rev. 4 in April 2013, which all agencies are expected to be in compliance within one year of the publication date. 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 evaluation's objective as listed below:

PHASE A: Assessment of Treasury 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 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, as well as Treasury guidelines developed in response to FISMA. This included program controls applicable to information security governance, 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, 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[5] bureau- and office-wide information security programs according to requirements defined in FISMA and DHS *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, as well as Treasury guidelines developed in response to FISMA. This included program controls applicable to information security governance, certification and accreditation, security configuration management, incident response and reporting, security training, plan of action

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

and milestones, remote access, account and identity management, continuous monitoring, contingency planning, and contractor systems.

PHASE C: System Level (Limited)

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 114 non-IRS major applications and general support systems as of May 6, 2014.[6] 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 10 of 12 Treasury bureaus, excluding IRS and the OIG.[7]

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 the period of March 24, 2014 through July 31, 2014. During our evaluation, we met with Treasury management to discuss our preliminary conclusions.

Criteria

We focused our FISMA evaluation 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.[8] The

[6] 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 and OIG, rather than selecting a random sample of information systems that might exclude a Treasury bureau.

[7] 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 2014.

[8] Note (per *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*): 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.

following is a listing of the criteria used in the performance of the fiscal year (FY) 2014 FISMA evaluation:

NIST FIPS and/or Special Publications

- 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, *Risk Management Guide for Information Technology Systems*
- 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 800-39, *Managing Risk from Information Systems: An Organizational, Mission and Information System View*
- NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A, Rev. 1, *Guide for Assessing the Security 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. 1, *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 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- OMB Memorandum 07-18, *Ensuring New Acquisitions Include Common Security Configurations*
- OMB Memorandum 14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
- OMB Memorandum 15-01, *Fiscal Year 2014 – 2015 Guidance on Improving Federal Information Security and Privacy Management Practices*

United States Department of Homeland Security

- *DHS FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*

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) 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. In 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. As part of this year's FISMA Evaluation 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 – 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.	**Partially Implemented/Open** We noted management was able to provide listings of administrator accounts with account creation dates but was unable to provide access approval evidence for 11 of the 25 new administrators selected

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2013 Finding #1– Mint Logical account management activities were not in place or not consistently performed.	For a selected Mint system, Mint management did not formally document and maintain access request forms for 2 of 11 new user accounts. One of these two users was a system administrator who did not have any documentation of authorization. We noted the defined procedure for approving new users for the selected system lacked the creation and proper retention of new user access request forms, per policy.	We recommend that Mint management: 1 For the selected system, update the process for approving users to the system to ensure that there is appropriate creation and preservation of user access authorization to this system. The system security plan (SSP) should also be updated to reflect the new process. 2 For the selected system, reapprove all existing users under the new process to ensure their access is appropriate.	**Implemented/Closed** We noted management updated their Standard Operating Procedures (SOP) for approving and adding new users as stated in recommendation #1. Additionally, it was noted Mint reapproved all existing users under the SOP as of 11/25/2013 as stated in recommendation #2.
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.

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.	**Open** Fiscal Service has not fully implemented the Incident Handling and Response SOP. Additionally, we noted that three incidents in FY14 were not reported to TCSIRC in accordance with the US-CERT timeframes.
Prior Year FY 2013 Finding #2 – Office of Inspector General (OIG) Security incidents were not reported correctly.	OIG incorrectly reported 2 of 8 CAT 1 incidents as CAT 4 incidents. Both incidents were reported in the required 1-hour deadline for a CAT 1 incident. OIG management was categorizing incidents based on an older Treasury policy dated 2008 that did not provide examples of the types of incidents that fall into each category. They were not aware of the newer Treasury policy dated 2011 that has specific examples of the types of incidents for each category.	We recommend that OIG management ensure that OIG's CSIRC categorizes incidents based on guidelines set forth in the most recent Treasury policy and provides training to staff regarding this new Treasury Policy.	**Implemented/Closed** We noted management did ensure that OIG's categorizes incidents based on guidelines set forth in the most recent Treasury policy and provides training to staff.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2013 Finding #3 – Financial Crimes Enforcement Network (FinCEN) Did not follow NIST guidance for SSPs.	FinCEN's SSP for the selected system did not follow NIST SP 800-53, Rev. 3, guidance on required controls for HIGH categorized systems. Specifically, publicly assessable content (AC-22), non-repudiation (AU-10), incident response (IR-8), and information system partitioning (SC-32) were not addressed in the SSP. FinCEN management did not perform an adequate review of the SSP and overlooked the lack of these controls when updating the SSP.	We recommend that FinCEN management: 1 Update the system SSP to address and reference the outstanding NIST SP 800-53, Rev. 3, controls and control enhancements for a HIGH baseline. 2 Conduct thorough reviews of the system SSP annually to ensure that it includes applicable NIST SP 800-53, Rev. 3, controls.	**Implemented/Closed** We obtained and inspected the updated SSP and noted that the missing controls have been added and the SSP has been updated for the current year. However, we noted that the SSP did not address the NIST SP 800-53, Rev. 4, security controls.
Prior Year FY 2013 Finding #3 – Fiscal Service Did not follow NIST guidance for SSPs.	Fiscal Service's SSP for the selected system was last updated in November 2011 and had not been reviewed annually as required by the Fiscal Service guidelines. Fiscal Service management decided not to update a selected system SSP in FY13 as the system was scheduled for annual security assessment with completion projected in mid-December 2013 and the SSP would be updated at that time.	We recommend that Fiscal Service management Ensure that subsequent to the selected system's security assessment, the SSP should undergo annual reviews,	**Implemented/Closed** We obtained and inspected the updated SSP and noted that the SSP was reviewed within the last year. Additionally, we noted that system received an Authority to Operate (ATO) on February 15, 2014.
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.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2013 Finding #5 – OIG Evidence of successful completion of annual security awareness training was not retained for some users.	OIG management did not maintain evidence of the successful completion of security awareness training by their users. OIG management was unable to provide evidence of successful security awareness training completion for 4 of the 25 users selected for testing. OIG management reported that users verbally reported completion of the training using the Treasury Learning Management System (TLMS); however, the system did not record their successful submission. In addition, management does not require users to retain copies of their security certificates to show evidence of completion.	We recommend that OIG management implement processes or mechanisms to ensure that users complete the annual security awareness training and that the records of users' successful completion of this training is retained.	**Implemented/Closed** We noted that OIG management did implement processes or mechanisms to ensure that users complete the annual security awareness training and that the records of users' successful completion of this training is retained.

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.	**Partially Implemented/Open** 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. Therefore, we determined recommendation #1 is closed. However, we noted that some users were not disabled after 120 days of inactivity. Therefore, recommendation #2 remains open.
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** DO updated the POA&M to include all the findings and remediation's documented in the selected system's security requirements compliance matrix.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #6 – Bureau of the Public Debt (BPD) Vulnerability scanning and remediation was not performed in accordance with Treasury requirements.	For both selected BPD systems, BPD management identified that there were insufficient procedures over vulnerability remediation in place. This was a self-reported finding and documented within BPD's POA&M report on TAF. The POA&M item is scheduled to be completed on June 30, 2013.	Based upon the planned correction actions for BPD, we are not making a recommendation.	**Implemented/Closed** FMS and BPD consolidated into one organization, Fiscal Service in October 2012. We obtained and inspected the Vulnerability Management and Remediation SOP and noted management created and implemented an enterprise procedure, using automated solutions where feasible, for vulnerability remediation.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding#10 – Financial Management Service (FMS) System baselines were not documented properly.	A selected FMS system lacked sufficient system baseline documentation. Specifically, the baseline documentation did not establish operational requirements. Moreover, documentation of the following elements did not exist: mandatory configuration settings for the information system components to reflect the most restrictive mode; list of authorized and unauthorized programs; and mechanisms to verify configuration settings and respond to unauthorized changes. The selected system Configuration Management Plan did not provide a clear distinction between program change control and system configuration management processes identified in the FMS Entity-Wide IT Standards. The lack of clarity and baseline features within the selected system Configuration Management Plan was overlooked by FMS management when establishing the plan.	We recommend that FMS management: 1 Clarify the distinction between program change control and system configuration management within the FMS Entity-Wide IT Standards and the selected system Configuration Management Plan by documenting and considering correcting gaps in the current process and work flow to clearly outline work flow, tasks, and management oversight. 2 Update the selected system Configuration Management Plan to establish operational requirements and document the following elements: mandatory security relevant configuration settings, description of the controls to address unauthorized security relevant changes to the configuration of the system, and a list of authorized/unauthorized changes. 3 Document a secure baseline and mandatory configuration settings for the information system components in the selected system Configuration Management Plan to reflect the most restrictive mode in support of the security controls for the system.	**Implemented/Closed** FMS and BPD consolidated into one organization, Fiscal Service in October 2012. In 2013, we noted that management developed an Enterprise Configuration Management Plan to address Recommendations #1 and #3 in March 2013. In 2014, We obtained and inspected the system's Configuration Management Plan and noted that the plan was updated to include the missing components as well as a secure baseline to address Recommendation #2.

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.	**Open.** TIGTA has not finished completing its corrective action.
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.	**Partially Implemented/Open** FMS and BPD consolidated into one organization, Fiscal Service in October 2012. Fiscal Service has not finished completing its corrective action.

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.
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 one 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.	**Open.** TIGTA has not finished completing its corrective action.
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.	**Open.** TIGTA has not finished completing its corrective action.

APPENDIX III – DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS's FISMA 2014 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 2014 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		
Status of Continuous Monitoring Program [check one: Yes or No]	Yes	**1.1** Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems 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	**1.1.1.** Documented policies and procedures for continuous monitoring (NIST SP 800-53: CA-7).
	Yes	**1.1.2.** Documented strategy for information security continuous monitoring (ISCM) (NIST 800-37 Rev 1, Appendix G).
	No	**1.1.3.** Implemented ISCM for information technology assets. **Comments – Treasury OIG:** While Treasury has finalized their ISCM strategy, the bureaus are currently in different phases of implementing the strategy. **Comments – TIGTA**: The IRS has not yet implemented its ISCM strategy, but it 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.
	Yes	**1.1.4.** Evaluate risk assessments used to develop their ISCM strategy.
	No	**1.1.5.** Conduct and report on ISCM results in accordance with their ISCM strategy. **Comments – Treasury OIG:** While Treasury has finalized their ISCM strategy, the bureaus are currently in different phases of implementing the strategy. **Comments – TIGTA**: The IRS has not yet implemented its ISCM strategy, but it 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.
	Yes	**1.1.6.** Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53, NIST SP 800-53A).

1: Continuous Monitoring		
	Yes	**1.1.7.** Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, NIST SP 800-53A).
		1.2. Please provide any additional information on the effectiveness of the organization's Continuous Monitoring Management Program that was not noted in the questions above.

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.
	No	**2.1.2.** Defined standard baseline configurations. **Comments – Treasury OIG:** OIG did not conduct a United States Government Configuration Baseline (USGCB) baseline review for Windows 7 components and document deviations. TIGTA did not identify standard baseline configurations. (See Finding #8 and Prior Year FY 2011 Finding #12)
	No*	**2.1.3.** Assessments of compliance with baseline configurations. **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 (SCAP) format for all of its IT assets.
	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.
	No	**2.1.5.** For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings fully documented. **Comments – Treasury OIG:** OIG did not conduct a United States Government Configuration Baseline (USGCB) baseline review for Windows 7 components and document deviations. (See Finding #8)

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

2: Configuration Management		
	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.** Process for the timely and secure installation of software patches. **Comments – TIGTA**: The IRS has not implemented an adequate enterprise-wide process to ensure timely installation of software patches on all platforms.
	No*	**2.1.8.** Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53: RA-5, SI-2). **Comments – TIGTA**: Monthly software assessment vulnerability scans are not performed on all systems.
	No*	**2.1.9.** 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 – 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. Also, IRS processes to share vulnerability information with system owners and administrators are still under development.
	No*	**2.1.10.** 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 an adequate enterprise-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 – TIGTA**: The IRS intends to create and deploy a standard change management process for its Information Technology organization, supported by an integrated change management system called the Enterprise Configuration Management System.
	No*	**2.3.** Does the organization have an enterprise deviation handling process and is it integrated with the automated capability **Comments – TIGTA**: The IRS has not yet implemented its ISCM strategy in order to accomplish an enterprise deviation handling process that is integrated with an automated capability.

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

2: Configuration Management		
	No*	**2.3.1.** Is there a process for mitigating the risk introduced by those deviations? **Comments – TIGTA**: The IRS has not yet implemented its ISCM strategy in order to accomplish an enterprise deviation handling process that is integrated with an 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 identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?
	No	**3.1.1.** Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1) **Comments – Treasury OIG:** TIGTA did not formally document account management activities for a selected system. (See Prior Year FY 2011 Finding #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**: Users are not uniquely identified and authenticated on all IRS systems. Also, the IRS has not fully implemented unique user identification and authentication that complies with HSPD-12. In addition, nine of the 10 systems we reviewed did not have the NIST SP 800-53 AC-2 security control fully in place.
	No*	**3.1.3.** Identifies when special access requirements (e.g., multi-factor authentication) are necessary. **Comments – TIGTA**: The IRS has not fully implemented multifactor authentication in compliance with HSPD-12.
	No*	**3.1.4.** If multi-factor authentication is in use, it is linked to the organization's PIV program where appropriate (NIST SP 800-53, IA-2). **Comments – TIGTA**: The IRS has not fully deployed multifactor authentication via the use of an HSPD-12 PIV card for all users for network and local access to nonprivileged or privileged accounts as required by HSPD-12.

* 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.** 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 – TIGTA**: Considerable challenges still exist for the IRS in achieving full implementation of PIV for logical access due to its legacy environment and other factors.
	No*	**3.1.6.** Organization has adequately 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**: During the FY14 FISMA evaluation period, the IRS had not planned to implement PIV for physical access at all its facilities. However, the IRS has informed us that it has prioritized the remaining locations and developed a long-range plan, dependent on the availability of funding.
	No	**3.1.7.** Ensures that the users are granted access based on needs and separation-of-duties principles. **Comments – Treasury OIG:** OCC had an Information System Owner inappropriately approve and modify their own elevated role requests. DO 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 2013 and FY 2014, the GAO identified users that had been granted more access than needed and instances where the separation-of-duties principle was not enforced.
	No*	**3.1.8.** Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts). **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.
	Yes	**3.1.9.** Identifies all user and non-user accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users).

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

3: Identity and Access Management		
	No	**3.1.10.** Ensures that accounts are terminated or deactivated once access is no longer required. **Comments – Treasury OIG:** Fiscal Service did not deactivate accounts after 90 days of inactivity. (See Prior Year FY 2011 Finding #1) **Comments – TIGTA**: The IRS identified systems that do not have controls in place to ensure that accounts are terminated or deactivated once access is no longer needed.
	No*	**3.1.11.** Identifies and controls use of shared accounts. **Comments – TIGTA**: During FY 2013 and FY 2014, the GAO identified improper use of shared accounts; for example, use of a generic administrator accounts and passwords.
		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 and Fiscal Service were unable to provide documentation evidencing administrators account creation dates. FinCEN was unable to provide evidence for one of their user's access authorization. Fiscal Service had an ISSO approving access prior to their official appointment. Fiscal Service and TIGTA were unable to provide documentation evidencing the users' last log-on date or time. (See Finding #1, Prior Year FY 2013 Finding #1 and Prior Year FY 2012 Finding #1)

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).
	No	**4.1.2.** Comprehensive analysis, validation, and documentation of incidents. **Comments – Treasury OIG:** DO incorrectly categorized reported incident. (See Finding #2)

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

4: Incident Response and Reporting		
	No	**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). **Comments – Treasury OIG:** BEP, DO, Fiscal Service and OIG did not report incidents within required time frames. (See Finding #2 and Prior Year FY 2013 Finding #2) **Comments – TIGTA**: The IRS did not always report incidents involving Personally Identifiable Information to the US-CERT within established time frames.
	Yes	**4.1.4.** When applicable, reports to law enforcement 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, and OMB M-07-16, M-06-19).
	Yes	**4.1.6.** Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.
	Yes	**4.1.7.** Is capable of correlating incidents.
	Yes	**4.1.8.** 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).
		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.** Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.
	No	**5.1.2.** 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. **Comments – Treasury OIG:** TIGTA did not update risk management program with NIST SP 800-37, Rev.1 guidance. (See Prior Year FY 2011 Finding #10)
	No	**5.1.3.** 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. **Comments – Treasury OIG:** TIGTA did not update risk management program with NIST SP 800-37, Rev.1 guidance. (See Prior Year FY 2011 Finding #10)
	Yes	**5.1.4.** 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.

5: Risk Management		
	Yes	**5.1.5.** Has an up-to-date system inventory.
	Yes	**5.1.6.** Categorizes information systems in accordance with government policies.
	Yes	**5.1.7.** Selects an appropriately tailored set of baseline security controls.
	No	**5.1.8.** Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation. **Comments – Treasury OIG:** DO, Fiscal Service, and Mint did not adequately document the implementation of NIST SP 800-53, Rev. 4, security controls as required by NIST and Treasury guidance. (See Finding #3)
	No	**5.1.9.** 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:** DO, Fiscal Service, and Mint did not assess the NIST SP 800-53, Rev. 4, security controls as required by NIST and Treasury guidance. (See Finding #3)
	Yes	**5.1.10.** 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.
	No	**5.1.11.** Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. **Comments – Treasury OIG:** Mint did not review the SSP annually. (See Finding #3)
	Yes	**5.1.12.** Information-system-specific risks (tactical), mission/business-specific risks and organizational-level (strategic) risks are communicated to appropriate levels of the organization.
	Yes	**5.1.13.** Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).
	Yes	**5.1.14.** 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	**5.1.15.** Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies (NIST SP 800-18, SP 800-37).
	Yes	**5.1.16.** Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems.

5: Risk Management		
		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:** BEP and FinCEN had not updated or reviewed their bureau policies to address NIST and Treasury requirements. (See Finding #5) **Comments – TIGTA**: TIGTA found deficiencies with the IRS's risk-based decisions process that were not in alignment with policy. Specifically, we found that not all risk-based decisions are adequately documented and tracked.

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.
	No	**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. **Comments – Treasury OIG:** CDFI, DO and Mint were unable to provide evidence of successful completion of security awareness training. (See Finding #4)
	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 has not yet fully implemented a process for identifying and tracking contractors who are required to complete specialized training, but it stated that it continues to make progress and is working to incorporate a clause into contracts that requires contractors to complete and record such training.

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

6: Security 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: 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.
	No	**7.1.2.** Tracks, prioritizes, and remediates weaknesses. **Comments – Treasury OIG:** DO did not track the POA&Ms for one of the systems selected. (See Finding #7)
	Yes	**7.1.3.** Ensures remediation plans are effective for correcting weaknesses.
	Yes	**7.1.4.** Establishes and adheres to milestone remediation dates.
	Yes	**7.1.5.** Ensures resources and ownership are provided for correcting weaknesses.
	No	**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). **Comments – Treasury OIG:** DO did not create POA&Ms for security weaknesses discovered during security assessment and continuous monitoring. (See Finding #7)
	Yes	**7.1.7.** Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control 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, Rev. 3, Control CA-5; and 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?

8: Remote Access Management		
	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 has 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.** If applicable, multifactor authentication is required for remote access (NIST 800-46, Section 2.2, Section 3.3). **Comments – TIGTA**: The IRS has not fully implemented multifactor authentication that complies with HSPD-12.
	No†	**8.1.6.** Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. **Comments – TIGTA**: The IRS has not fully implemented multifactor authentication that complies with HSPD-12.
	Yes	**8.1.7.** Defines and implements encryption requirements for information transmitted across public networks.
	Yes	**8.1.8.** 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	**8.1.9.** Lost or stolen devices are disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).
	Yes	**8.1.10.** Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4).
	Yes	**8.1.11.** 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?

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

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 (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (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 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 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 Finding #6 and Prior Year FY 2013 Finding #4)
	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 Finding #6 and Prior Year FY 2013 Finding #4)

9: Contingency Planning		
	Yes	**9.1.9.** Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).
	Yes	**9.1.10.** Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).
	Yes	**9.1.11.** Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).
	Yes	**9.1.12.** 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 [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 organization systems and services residing in public 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 organization systems and services residing in public cloud. **Comments – TIGTA**: In FY 2014, the IRS maintained two contractor-managed systems in the Treasury FISMA Information Management System (formerly, the Trusted Agent FISMA), which is the U.S. Department of the Treasury's system for reporting FISMA data. The IRS Contractor Security Assessments Office maintains a separate listing of contractor sites that the IRS does not consider "FISMA-reportable," but that require annual security reviews because each handles or processes IRS information. The IRS Contractor Security Assessments Office is responsible for evaluating security controls at these contractor sites.
	Yes	**10.1.4.** The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5).
	Yes	**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.
	Yes	**10.1.6.** The inventory of contractor systems is updated at least annually.
	Yes	**10.1.7.** Systems that are owned or operated by contractors or entities, including organization systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

10: Contractor Systems		
		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.

11: Security Capital Planning		
Status of Security Capital Planning [check one: Yes or No]	Yes	**11.1** Has the organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**11. 1.1.** Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process.
	Yes	**11.1.2.** Includes information security requirements as part of the capital planning and investment process.
	Yes	**11.1.3.** Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53: SA-2).
	Yes	**11.1.4.** Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3).
	Yes	**11.1.5.** Ensures that information security resources are available for expenditure as planned.
		11.2. Please provide any additional information on the effectiveness of the organization's Security Capital Planning Program that was not noted in the questions above.

APPENDIX IV – APPROACH TO SELECTION OF SUBSET OF SYSTEMS

In fiscal year (FY) 2014, we continued to use a risk-based approach was employed to determine the subset of United States Department of the Treasury (Treasury) information systems for the FISMA Evaluation. 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 Trusted Agent FISMA system (TAF) as the population for this subset.

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, 2014.
- 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 should not exceed the percentage of Treasury's population of financial systems. We defined financial systems as those information systems that have been designated as "Financial" or "Mixed Financial" systems in the Treasury's TAF System.

Based on our analysis of Treasury's inventory of information systems as of May 6, 2014, we noted a total of 185 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	127	2	43	36	46
General Support Systems	58	0	26	2	30
Total	185	2	69	38	76

From the analysis above, it was determined that IRS systems make up 38% of the total population of Major Applications and General Support systems and Non-IRS systems make up 62%. 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 72% of the population of the Non-IRS population and General Support Systems account for 28%. We further determined that systems designated as "Financial" and "Mixed Financial" in TAF account for 33% of all Non-IRS Major Applications and General Support Systems. Lastly, we determined that 32% of the Non-IRS Major Applications and General Support Systems are assigned a FIPS 199 System Impact Level of "High," while 68% are assigned a FIPS 199 System Impact Level of "Moderate."

Total Selected	15
Total Major Applications	11
Total General Support Systems	4
Total Systems with a FIPS 199 System Impact Level of "High"	5
Total Systems with a FIPS 199 System Impact Level of "Moderate"	10
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 114 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	49	43%	5
CDFI Fund	3	3%	1 (See Note 2)
DO	28	24%	3
FinCEN	6	5%	1
Mint	9	8%	1
OCC	7	6%	1
OIG	1	1%	0 (See Note 1)
TIGTA	2	2%	1 (See Note 2)
TTB	3	3%	1 (See Note 2)
Total	114	100%	15

(**Note 1:** 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 2014.)
(**Note 2:** 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.)

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
COOP	Continuity of Operations Plan
COR	Contracting Officer Representative
CPIC	Capital Planning and Investment Control
CSIRC	Computer Security Incident Response Center
CSS	Cyber Security Sub-Council
DHS	Department of Homeland Security
DO	Departmental Offices
DRP	Disaster Recovery Plan
FCD	Federal Continuity Directive
FinCEN	Financial Crimes Enforcement Network
FIPS	Federal Information Processing Standards
Fiscal Service	The Bureau of the Fiscal Service
FISMA	Federal Information Security Management 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
ISSO	Information Systems Security Officer

Acronym	Definition
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
TAF	Trusted Agent FISMA
TARP	Troubled Asset Relief Program
TCSIRC	Treasury Computer Security Incident Response Capability
TD P	Treasury Directive Publication
TIGTA	Treasury Inspector General for Tax Administration
TLMS	Treasury Learning Management System
Treasury	The 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 Stated Government Configuration Baseline

ATTACHMENT 2

Treasury Inspector General for Tax Administration –
Federal Information Security Management Act Report for Fiscal Year 2014
Reference Number: 2014-20-090
September 23, 2014

THIS PAGE INTENTIONALLY LEFT BLANK

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2014

September 23, 2014

Reference Number: 2014-20-090

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 MANAGEMENT ACT REPORT FOR FISCAL YEAR 2014

Highlights

Final Report Issued on September 23, 2014

Highlights of Reference Number: 2014-20-090 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 (FISMA) was 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 the confidentiality of this sensitive information against unauthorized access or loss.

WHY TIGTA DID THE AUDIT

As part of the FISMA legislation, the Offices of Inspectors General are required to perform an annual independent evaluation of each Federal agency's information security programs and practices. This report presents the results of TIGTA's FISMA evaluation of the IRS for Fiscal Year 2014.

WHAT TIGTA FOUND

Based on this year's FISMA evaluation, five of the 11 security program areas met the performance metrics specified by the Department of Homeland Security's *Fiscal Year 2014 Inspector General Federal Information Security Management Act Reporting Metrics:*

- Risk Management.
- Plan of Action and Milestones.
- Contingency Planning.
- Contractor Systems.
- Security Capital Planning.

Four security program areas were not fully effective due to one or more program attributes that were not met:

- Continuous Monitoring Management.
- Incident Response and Reporting.
- Security Training.
- Remote Access Management.

Two security program areas did not meet the level of performance specified due to the majority of the attributes not being met:

- Configuration Management.
- Identity and Access Management.

To meet the expected level of performance for Configuration Management, the IRS needs to improve enterprise-wide processes for assessing configuration settings and vulnerabilities through automated scanning, timely remediating scan result deviations, timely installing software patches, and controlling changes to hardware and software configurations.

To meet the expected level of performance for Identity and Access Management, the IRS needs to fully implement unique user identification and authentication that complies with Homeland Security Presidential Directive-12, ensure that users are only granted access based on needs, ensure that user accounts are terminated when no longer required, and control the improper use of shared accounts.

WHAT TIGTA RECOMMENDED

TIGTA does not include recommendations as part of its annual FISMA evaluation and reports only on the level of performance achieved by the IRS using the guidelines 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 23, 2014

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 Management Act Report for Fiscal Year 2014 (Audit # 201420001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Management Act[1] evaluation of the Internal Revenue Service for Fiscal Year 2014. 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.

The 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 IRS managers affected by the report results.

If you have any questions, please contact me or Kent Sagara, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

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

Table of Contents

Abbreviations

CIO	Chief Information Officer
DHS	Department of Homeland Security
FCD1	Federal Continuity Directive 1
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
HSPD-12	Homeland Security Presidential Directive-12
IP	Internet Protocol
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SCAP	Security Content Automation Protocol
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 (FISMA) of 2002[1] was enacted to strengthen the security of information and systems within Federal agencies. The 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 FISMA requires the Office of Management and Budget (OMB) to develop and oversee the implementation of policies, principles, standards, and guidelines on information security that are commensurate with the risk and magnitude of the possible harm to Federal systems or information. To ensure uniformity in this process, the FISMA requires the National Institute of Standards and Technology (NIST) to prescribe standards and guidelines pertaining to Federal information systems. The FISMA also charges the OMB with producing an annual report to keep Congress apprised of Federal progress in increasing information security.

Agency heads are responsible for complying with the requirements of FISMA and related OMB policies and NIST procedures, standards, and guidelines. In addition, the FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to the OMB. The FISMA states that the independent evaluation is to be performed by the agency Inspector General or an independent external auditor as determined by the Inspector General.

In July 2010, OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, expanded the role of the DHS in regard to the operational aspects of Federal agency cybersecurity and information systems that fall within FISMA requirements. The DHS prepares the security metrics to assist the Federal agencies and the Inspectors General in evaluating agency progress in achieving compliance with Federal security standards.

FISMA oversight of the Department of the Treasury is performed by two distinct Inspector General offices: the Treasury Inspector General for Tax Administration (TIGTA) and the Treasury Office of the Inspector General (OIG). The TIGTA is responsible for oversight of the Internal Revenue Service (IRS), while the Treasury OIG is responsible for all other Treasury bureaus. The Treasury OIG has contracted with KPMG LLP to perform the FISMA evaluation of the non-IRS bureaus. The 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.

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

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.

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 period May through August 2014. 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 Internal Revenue Service's Information Security Program Generally Complies With the Federal Information Security Management Act, but Improvements Are Needed in Configuration Management and Identity and Access Management

To assist the Inspectors General in evaluating Federal agencies' compliance with the FISMA, the DHS issued the *Fiscal Year (FY) 2014 Inspector General Federal Information Security Management Act Reporting Metrics* on December 2, 2013, which specified 11 information security program areas and listed specific attributes within each area for evaluation. The 11 information security program areas are continuous monitoring management, configuration management, identity and access management, incident and response reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, contractor systems, and security capital planning.

Overall, the IRS has established an information security program and related practices that cover the 11 FISMA program areas. However, based on our FY 2014 FISMA evaluation, two of the program areas, Configuration Management and Identity and Access Management, did not meet applicable FISMA requirements due to the majority of the program attributes specified by the DHS guidelines not being met. We also identified improvements needed in five other FISMA program areas.

Based on our FY 2014 FISMA evaluation, five of the 11 security program areas met the performance metrics specified in the DHS guidelines:

- Risk Management.[2]
- Plan of Action and Milestones.
- Contingency Planning.
- Contractor Systems.
- Security Capital Planning.

[2] Although the IRS met the performance metrics specified by the DHS for Risk Management, TIGTA found deficiencies with the IRS's risk-based decisions process that were not in alignment with policy. Specifically, we found that not all risk-based decisions are adequately documented and tracked.

Four security program areas were not fully effective due to one or more DHS guideline program attributes that were not met:

- Continuous Monitoring Management.

  The IRS has not yet implemented its Information Security Continuous Monitoring (ISCM) strategy, but stated that it is fully participating in the DHS's Continuous Diagnostics and Mitigation Program to comply with the OMB M-14-03[3] mandate to implement ISCM and is in the process of determining its final toolset to meet the program requirements.

- Incident Response and Reporting.

  The IRS did not always report incidents involving Personally Identifiable Information to the U.S. Computer Emergency Response Team (US-CERT) within established time frames.

- Security Training.

  The IRS has not yet fully implemented a process for identifying and tracking contractors who are required to complete specialized training, but stated that it continues to make progress and is working to incorporate a clause into contracts that requires contractors to complete and record such training.

- Remote Access Management.

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

Two security program areas, Configuration Management and Identity and Access Management, did not meet the level of performance specified by the DHS guidelines due to the majority of the specified attributes not being met:

- Configuration Management.

  To meet the expected level of performance for Configuration Management, the IRS needs to improve enterprise-wide processes for assessing configuration settings and vulnerabilities through automated scanning, timely remediating scan result deviations, timely installing software patches, and controlling changes to hardware and software configurations.

[3] OMB, OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems* (Nov. 2013).

- Identity and Access Management.

  To meet the expected level of performance for Identity and Access Management, the IRS needs to fully implement unique user identification and authentication that complies with HSPD-12, ensure that users are only granted access based on needs, ensure that user accounts are terminated when no longer required, and control the improper use of shared accounts.

Until the IRS takes steps to improve its security program deficiencies and fully implements all 11 security program areas required by the FISMA, taxpayer data will remain vulnerable to inappropriate use, modification, or disclosure, possibly without being detected.

Figure 1 presents TIGTA's detailed results for the 11 security program areas in response to the DHS's *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*.[4] TIGTA's results will be consolidated with the Treasury OIG's results of non-IRS bureaus and reported to the OMB.

Figure 1: TIGTA's Responses to the DHS's FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics

1: Continuous Monitoring Management

Status of Continuous Monitoring Management Program [check one: Yes or No]	Yes	**1.1.** Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems 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	**1.1.1.** Documented policies and procedures for continuous monitoring. (NIST SP 800-53: CA-7)
	Yes	**1.1.2.** Documented strategy for information security continuous monitoring. (ISCM)
	No	**1.1.3.** Implemented ISCM for information technology assets. **TIGTA Comments:** The IRS has not yet implemented its ISCM strategy, but it 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.
	Yes	**1.1.4.** Evaluate risk assessments used to develop their ISCM strategy.

[4] 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.

	No	**1.1.5.** Conduct and report on ISCM results in accordance with their ISCM strategy. **TIGTA Comments:** The IRS has not yet implemented its ISCM strategy, but it 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.
	Yes	**1.1.6.** Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans. (NIST SP 800-53, NIST SP800-53A)
	Yes	**1.1.7.** Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans. (NIST SP 800-53, 800-53A)
		1.2. Please provide any additional information on the effectiveness of the organization's Continuous Monitoring Management Program that was not noted in the questions above.

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.
	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 (SCAP) format for all of its IT assets.
	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.** Process for the timely and secure installation of software patches. **TIGTA Comments:** The IRS has not implemented an adequate enterprise-wide process to ensure timely installation of software patches on all platforms.
	No	**2.1.8.** Software assessing (scanning) capabilities are fully implemented. (NIST SP 800-53: RA-5, SI-2) **TIGTA Comments:** Monthly software assessment vulnerability scans are not performed on all systems.
	No	**2.1.9.** 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. Also, IRS processes to share vulnerability information with system owners and administrators are still under development.
	No	**2.1.10.** Patch management process is fully developed, as specified in organization policy or standards. (NIST SP 800-53: CM-3, SI-2) **TIGTA Comments**: The IRS has not implemented an adequate enterprise-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. **TIGTA Comments:** The IRS intends to create and deploy a standard change management process for its Information Technology organization, supported by an integrated change management system called the Enterprise Configuration Management System.
	No	**2.3.** Does the organization have an enterprise deviation handling process and is it integrated with the automated capability? **TIGTA Comments:** The IRS has not yet implemented its ISCM strategy in order to accomplish an enterprise deviation handling process that is integrated with an automated capability.

	No	**2.3.1.** Is there a process for mitigating the risk introduced by those deviations? **TIGTA Comments:** The IRS has not yet implemented its ISCM strategy in order to accomplish an enterprise deviation handling process that is integrated with an 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. (NIST SP 800-53: AC-2) **TIGTA Comments:** Users are not uniquely identified and authenticated on all IRS systems. Also, the IRS has not fully implemented unique user identification and authentication that complies with HSDP-12. In addition, nine of the 10 systems we reviewed did not have the NIST SP 800-53 AC-2 security control fully in place.
	No	**3.1.3.** Identifies when special access requirements (*e.g.*, multifactor authentication) are necessary. **TIGTA Comments:** The IRS has not fully implemented multifactor authentication in compliance with HSPD-12.
	No	**3.1.4.** If multifactor authentication is in use, it is linked to the organization's PIV program where appropriate. (NIST SP 800-53: IA-2) **TIGTA Comments:** The IRS has not fully deployed multifactor authentication via the use of an HSPD-12 PIV card for all users for network and local access to nonprivileged or privileged accounts as required by HSPD-12.
	No	**3.1.5.** 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) **TIGTA Comments:** Considerable challenges still exist for the IRS in achieving full implementation of PIV for logical access due to its legacy environment and other factors.

	No	**3.1.6.** Organization has adequately 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) **TIGTA Comments:** During the FY14 FISMA evaluation period, the IRS had not planned to implement PIV for physical access at all its facilities. However, the IRS has informed us that it has prioritized the remaining locations and developed a long-range plan, dependent on the availability of funding.
	No	**3.1.7.** Ensures that the users are granted access based on needs and separation-of-duties principles. **TIGTA Comments:** During FY 2013 and FY 2014, the GAO identified users that had been granted more access than needed and instances where the separation-of-duties principle was not enforced.
	No	**3.1.8.** Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts.) **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.
	Yes	**3.1.9.** Identifies all user and nonuser accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.)
	No	**3.1.10.** Ensures that accounts are terminated or deactivated once access is no longer required. **TIGTA Comments:** The IRS identified systems that do not have controls in place to ensure that accounts are terminated or deactivated once access is no longer needed.
	No	**3.1.11.** Identifies and controls use of shared accounts. **TIGTA Comments:** During FY 2013 and FY 2014, the GAO identified improper use of shared accounts; for example, use of a 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.

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.
	No	**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) **TIGTA Comments:** The IRS did not always report incidents involving Personally Identifiable Information to the US-CERT within established time frames.
	Yes	**4.1.4.** When applicable, reports to law enforcement 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 tracking and managing risks in a virtual/cloud environment, if applicable.
	Yes	**4.1.7.** Is capable of correlating incidents.
	Yes	**4.1.8.** 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.** Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.

	Yes	**5.1.2.** 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	**5.1.3.** 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	**5.1.4.** 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	**5.1.5.** Has an up-to-date system inventory.
	Yes	**5.1.6.** Categorizes information systems in accordance with Government policies.
	Yes	**5.1.7.** Selects an appropriately tailored set of baseline security controls.
	Yes	**5.1.8.** Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.
	Yes	**5.1.9.** 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	**5.1.10.** 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	**5.1.11.** Ensures that information security controls are monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.
	Yes	**5.1.12.** Information system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.
	Yes	**5.1.13.** Senior officials are briefed on threat activity on a regular basis by appropriate personnel (*e.g.*, Chief Information Security Officer).
	Yes	**5.1.14.** 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	**5.1.15.** Security authorization package contains system security plan, security assessment report, and POA&M in accordance with Government policies. (NIST SP 800-18, 800-37)
	Yes	**5.1.16.** Security authorization package contains accreditation boundaries, defined in accordance with Government policies, for organization information 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. **TIGTA Comments:** TIGTA found deficiencies with the IRS's risk-based decisions process that were not in alignment with policy. Specifically, we found that not all risk-based decisions are adequately documented and tracked.

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 has not yet fully implemented a process for identifying and tracking contractors who are required to complete specialized training, but it stated that it continues to make progress and is working to incorporate a clause into contracts that requires contractors to complete and record such 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 IT security weaknesses discovered during security control assessments and that require remediation.
	Yes	**7.1.2.** Tracks, prioritizes, and remediates weaknesses.
	Yes	**7.1.3.** Ensures that remediation plans are effective for correcting weaknesses.
	Yes	**7.1.4.** Establishes and adheres to milestone remediation dates.
	Yes	**7.1.5.** Ensures that 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. (NIST SP 800-53: PM-3; OMB M-04-25)
	Yes	**7.1.8.** Program officials report progress on remediation to the 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; 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 has 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.** If applicable, multifactor authentication is required for remote access. (NIST SP 800-46, Section 2.2, Section 3.3) **TIGTA Comments:** The IRS has not fully implemented multifactor authentication that complies with HSPD-12.
	No	**8.1.6.** Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. **TIGTA Comments:** The IRS has not fully implemented multifactor authentication that complies with HSPD-12.
	Yes	**8.1.7.** Defines and implements encryption requirements for information transmitted across public networks.
	Yes	**8.1.8.** Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity, after which reauthentication is required.
	Yes	**8.1.9.** Lost or stolen devices are disabled and appropriately reported. (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines)
	Yes	**8.1.10.** Remote access rules of behavior are adequate in accordance with Government policies. (NIST SP 800-53: PL-4)
	Yes	**8.1.11.** 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 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 IT 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. (FDC1, NIST SP 800-34)
	Yes	**9.1.9.** Systems that have alternate processing sites. (FCD1, NIST SP 800-34, NIST SP 800-53)
	Yes	**9.1.10.** Alternate processing sites are not subject to the same risks as primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53)
	Yes	**9.1.11.** Backups of information that are performed in a timely manner. (FCD1, NIST SP 800-34, NIST SP 800-53)
	Yes	**9.1.12.** 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 organization systems and services residing in a public 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 organization systems and services residing in a public cloud. **TIGTA Comments:** In FY 2014, the IRS maintained two contractor-managed systems in the Treasury FISMA Information Management System (formerly, the Trusted Agent FISMA), which is the U.S. Department of the Treasury's system for reporting FISMA data. The IRS Contractor Security Assessments Office maintains a separate listing of contractor sites that the IRS does not consider "FISMA-reportable," but that require annual security reviews because each handles or processes IRS information. The IRS Contractor Security Assessments Office is responsible for evaluating security controls at these contractor sites.
	Yes	**10.1.4.** The inventory identifies interfaces between these systems and organization-operated systems. (NIST SP 800-53: PM-5)
	Yes	**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.
	Yes	**10.1.6.** The inventory of contractor systems is updated at least annually.
	Yes	**10.1.7.** Systems that are owned or operated by contractors or entities, including organization systems and services residing in a public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.
		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.

11: Security Capital Planning

Status of Security Capital Planning Program [check one: Yes or No]	Yes	**11.1.** Has the organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**11.1.1.** Documented policies and procedures to address information security in the capital planning and investment control process.
	Yes	**11.1.2.** Includes information security requirements as part of the capital planning and investment process.
	Yes	**11.1.3.** Establishes a discrete line item for information security in organizational programming and documentation. (NIST SP 800-53: SA-2)
	Yes	**11.1.4.** Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required. (NIST SP 800-53: PM-3)
	Yes	**11.1.5.** Ensures that information security resources are available for expenditure as planned.
		11.2. Please provide any additional information on the effectiveness of the organization's Security Capital Planning Program that was not noted in the questions above.

Source: Results of TIGTA's FY 2014 FISMA evaluation of the IRS.

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 for the period July 1, 2013, to June 30, 2014. To accomplish our objective, we responded to the questions provided in the DHS *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, issued on December 2, 2013. The questions related to the following 11 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.
11. Security Capital Planning.

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[1] 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 2014 FISMA evaluation period, as listed in Appendix IV, as well as results from ongoing audits for which draft reports were issued to the IRS by August 8, 2014.

Based on our evaluative work, we indicated with a yes or no whether the IRS had achieved a satisfactory level of performance for each security program area as well as each specific attribute listed in the DHS *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*. The Treasury OIG will combine our results for the IRS with its results for the non-IRS bureaus and submit the combined yes or no responses to the OMB.

[1] Formerly the Trusted Agent FISMA system.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Midori Ohno, Lead Auditor
Cindy Harris, Senior Auditor
Bret Hunter, Senior Auditor
Mary Jankowski, Senior Auditor
Louis Lee, Senior Auditor
Esther Wilson, Senior 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
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
- Business Planning and Risk Management OS:CTO:SP:RM
- Cybersecurity OS:CTO:C

Appendix IV

Treasury Inspector General for Tax Administration Information Technology Security-Related Reports Issued During the Fiscal Year 2014 Evaluation Period

1. TIGTA, Ref. No. 2014-20-021, *Used Information Technology Assets Are Being Properly Donated; However, Disposition Procedures Need to Be Improved* (April 2014).
2. TIGTA, Ref. No. 2014-20-016, *Planning Is Underway for the Enterprise-Wide Transition to Internet Protocol Version 6, but Further Actions Are Needed* (Feb. 2014).
3. TIGTA, Ref. No. 2013-20-063, *Improvements Are Needed to Ensure Successful Development and System Integration for the Return Review Program* (Jul. 2013).
4. TIGTA, Ref. No. 2013-20-089, *Weaknesses in Asset Management Controls Leave Information Technology Assets Vulnerable to Loss* (Sept. 2013).
5. TIGTA, Ref. No. 2013-20-106, *Automated Monitoring Is Needed for the Virtual Infrastructure to Ensure Secure Configurations* (Sept. 2013).
6. TIGTA, Ref. No. 2013-20-107, *Full Compliance With Trusted Internet Connection Requirements Is Progressing; However, Improvements Would Strengthen Security* (Sept. 2013).
7. TIGTA, Ref. No. 2013-20-108, *Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot* (Sept. 2013).
8. TIGTA, Ref. No. 2013-20-117, *Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data* (Sept. 2013).
9. TIGTA, Ref. No. 2013-20-118, *Foreign Account Tax Compliance Act: Improvements Are Needed to Strengthen Systems Development Controls for the Foreign Financial Institution Registration System* (Sept. 2013).
10. TIGTA, Ref. No. 2013-20-125, *Customer Account Data Engine 2 Database Deployment Is Experiencing Delays and Increased Costs* (Sept. 2013)
11. TIGTA, Ref. No. 2013-20-127, *While Efforts Are Ongoing to Deploy a Secure Mechanism to Verify Taxpayer Identities, the Public Still Cannot Access Their Tax Account Information Via the Internet* (Sept. 2013).