Evaluation Report

OIG-CA-14-006

INFORMATION TECHNOLOGY: The Department of the Treasury Federal Information Security Management Act Fiscal Year 2013 Evaluation

November 25, 2013

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 25, 2013

MEMORANDUM FOR NANI COLORETTI
ASSISTANT SECRETARY FOR MANAGEMENT

ROBYN EAST
DEPUTY ASSISTANT SECRETARY FOR INFORMATION SYSTEMS AND CHIEF INFORMATION OFFICER

FROM: Marla A. Freedman /s/
Assistant Inspector General for Audit

SUBJECT: Evaluation Report – *The Department of the Treasury's Federal Information Security Management Act Fiscal Year 2013 Evaluation*

We are pleased to transmit the following reports:

- *The Department of the Treasury Federal Information Security Management Act Fiscal Year 2013 Evaluation* (Attachment 1), and

- *Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2013* (Attachment 2).

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies, including the Department of the Treasury (Treasury), to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluations 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 independent evaluation be performed by the agency Inspector General (IG) or an independent external auditor as determined by the IG. 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 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, KPMG concluded that Treasury has established an information security program and related practices for its non-IRS bureaus' unclassified systems. The information security program covers the 11 FISMA program areas: 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. While Treasury did establish an information security program and practices, KPMG identified needed improvements in 5 of 11 FISMA program areas and made 11 recommendations to the responsible officials to address the findings.

TIGTA reported that the IRS's information security program generally complies with FISMA, but improvements are needed. Specifically, TIGTA determined that 9 of the 11 security program areas were generally compliant with the FISMA requirements. However, TIGTA reported that 2 IRS security program areas were not compliant with FISMA requirements.

Based on the results reported by KPMG and TIGTA, we determined that while Treasury's information security program and practices for its unclassified systems are in place and are generally consistent with FISMA, they could be more effective. See appendix III of the attached KPMG report for *The Department of the Treasury's Consolidated Response to DHS's FISMA 2013 Questions for Inspectors General*.

In connection with the contract with KPMG, we reviewed its report and related documentation and inquired of its representatives. Our review was differentiated from an evaluation performed in accordance with Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation.

If you have any questions or require further information, you may contact me at (202) 927-5400, or Tram J. Dang, Director, Information Technology Audit, at (202) 927-5171.

Attachments

cc: Edward A. Roback
Associate Chief Information Officer
Cyber Security

ATTACHMENT 1

The Department of the Treasury
Federal Information Security Management Act
Fiscal Year 2013 Evaluation,
November 18, 2013

THIS PAGE INTENTIONALLY LEFT BLANK

The Department of the Treasury
Federal Information Security Management Act
Fiscal Year 2013 Evaluation

November 18, 2013

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

The Department of the Treasury
Federal Information Security Management Act Fiscal Year 2013 Evaluation

Table of Contents

FISMA Evaluation Report

Appendices

KPMG LLP
1676 International Drive
McLean, VA 22102

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

Re: The Department of the Treasury's Federal Information Security Management Act Fiscal Year 2013 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 2013 questionnaire to collect these responses. Appendix III, *The Department of the Treasury's Consolidated Response to DHS's FISMA 2013 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 objective for this independent evaluation was to assess the effectiveness of the Treasury's information security program and practices for the period July 1, 2012 to June 30, 2013 for its unclassified systems, including the 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-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, *The Department of the Treasury's Consolidated Response to DHS's FISMA 2013 Questions for Inspectors General*. Additional details regarding the scope of our independent evaluation are included in Appendix I, *Objective, Scope & Methodology*.

Consistent with applicable FISMA requirements, OMB policy and guidelines, and the National Institute of Standards and Technology (NIST) standards and guidelines, the Treasury's information security program and practices for its non-IRS bureaus' unclassified systems have established and are maintaining security programs for the 11 FISMA program areas.[1] However, while the security program has been implemented across the Treasury for its non-IRS bureaus, we identified 5 of 11 FISMA program areas that needed improvements.

1. Logical account management activities were not in place or not consistently performed by the Departmental Offices (DO), United States Mint (Mint), and TIGTA.
2. Security incidents were not reported correctly at the Bureau of the Fiscal Service (Fiscal Service) and OIG.
3. Financial Crimes Enforcement Network (FinCEN) and Fiscal Service did not follow NIST guidance for System Security Plans (SSPs).
4. Contingency planning and testing controls were not fully implemented or operating as designed at TIGTA.
5. Evidence of successful completion of annual security awareness training was not retained for some users at OIG.

We have made 11 recommendations related to these control deficiencies that, if effectively addressed by management, should strengthen the respective bureaus, offices, and the Treasury's information security program. In a written response, the Treasury Chief Information Officer (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 and will be evaluated as part of the FY 2014 independent evaluation. 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.

Appendix I describes the FISMA evaluation's objective, scope, and methodology. Appendix II, *Status of Prior-Year Findings*, summarizes the Treasury's progress in addressing prior-year recommendations. Appendix III provides *The Department of the Treasury's Consolidated Response to DHS's FISMA 2013 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

November 18, 2013

[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.

BACKGROUND

Federal Information Security Management Act (FISMA)

Title III of the E-Government Act of 2002 (the Act), commonly referred to as FISMA, focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The Act assigns specific responsibilities to agency heads and Inspectors Generals (IGs) in complying with requirements of FISMA. The Act is supported by the Office of Management and Budget (OMB), 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 the Treasury 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 the Treasury 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 2013 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 2013 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 the Treasury's bureaus. The OCIO Cyber Security Program's mission focuses on the following areas:

1. **Cyber Security Policy** – Manages and coordinates the Departmental cyber security policy for sensitive (unclassified) systems throughout the 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 the Bureaus' and the 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 the 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 the 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, the 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 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

Consistent with applicable FISMA requirements, OMB policy, and NIST guidelines, the Treasury has established an information security program and related practices for its non-IRS bureaus' unclassified systems. This program covers the 11 FISMA program areas: 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 needed improvements in 5 of 11 FISMA program areas. We have made 11 recommendations related to these control deficiencies that, if effectively addressed by management, should strengthen the respective bureaus, offices, and the 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 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.

Additionally, we evaluated all prior-year findings from the fiscal year (FY) 2012 and 2011 FISMA Performance Audits and noted that management had closed 33 of 40 findings. For 2 of the 40 findings, we were unable to test the corrective actions by our end of fieldwork date, June 30, 2013. For these findings, we noted they were closed by Treasury but untested by KPMG and should be evaluated as part of the FY 2014 independent evaluation. See Appendix II, *Status of Prior-Year Findings*, for additional details.

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

FINDINGS

1. Logical account management activities were not in place or not consistently performed by DO, Mint, and TIGTA

We identified instances of noncompliance with logical access policies at DO, Mint, and TIGTA. We noted the following:

1. Account management activities were not consistently performed as required by TD P 85-01 Volume I, *Treasury Information Technology Security Program*, and bureau-specific policies at DO and Mint.
   - 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. *(See Recommendations #1 and #2.)*
   - 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. *(See Recommendations #3 and #4.)*

2. 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.

These control deficiencies demonstrate that these bureaus did not appropriately implement policies for approving and reviewing user access and following NIST's concept of least privilege.[3]

By failing to retain evidence of all user and administrator accounts approvals, there is an increased risk that users could have unauthorized access and/or modify production data on their respective systems or the network.

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.

[3] The NIST SP 800-53, Rev. 3, defines least privilege as allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

2. For the selected system, ensure that all users are authorized and maintain evidence of the authorization of users.

We recommend that Mint management:

3. 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.

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

Based on the planned corrective actions for TIGTA, we are not making additional recommendations.

2. Security incidents were not reported correctly at Fiscal Service and OIG

Treasury bureaus are required to submit all security incidents to the TCSIRC within specified time frames categorized by incident severity. The evaluation identified that Fiscal Service reported incidents later than United States Computer Emergency Readiness Team (US-CERT) and Treasury recommended guidelines. We also noted that OIG reported Category (CAT) 1 incidents incorrectly as CAT 4 incidents. Specifically, we noted the following:

- 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. *(See Recommendations #5 and #6.)*
- 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. *(See Recommendation #7.)*

By not reporting security incidents in a timely manner and under the correct categorization, these bureaus 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, the bureaus can impair the TCSIRC's and the US-CERT's ability to track, analyze, and act on aggregated incident data within prescribed timeframes.

We recommend that Fiscal Service management:

5. 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.

6. 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.

We recommend that OIG management:

7. 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.

3. FinCEN and Fiscal Service did not follow NIST guidance for SSPs

NIST and Treasury guidance require that Treasury SSPs remain up-to-date and current with the NIST Risk Management Framework and require NIST Special Publication (SP) 800-53, Revision (Rev.) 3, security controls. Specifically, we noted that:

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

Failing to document an up-to-date baseline of security controls may have a negative effect on subsequent security activities. Specifically, FinCEN and Fiscal Service may not be able to implement, assess, authorize, and monitor the security 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 FinCEN management:

8. Update the system SSP to address and reference the outstanding NIST SP 800-53 Rev. 3 controls and control enhancements for a HIGH baseline.

9. Conduct thorough reviews of the system SSP annually to ensure that it includes applicable NIST SP 800-53 Rev. 3 controls.

We recommend that Fiscal Service management:

10. Ensure that subsequent to the selected system's security assessment, the SSP should undergo annual reviews.

4. Contingency planning and testing controls were not fully implemented or operating as designed at TIGTA

The TD P 85-01 requires Treasury bureaus to protect their information systems in the event of a disaster. Bureaus must create plans for system recovery and test these plans. 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.

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 TIGTA 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 TIGTA information and information systems in the event of a disaster.

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

5. Evidence of successful completion of annual security awareness training was not retained for some users at OIG

NIST standards and the TD P 85-01 requires that all users complete IT Security Awareness Training on an annual basis. Additionally, department guidance requires that individual training records are retained for a period of five years. 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. *(See Recommendation #11.)*

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 OIG management:

11. 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.

MANAGEMENT RESPONSE TO THE REPORT

The following is the Treasury CIO's response, dated October 29, 2013, to the FY 2013 FISMA Evaluation Report.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OCT 29 2013

MEMORANDUM FOR MARLA A. FREEDMAN
ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: Robyn East
Deputy Assistant Secretary for Information Systems
and Chief Information Officer (CIO)

SUBJECT: Management Response to Draft Evaluation Report – "The Department of the Treasury's Federal Information Security Management Act Fiscal Year 2013 Evaluation"

Thank you for the opportunity to comment on the draft report entitled, "The Department of the Treasury Federal Information Security Management Act [FISMA] Fiscal Year 2013 Evaluation." We are pleased that the report found that our security program is generally consistent with FISMA requirements, OMB information security policy, and related information security standards and guidance published by the National Institute of Standards and Technology. 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 items 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. For example, we closed all but three of the 31 recommendations from last year's FISMA audit. Also, as the Department continues to transition to OMB's eventual goal of "real-time" reporting capability, we have accomplished a number of achievements, to include:

- Consolidated 99 percent of external network traffic through Trusted Internet Connection access points, achieving "green" status against a Cross-Agency Administration Priority target.

- Complied with OMB policy on Domain Name Server (DNS) Security by digitally signing at least 95 percent of external-facing second-level DNS names. This is important to reduce the ability of others to impersonate Treasury websites.

- Re-aligned and updated the Department's core cybersecurity policies for unclassified and collateral classified information systems to be consistent with the latest federal policies and guidelines to protect the agency from potential adversaries and other threats.

- Began participation in the Department of Homeland Security-sponsored Continuous Diagnostic and Mitigation Program, which will provide Continuous Monitoring as a Service–related products, services, and solutions at minimal cost to the agency. We anticipate that participation in this program will enable the Department to improve its performance with respect to government-wide goals for continuous monitoring in FY 2014.

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 were not in place or not consistently performed by DO, Mint, and TIGTA

KPMG Recommendation 1: For DO, we recommend that management: For the selected system, implement a process or mechanism to track the administrators' account information, including account creation date.

> **Treasury Response:** Treasury agrees with the finding and recommendation. The process for granting administrative privileges was instituted in April 2013 to ensure all vendor access has been authorized in the form of a background investigation. A collaborative workspace was stood up to increase visibility of the vendor account management process and includes artifacts to support submission and successful adjudication of a background investigation, which leads to account creation and is tracked with a date on the vendor system. Target Completion: April 7, 2013
>
> **Responsible Official:** Departmental Offices, Information Owner (IO) for the selected system.

KPMG Recommendation 2: For DO, we recommend that management: For the selected system, ensure that all users are authorized and maintain evidence of the authorization of users.

> **Treasury Response:** Treasury agrees with the finding and recommendation. DO will establish annual reviews of user accounts to ensure that all users are authorized. The IO will maintain evidence of the authorization of all users. Target Completion: April 7, 2014
>
> **Responsible Official:** Departmental Offices, IO for the selected system.

KPMG Recommendation 3: For Mint, we recommend that management: 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.

> **Treasury Response:** Treasury agrees with the finding and recommendation. Mint has instituted development of new Standard Operating Procedures that outline the approval process for approving users' access to the system, management and disposition of user access authorization, and periodic review of procedures. System documentation will be updated to reflect new processes. Target Completion: January 15, 2014
>
> **Responsible Official:** Mint, Chief Information Security Officer

KPMG Recommendation 4: For Mint, we recommend that 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. Validation for all existing users' access will occur using the new processes being developed by the Mint. This will ensure the creation and preservation of user access, determination that users have appropriate access, and completion of updates to system documentation to reflect new processes is addressed in a timely manner. Target Completion: January 15, 2014

Responsible Official: Mint, Chief Information Security Officer

KPMG: Based on the planned corrective actions for TIGTA, we are not making additional recommendations.

KPMG Finding 2: Security incidents were not reported correctly at Fiscal Service and OIG

KPMG Recommendation 5: For Fiscal Service, we recommend that management: 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.

Treasury Response: Treasury agrees with the finding and recommendation. Fiscal Service will update its Incident Handling and Response Standard Operating Procedures to account for the additional processes performed by the Enterprise Security Services – Security Divisions. Target Completion: May 30, 2014

Responsible Official: Fiscal Service, Chief Information Officer

KPMG Recommendation 6: For Fiscal Service, we recommend that management: Ensure that Fiscal Service Security reports all CAT 1 incidents to TCSIRC [the Treasury Cyber Security Incident Response Center] 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.

Treasury Response: Treasury agrees with the finding and recommendation. Fiscal Service will ensure that all CAT 1 incidents are reported to TCSIRC in compliance with revised standard operating procedures. In addition, the Bureau will provide additional training to the Incident Responder team once the incident response standard operating procedures are revised. Target Completion: May 30, 2014

Responsible Official: Fiscal Service, Chief Information Officer

KPMG Recommendation 7: For OIG, we recommend that 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.

Treasury Response: Treasury agrees with the finding and recommendation. OIG has ensured that its staff is aware of the current Treasury Policy regarding the proper categorizing of incidents. Completed: September 30, 2013

Responsible Official: OIG, Director of Information Technology

KPMG Finding 3: FinCEN and Fiscal Service did not follow NIST guidance for SSPs

KPMG Recommendation 8: For FinCEN, we recommend that management: Update the system SSP to address and reference the outstanding NIST SP 800-53 Rev. 3 controls and control enhancements for a HIGH baseline.

Treasury Response: Treasury agrees with the finding and recommendation. FinCEN will update the SSP document with the missing controls. Target Completion: November 30, 2013

Responsible Official: FinCEN, Chief Information Security Officer

KPMG Recommendation 9: For FinCEN, we recommend that management: Conduct thorough reviews of the system SSP annually to ensure that it includes applicable NIST SP 800-53 Rev. 3 controls.

Treasury Response: Treasury agrees with the finding and recommendation. FinCEN will review system security plans annually to ensure applicable NIST SP 800-53 Rev. 3 controls are included. Target Completion: November 30, 2013

Responsible Official: FinCEN, Chief Information Security Officer

KPMG Recommendation 10: For Fiscal Service, we recommend that management: Ensure that subsequent to the selected system's security assessment, the SSP should undergo annual reviews.

Treasury Response: Treasury agrees with the finding and recommendation. Fiscal Service will ensure that, subsequent to the selected system's security assessment, the SSP will undergo annual reviews. Target Completion: September 30, 2014

Responsible Official: Fiscal Service, Chief Information Officer

KPMG Finding 4: Contingency planning and testing controls were not fully implemented or operating as designed at TIGTA

KPMG: Based on the planned corrective actions for TIGTA, we are not making a recommendation.

KPMG Finding 5: Evidence of successful completion of annual security awareness training was not retained for some users at OIG

KPMG Recommendation 11: For OIG, we recommend that 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 are retained.

Treasury Response: Treasury agrees with the finding and recommendation. OIG will ensure successful completions of annual security awareness training by requiring that employees provide a copy of the completed training certificate to supplement the reports provided by the Treasury Learning Management System (TLMS). Target Completion: June 1, 2014

Responsible Official: OIG, Director of Information Technology

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY

The objectives for this Federal Information Security Management Act (FISMA) evaluation was to conduct an independent evaluation of the information security program and practices of Department of the Treasury (Treasury) to assess the effectiveness of such programs and practice for the year ending June 30, 2013 as they relate to non-Internal Revenue Service (IRS) information systems. Specifically, the objectives of this evaluation are 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 2013 Inspector General Federal Information Security Management Act Reporting Metrics*, dated November 30, 2012. We reviewed the Treasury information security program for a program-level perspective and then examined how each bureau 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 Department-Level Compliance

To gain an enterprise-level understanding, we assessed management, policies, and guidance for the overall Treasury-wide information security program per requirements defined in FISMA and DHS *FY 2013 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-Level Compliance

To gain a bureau-level understanding, we assessed the implementation of the guidance for the 11[4] bureau- and office-wide information security programs according to requirements defined in FISMA and DHS *FY 2013 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 C: System Level (Limited)

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

To gain an understanding of how effectively the bureaus implemented information security controls at the system level, we assessed the implementation of a limited selection of security controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 3, for a subset of Treasury information systems (see Appendix IV).

We also tested a subset of 15 information systems from a total population of 113 non-IRS major applications and general support systems as of May 16, 2013.[5] We tested the 15 information systems to assess whether bureaus were effective in implementing the Treasury's security program and meeting the Federal Information Processing Standards (FIPS) 200 minimum-security standards to protect information and information systems. 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 Community Development Financial Institutions (CDFI) Fund.[6]

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 the Treasury's and bureaus' policies, procedures, and guidelines. Lastly, we evaluated selected security-related documents and records, including certification and accreditation (C&A) packages, configuration assessment results, and training records.

We performed our fieldwork at the Treasury's headquarters offices in Washington, D.C., and bureau locations in Washington, D.C.; Hyattsville, Maryland; and Vienna, Virginia, during the period of April 22, 2013 through July 31, 2013. 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.[7] The

[5] 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 CDFI Fund, rather than selecting a random sample of information systems that might exclude a Treasury bureau.

[6] Our rotational system selection strategy precludes selecting systems reviewed within the past two years. In FY 2012 and FY 2011, both of CDFI Fund's only two systems were selected. Therefore, and in accordance with the OIG's instruction, we excluded that bureau's systems from our sample selection in FY 2013.

[7] Note (per *FY 2013 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

following is a listing of the criteria used in the performance of the fiscal year (FY) 2013 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. 3, Recommended Security 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*

United States Department of Homeland Security

- *DHS FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*

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.

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 FY 2013, we conducted a FISMA Evaluation versus a FISMA Performance Audit, which were conducted in FY 2012 and FY 2011. 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 recommendations were determined to be implemented, we closed the findings. If recommendations were determined to be only partially implemented or not implemented at all, we determined the finding to be open. For 2 of the 40 findings, we were unable to test the corrective actions by our end of fieldwork date, June 30, 2013. For these findings, we noted that they were closed but untested and should be evaluated as part of the FY 2014 independent evaluation.

Prior Year Findings – 2012 Performance Audit

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #1 – Bureau of the Public Debt (BPD) Logical account management activities were not in place or not consistently performed.	For the two selected BPD systems, BPD management could not provide sufficient supporting documentation evidencing the users' last log-on date or time. As a result, we were unable to test the operating effectiveness of the controls over whether inactive users are disabled.	We recommend that BPD management: 1 For both selected systems, develop or acquire additional system capability that generates user lists with last log-on dates so that inactive users are automatically disabled in a timely manner. 2 For both selected systems, in the absence of a long-term system capability solution, perform manual monthly reviews of all system user accounts and disable or delete accounts that no longer need access.	**Implemented/Untested** FMS and BPD consolidated into one organization, Fiscal Service, in October 2012. Fiscal Service reports that it implemented automated emails that run on a daily basis to show users' last log-on dates for the two selected systems. However, Fiscal Service did not complete the corrective actions until June 2013. Therefore, we were unable to test the effectiveness. The finding will be tested as part of the FY 2014 FISMA evaluation.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #1 – Bureau of Alcohol and Tobacco Tax and Trade Bureau (TTB) Logical account management activities were not in place or not consistently performed.	TTB had three active user accounts that should have had access revoked. One account, a test account, had last logged in on March 22, 2012 and the account was not deactivated after 60 days of inactivity. Another account was for an individual who had separated in July 2011 but still had an enabled account. Additionally, there was a separated individual whose account was still active 20 days after her departure. TTB management explained that it did not have an automated mechanism to disable inactive accounts due to a technical limitation; therefore, some user accounts were not properly disabled in a timely manner. Additionally, TTB stated that access removal for separated employees was a manual process by each employee's supervisor and that human error occurred.	We recommend that TTB management: 1 Implement an automated mechanism, a script, or manual review process to ensure inactive accounts are disabled after 60 days of inactivity. 2 Ensure that supervisors are aware of their responsibilities to remove the access of separated employees.	**Implemented/Closed** TTB has implemented an automated script that runs on a weekly basis. Accounts that are 60 days inactive are automatically disabled. In addition, a notice was sent out to all supervisory staff and Contract Officer Representatives (CORs) detailing their responsibility for completing the "Delete All Access" process for departing staff members.
Prior Year FY 2012 Finding #1 –Departmental Office (DO) Logical account management activities were not in place or not consistently performed.	For a selected DO system, DO management did not formally document and maintain access request forms for privileged user accounts. This was self-discovered during the systems continuous monitoring test performed in June 2012. While there was a documented corrective action plan in the continuous monitoring report, there was not an updated POA&M item during the FISMA year.	We recommend that DO management include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.	**Implemented/Closed** We noted that a POA&M item was added for the selected system, which cross-referenced the corrective action plans from the continuous monitoring report.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #1 –Office of Comptroller of the Currency (OCC) Logical account management activities were not in place or not consistently performed.	OCC did not incorporate all general support system user accounts of Office of Thrift Supervision (OTS), the bureau that OCC partially took over last year, as part of its access review process. When OTS migrated to OCC, most of the accounts were changed from OTS accounts to OCC accounts. Fourteen users were not transferred over. OCC noticed this when they did their account review and created a POA&M to remediate it. This was a self-reported finding and documented within OCC's POA&M report in the Trusted Agent FISMA (TAF) system and scheduled to be corrected on July 31, 2012.	Based on the planned corrective actions for OCC, we are not making additional recommendations.	**Implemented/Closed** We noted all old OTS accounts have been changed to OCC accounts.
Prior Year FY 2012 Finding #1 –Financial Crimes Enforcement Network (FinCEN) Logical account management activities were not in place or not consistently performed.	A selected FinCEN system had a user account on the database that had unnecessary access permissions. We noted this was due to database accounts not being sufficiently reviewed for access privileges. This was a self-identified weakness as a result of FinCEN's security assessment and authorization and scheduled to be corrected on January 14, 2013.	Based on the planned corrective actions for FinCEN, we are not making additional recommendations.	**Implemented/Closed** The SSP for the selected system, dated June 2013, states that POA&M has been closed. User accounts on the database are reviewed for unnecessary access privileges on a regular basis.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #2 - Bureau of Engraving & Printing (BEP) Security incidents were not reported in a timely manner.	BEP did not report 3 of the 15 sampled security incidents to TCSIRC within the one-hour time period required for a CAT 1 incident. Specifically, one incident was reported 50 minutes late, one incident was reported 65 minutes late, and another incident was not reported until seven days after identification. BEP Help Desk reports incidents to the designated BEP Incident Coordinator, who then forwards the reported incident to the BEP CSIRC Management Team. This two-step process caused delays with the submission of the security incident to TCSIRC within BEP's documented time frames. Additionally, not all Help Desk members had been fully trained to respond to security incidents and properly report them to the BEP CSIRC Management Team.	We recommend that BEP management: 1 Revise the current Incident Response reporting process and written procedures to have the Help Desk send all incidents to the CSIRC group as opposed to the BEP Incident Coordinator. 2 Provide additional training to the Help Desk team members regarding BEP's incident response policies and procedures to ensure they are consistently implemented. Additional training for Help Desk personnel should include the same curriculum used by BEP CSIRC management team members to allow for better understanding of the incident reporting process.	**Implemented/Closed** Policies, procedures and training materials have been updated to document and train Help Desk staff on the new process for reporting security incidents. When a ticket is created for a CAT 1 incident, the system automatically notifies the BEP CSIRC and the TCSIRC of the incidents. In addition, every member who was noted in the CSIRC training attendance sheet attended the required BEP CSIRC training.
Prior Year FY 2012 Finding #2 - Bureau of the Public Debt (BPD) Security incidents were not reported in a timely manner.	BPD did not report one out of three security incidents within the required one-hour time period for a CAT 1 incident (the incident took 14 hours to report). The delay was caused by BPD's reliance on United Parcel Service (UPS) to verify the status of a missing package. BPD followed UPS's advice and waited until the following day when the next UPS delivery was made to ensure that the package was truly lost.	We recommend that BPD management: 1 Ensure that BPD's CSIRC report all CAT 1 incidents to US-CERT within one hour regardless of any additional procedures (follow- up, confirmation, or additional feedback from third party) performed by CSIRC personnel. 2 Provide additional training to the BPD's CSIRC management team regarding BPD's incident response policies and procedures to ensure that all incidents are reported in time regardless of reliance on third parties to confirm incident	**Reissued/Closed** FMS and BPD consolidated into one organization, Fiscal Service, in October 2012. As a result of this consolidation, we closed this prior year finding and created a new security incident finding specific to Fiscal Service.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #2 - Financial Crimes Enforcement Network (FinCEN) Security incidents were not reported in a timely manner.	FinCEN did not report 1 of the 12 incidents to TCSIRC within the required one-hour time period for a CAT 1. Specifically, the incident was reported 69 hours after identification. There was only one person responsible for FinCEN's CSIRC reporting, and the incident occurred when this person was out of the office, which delayed reporting until he returned. At the time, there were no backup CSIRC personnel.	We recommend that FinCEN management evaluate its current CSIRC capability for collecting and submitting incident responses and implement backup CSIRC personnel to ensure that incident response tickets are handled in a timely fashion.	**Implemented/Closed** Updated policies, procedures, and training materials have been implemented. The updates help to document and train the help desk staff about the improved way of reporting security incidents. In addition, all security incident response reports received for the current year are compliant and have been handled in a timely manner.
Prior Year FY 2012 Finding #3 – Office of Comptroller of the Currency (OCC) System security plans at OCC and FMS did not fully document all security controls from NIST SP 800-53, Rev. 3.	The two selected information systems from OCC did not include all required security controls in areas such as access control, audit and accountability, contingency planning, identification and authentication, maintenance, media protection, system and communications protection, and system and information integrity, as specified in NIST SP 800-53, Rev. 3. We noted that the conditions cited above occurred because OCC management did not perform an adequate review of the two selected systems' SSPs and overlooked the lack of these controls and control enhancements when updating the SSPs.	We recommend that OCC management: 1 For both selected systems, update the SSP to address and reference all the NIST SP 800-53, Rev. 3, security controls and control enhancements for a Moderate baseline. 2 For both selected systems, ensure management conducts an adequate review of the SSPs to ensure that it includes applicable NIST SP 800-53, Rev. 3, and controls.	**Implemented/Closed** Both selected system's SSPs have been updated and reviewed by management to ensure all the NIST SP 800-53, Rev. 3, security controls and control enhancements for a Moderate baseline have been referenced.
Prior Year FY 2012 Finding #3 – Financial Management Service (FMS) One SSP [system security plans] for FMS was not updated to address weaknesses identified in the security assessments.	The SSP for a selected FMS system did not reflect the current and primary source of backups for the application. FMS management stated that the error was due to a management oversight when updating the SSP.	We recommend that FMS management update the selected system's SSP to reflect the current and primary source of backups for the application.	**Implemented/Closed** FMS and BPD consolidated into one organization, Fiscal Service, in October 2012. Fiscal Service has updated the system security plan documentation to reflect the current primary backup process accurately.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #3 – Financial Crimes Enforcement Network (FinCEN) One SSP [system security plans] for FinCEN was not updated to address weaknesses identified in the security assessments.	FinCEN's SSP for the selected system did not reflect the results of their latest Security Assessment and Authorization, which required certain controls to be updated to reflect self-identified weaknesses. It was noted that this was a self-reported finding and was listed as a POA&M with the TAF system with an estimated date of completion of January 14, 2013.	Based on the planned corrective actions for FinCEN, we are not making a recommendation.	**Implemented/Closed** The SSP has been updated on June 2013 and signed off by the System Owner. The SSP reflects the results of their latest Security Assessment and Authorization.
Prior Year FY 2012 Finding #4 – Financial Management Service (FMS) Audit logs were not sufficiently reviewed by FMS in accordance with NIST and Department of the Treasury requirements.	A selected FMS system's audit capabilities and functions did not adhere to the Fiscal Service Baseline Services Requirements (BLSR) and NIST SP 800-53, Rev. 3, guidance as required for HIGH categorized systems. Specifically, it did not have any automated capabilities or any supporting processes to log and monitor security-relevant events. When designing the system, FMS management did not adequately identify requirements and provide capabilities to log and monitor security-related events. In addition, management did not establish a robust monitoring process to support the review and follow-up of selected auditable events, and management did not document within their system security plan specific security-related events that will be monitored on an ongoing basis.	We recommend that FMS management: 1 Enhance the selected system audit capabilities to capture security-related events as prescribed by the BLSR and NIST SP 800-53 guidance. 2 Establish a clear oversight process to review the security-related events and ensure appropriate follow-up action is taken as prescribed by the BLSR and NIST SP 800-53. 3 Update the selected system's system security plan to document security-related events that need to be monitored as prescribed by the BLSR.	**Implemented/Closed** FMS and BPD consolidated into one organization, Fiscal Service, in October 2012. Fiscal Service has updated the system security plan to document security related events that need to be monitored and it is consistent with the BLSR. In addition, management has enhanced its system audit capabilities to capture security events as prescribed by the BLSR and NIST SP 800-53 and established a clear oversight process to review the security-related events and follow-up where appropriate.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #4 – Departmental Offices (DO) Audit logs were not sufficiently reviewed by FMS and DO in accordance with NIST and Department of the Treasury requirements.	A selected DO system lacked a process to review audit records. DO management self-identified this weakness during a continuous monitoring assessment in June 2012. While there was a documented corrective action plan in the continuous monitoring report, there was not an updated POA&M item during the FISMA year.	We recommend that DO management include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.	**Implemented/Closed** We noted that a POA&M item was added for the selected system, which cross-referenced the corrective action plans from the continuous monitoring report.
Prior Year FY 2012 Finding #5-Departmental Offices (DO) Plans of Action and Milestones (POA&Ms) were not tracked in accordance with NIST and Department of the 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.	**Partially Implemented/Open** DO updated the POA&M to include all the findings and remediation's documented in the selected system's Continuous Monitoring Test Report. There was no continuous monitoring test done this year due to moving of facilities, so they were not able to update the POA&M with any new results.
Prior Year FY 2012 Finding #6 – Financial Management Service (FMS) Vulnerability scanning and remediation was not performed in accordance with Department of the Treasury requirements.	For a selected FMS system, FMS was unable to provide us with supporting documentation confirming that vulnerability scans were being performed over the system's Internet Protocol (IP) addresses. Therefore, we could not determine if vulnerability scans had been performed, if any vulnerabilities were identified, and if any corresponding corrective actions or POA&M had been implemented	We recommend that FMS management: 1 Formally document the vulnerability scanning and flaw remediation processes for the Fiscal Services organization and communicate the processes to affected field personnel. 2 Maintain a complete listing of hosts and IP addresses for the selected FMS system production environment and document any changes to this listing, and retain enough supporting documentation to confirm the accuracy of completed vulnerability scans.	**Implemented/Closed** Formal documentation with the SOP was created to document the vulnerability scanning and flaw remediation process. Management maintains a complete listings of hosts and IP addresses and retains supporting documentation to confirm the accuracy of completed vulnerability scans.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #6 – Mint Vulnerability scanning and remediation was not performed in accordance with Department of the Treasury requirements.	For a selected Mint system, the November 2011 vulnerability scan contained vulnerabilities with a high risk rating that were not remedied prior to the March 2012 vulnerability scans. The Mint POA&M report from TAF, generated in June 2012, did not reflect the open vulnerabilities. These vulnerabilities were not properly remedied due to the Mint's management decision to remediate noncritical vulnerabilities using a risk-based approach. This risk-based approach did not address all noncritical vulnerabilities in a timely manner and deviated from the Mint's vulnerability remediation policy, which requires noncritical patches to be applies on a bimonthly basis.	We recommend that Mint management follow their vulnerability remediation policy for all vulnerabilities, including older, noncritical patches, to ensure that vulnerabilities are not missed in the remediation process.	**Implemented/Closed** Mint updated their vulnerability remediation policy and patched open vulnerabilities in a timely manner.
Prior Year FY 2012 Finding #6 – Departmental Offices (DO) Vulnerability scanning and remediation was not performed in accordance with Department of the Treasury requirements.	For the selected DO system, DO management identified multiple high-risk weaknesses in vulnerability scans and missing scans for database components during DO's continuous monitoring assessment in 2012. While a documented corrective action plan was established in the continuous monitoring report, the weaknesses were not recorded in the POA&M during the FISMA year.	We recommend that DO management include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.	**Implemented/Closed** We noted that a POA&M item was added for the selected system, which cross-referenced the corrective action plans from the continuous monitoring report.

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 Department of the 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/Untested** FMS and BPD consolidated into one organization, Fiscal Service, in October 2012. We noted that Fiscal Service corrected the vulnerability remediation procedures but did not complete all corrective actions until June 2013 and was unable to test the effectiveness. The finding will be tested as part of the FY 2014 FISMA evaluation.
Prior Year FY 2012 Finding #6 – Office of Comptroller of the Currency (OCC) Vulnerability scanning and remediation was not performed in accordance with Department of the Treasury requirements.	For both selected OCC systems, OCC management identified multiple high-risk weaknesses in vulnerability scans that were not remediated. This was a self-reported finding and documented within OCC's POA&M report on TAF. The POA&M item is scheduled to be completed on August 15, 2012.	Based upon the planned correction actions for OCC, we are not making a recommendation.	**Implemented/Closed** Weaknesses discovered in vulnerability scans were remediated.
Prior Year FY 2012 Finding #7 – Departmental Offices (DO) Contingency planning and testing controls were not fully implemented or operating as designed.	Contingency plan documentation for a selected DO system was not updated within the FISMA year. Additionally, contingency plan testing was not performed for the system within the FISMA year. DO management self-identified these weaknesses during a continuous monitoring assessment in June 2012. While there was a documented corrective action plan in the continuous monitoring report, there was not an updated POA&M item during the FISMA year.	We recommend that DO management include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.	**Implemented/Closed** We noted that a POA&M item was added for the selected system, which cross-referenced the corrective action plans from the continuous monitoring report.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #7 – Financial Management Service (FMS) Contingency planning and testing controls were not fully implemented or operating as designed.	For one selected FMS system, FMS management identified the contingency plan test was not performed within the FISMA year. This was a self-reported finding and documented within FMS's POA&M report on TAF, with an estimated completion date of August 30, 2012. For another selected FMS system, FMS management identified one of three disaster recovery exercise reconstitution test objectives was not completed during contingency plan testing. This was a self-reported finding and documented within FMS's POA&M report on TAF, with an estimated completion date of August 30, 2012.	Based on the planned corrective actions for FMS, we are not making a recommendation.	**Implemented/Closed** We determined that contingency plan tests were performed and completed as of September 2012 for both systems.
Prior Year FY 2012 Finding #8 – Bureau of the Public Debt (BPD) Backup controls were not in place or were not operating as designed**.**	BPD management could not provide sufficient supporting documentation evidencing that the backup jobs were run successfully. As a result, we were unable to test the operating effectiveness of the controls over backups. The weekly backup logs did not specify whether the selected backup jobs were successful or had failed. BPD stated that the system was not configured to include the backup status on the logs.	We recommend that BPD management enhance the logging capability of the system's backup process so management can determine whether the backups were successfully completed.	**Implemented/Closed** The audit logging capability of the system has been enhanced to confirm if a backup has been successfully completed.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #8 – Community Development Financial Institutions (CDFI) Fund Backup controls were not in place or were not operating as designed.	Backups of CDFI Fund data for the selected system were not being performed on a regular basis. Upon inspection of all successful backups between December 2011 and April 2012, it was noted that backups of data were occurring, but the frequency ranged from two to seven times a month. This did not comply with the SSP, which indicated that daily incremental backups and a weekly full backups occur. CDFI Fund stated that TTB took over the backup responsibilities in May 2012, and, as a result of the upcoming transition, evidence for successful backups was not maintained.	We recommend that CDFI Fund management ensure that the system backups are completed successfully per the defined frequency in the SSP, and retain evidence of successful completion for one year.	**Implemented/Closed** We noted daily incremental backups and a weekly full backup are being performed, as required by the SSP.
Prior Year FY 2012 Finding #9 – Departmental Offices (DO) System configuration settings were not implemented properly.	A selected DO system lacked sufficient mechanisms to track and detect unauthorized changes. DO management self-identified these weaknesses during a continuous monitoring assessment in June 2012. While there was a documented corrective action plan in the continuous monitoring report, there was not an updated POA&M item during the FISMA year.	We recommend that DO management include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.	**Implemented/Closed** We noted that a POA&M item was added for the selected system, which cross-referenced the corrective action plans from the continuous monitoring report.
Prior Year FY 2012 Finding #9 – Office of Comptroller of the Currency (OCC) System configuration settings were not implemented properly.	For both selected OCC systems, OCC management identified configuration settings were not set to the most restrictive settings possible. Both systems had multiple weaknesses identified in configuration settings that did not meet the require threshold for restrictive settings as stated by NIST. This was a self-reported finding and documented within OCC's POA&M report on TAF. The POA&M item is scheduled to be completed on December 31, 2013.	Based upon the planned correction actions for OCC, we are not making a recommendation.	**Implemented/Closed** Established the definitive OCC baseline configurations and reviewed all configurations to ensure compliance to the baseline.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #10 – Bureau of the Public Debt (BPD) System baselines were not documented properly.	Both selected BPD systems did not have baseline configurations formally documented. BPD management was aware of the lack of this documentation for both systems; however, management had planned to rely on system backups to restore system information in case of a disaster event.	We recommend that BPD management for both selected systems, develop baseline configurations (applications build guides) that are consistent with the system's SSP and Federal Enterprise Architecture.	**Implemented/Closed** Baseline configurations were developed that are consistent with both the SSP and Federal Enterprise Architecture.
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.	**Partially Implemented/Open** We noted that Management developed an Enterprise Configuration Management Plan to address Recommendations #1 and #3 in March 2013. However, Management has not updated the Configuration Management Plan per Recommendation #2, and is still open with a new estimate of completion in October 2013.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2012 Finding #10 – Financial Crimes Enforcement Network (FinCEN) System baselines were not documented properly.	KPMG confirmed that, for a selected FinCEN system, FinCEN management identified the baseline settings were outdated. This was a self-reported finding and documented within FinCEN's POA&M report on TAF. The POA&M item is scheduled to be completed on January 14, 2013.	Based upon the planned correction actions for FinCEN, we are not making a recommendation.	**Implemented/Closed** System baselines have been identified and documented properly.
Prior Year FY 2012 Finding#11 – Financial Management Service (FMS) Multifactor authentication was not implemented.	NIST SP 800-53, Rev. 3, guidance requires systems to implement multifactor authentication to local and network access to privileged and nonprivileged accounts. Multifactor authentication provides an additional level of security for accounts to prevent unauthorized access within the IT infrastructure. KPMG confirmed that, for the selected FMS system, FMS management identified it did not implement multifactor authentication for any level of access to the system. This was a self-reported finding and documented within FMS's POA&M report on TAF. The POA&M item is scheduled to be completed on December 31, 2012.	Based on FMS's planned corrective actions, we are not making a recommendation.	**Implemented/Closed** Management implemented multifactor authentication to local and network access for privileged and non-privileged accounts.

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.	**Open.** In FY 2012, we were informed that Recommendation #1 of the FY 2011 finding has been addressed. However in FY 2013, we noted that 19 active user accounts have not logged in greater than 120 days since the list was generated (July 15, 2013 or earlier). Also, of these active users, five accounts did not have a "last log on date", when their account had been created more than 120 days before the listing was generated.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2011 Finding #2 – FMS Security incidents were not reported timely.	FMS employees did not immediately report 10 of 10 confirmed security incidents to FMS's help desk as required by FMS policy. Additionally, FMS's information security group did not report seven of these confirmed security incidents to TCSIRC within the required one-hour time period for Category 1 incidents (three security incidents were reported in one day, two were reported in two days, and the remaining three were reported in three days). Rather than report all suspected and confirmed incidents, FMS failed to notify TCSIRC until sufficient evidence was gathered and approved by FMS executives as required by FMS policies and procedures. Contributing to the untimely reporting was a lack of after-hours coverage by the incident response personnel. Additionally, we attributed the untimely reporting by FMS employees to a lack of sufficient awareness and training.	We recommend that FMS management: 1 Revise the current incident reporting process and associated written procedures to ensure timely reporting. This could include the FMS incident response management notifying TCSIRC with suspected or confirmed security events without the need for further FMS Executive management approvals. 2 Provide additional training to FMS security personnel regarding FMS's revised incident response policies and procedures to ensure these policies and procedures are consistently implemented. 3 Consider, if feasible, a Distributed Incident Response Team or a Partially Outsourced Team to achieve 24x7x365 coverage, per the NIST SP 800-61, *Computer Security Incident Handling Guide*. Such a strategy could involve sharing TCSIRC resources with other Department of the Treasury bureaus. 4 Improve FMS employee awareness to report both confirmed and suspected security incidents to the FMS Service Desk. FMS could create awareness through periodic reminders via e-mail, posting security posters in common employee areas, and through increased emphasis in annual security and awareness training.	**Reissued/Closed** FMS and BPD consolidated into one organization, Fiscal Service, in October 2012. As a result of this consolidation, we closed this prior year finding and created a new security incident finding specific to Fiscal Service.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2011 Finding #3 – DO SSPs did not fully adopt NIST recommended security controls from NIST Special Publication (SP) 800-53, Rev. 3.	NIST and Treasury guidance require that Treasury SSPs remain up-to-date and current with the NIST Risk Management Framework and required NIST SP 800-53 security controls. We noted that one sampled information system from DO utilized outdated NIST guidance (Rev. 2). Specifically, the SSPs did not include all required security controls as specified in NIST SP 800-53, Rev. 3, *Recommend Security Controls for Federal Information Systems and Organizations*, dated August 2009. We noted that the conditions, cited above for DO had various factors including the bureau and vendor's misunderstanding of contract requirements to maintain compliance with all NIST standards.	We recommend that DO management instruct the vendor to update the SSPs to include NIST SP 800-53, Rev. 3, security controls and associated control enhancements.	**Implemented/Closed** The selected systems have updated the SSP to reference all of the NIST SP 800-53, Rev. 3, security controls and control enhancements for a High baseline.
Prior Year FY 2011 Finding #3 – FMS SSPs did not fully adopt NIST recommended security controls from NIST SP 800-53, Rev. 3.	During the audit period, FMS revised their SSP template and associated checklist to incorporate NIST SP 800-53, Rev. 3, controls. However, the sampled system's SSP utilized older Rev 2 controls and FMS's quality control process did not reject this sampled SSP.	We recommend that FMS management ensure that System Owners and ISSOs review and update SSPs by using the FMS-approved SSP template and baseline security requirements, which incorporate NIST SP 800-53, Rev. 3, security controls.	**Implemented/Closed** KPMG noted that the SSP had been updated on June 30, 2013 to align with NIST SP 800-53, Rev. 3 guidance.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2011 Finding #4 – FMS Insufficient audit log reviews.	For a sampled application, FMS did not document their weekly review of failed login events during the FISMA audit period. While FMS took actions to address a similar issue in a prior-year financial statement audit by developing audit log review procedures for failed login attempts, the limited scope of FMS's corrective actions did not include a risk analysis necessary to identify significant audit events worthy of review and subsequent investigations, as suggested by NIST SP 800-53 security control AU-2, *Auditable Events.* The audit log review and SSP did not address broader user account activities such as the creation of new accounts with administrative capabilities or changes in user account permissions. In addition, the proposed audit log review procedures did not include monitoring changes to specific information system components such as the database, sensitive files, or production source code. Finally, the implemented audit log procedures did not address potentially suspicious or unusual transactions that could be performed in the sampled payment management system.	We recommend that FMS management: 1 Identify and document significant audit events that warrant review and further investigation. 2 Update the SSP in order to reflect the results of the risk analysis and clearly assign ownership and responsibility for implementing the agreed upon audit log review procedures. 3 Ensure that sufficient resources are available to implement audit log review procedures.	**Implemented/Closed** Management has implemented procedures for reviewing and monitoring significant audit events and audit log reports, and has updated the SSP to reflect this process.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2011 Finding #6 – FMS POA&Ms were not tracked and remediated in accordance with NIST and Department of the Treasury requirements.	FMS did not record and update security vulnerabilities in a timely manner for three sampled systems. For the sampled systems, we noted that FMS did not review and revise expected completion dates for corrective actions, record known high-risk vulnerabilities that FMS could not close in 60 days, or correctly report the completion status on outstanding POA&M items. In both the FY 2009 and FY 2010 FISMA audits at FMS, we noted similar POA&M weaknesses for different information systems. FMS took corrective actions to resolve the immediate instances of noncompliance; however, FMS did not resolve bureau wide challenges to accurately and sufficiently report all system security weaknesses in POA&Ms. A lack of System Owner and ISSO accountability, as indicated in their Appointment Letter, and communication issues between ISSO and FMS's information security group contributed to the conditions described above.	We recommend that FMS management: 1 Perform a comprehensive study of FMS's POA&M management practices to resolve ongoing auditor-identified POA&M challenges. Based on the outcome of this study, FMS should implement corrective actions designed to ensure complete, accurate and timely reporting of POA&M items. 2 Strengthen FMS's existing policies and procedures regarding POA&Ms based on the outcome of FMS's study. The revised FMS policies and procedures should define roles, responsibilities, and expected communication frequency among key participants and decision makers. 3 Promote increased involvement by FMS executives and Authorizing Officials in the POA&M management process. Such actions could include establishing performance metrics and associated incentives and/or disincentives for FMS management personnel to accurately report and resolve noted security weaknesses in their portfolio of information systems. 4 Promote personal accountability for executing information security responsibilities, such as those listed in the ISSO and System Owner Appointment Letters, by incorporating those responsibilities and expected outcomes in the employees' Annual Performance Plan.	**Implemented/Closed** Management has developed a comprehensive POA&M process and has strengthened its existing policies and procedures to define roles and responsibilities.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2011 Finding #8 – FMS Contingency planning and testing and backup controls were not fully implemented or operating as designed.	FMS did not complete a failover, and contingency plan test for two Critical Infrastructure Protection (CIP) payment management systems residing at FMS in accordance with FMS security standards and NIST SP 800-53 Rev. 3 requirements. During the nine-month period from October 1, 2010 through June 30, 2011, these two CIP systems processed 911 million payments totaling $1.93 trillion. These two systems process approximately all Social Security Administration payments, Medicare and Medicaid payments, IRS tax refunds, Veteran Affairs payments, and other United States government vendor payments. However, these two systems had only undergone a tabletop disaster recovery test during FY 2010 and FY 2011 and had not completed a full disaster recovery test at the recovery site in the prior two years. Per FMS and NIST SP 800-34 requirements, disaster recovery simulation exercises, such as tabletop exercises, are sufficient for "Moderate" systems but not "High" impact systems. FMS categorized these CIP systems as having a "High" FIPS 199 impact rating with a two-hour recovery time objective. This designation requires FMS to perform a failover, recovery and reconstitution (including communications with applications and third parties) of critical systems at an alternate site on an annual basis. FMS delayed failover contingency plan tests in FY 2011 and FY 2010 due to operational priorities to relocate and consolidate data centers.	We recommend that FMS management expedite the planned disaster recovery testing at the alternate recovery site to confirm that (a) FMS can resume mission critical functions within the stated two-hour recovery window and (b) the applications can operate successfully and communicate with other essential applications and third parties.	**Implemented/Closed** FMS and BPD consolidated into one organization, Fiscal Service, in October 2012. Fiscal Service management completed contingency plan testing for both systems in September 2012.

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 – THE DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS's FISMA 2013 QUESTIONS FOR INSPECTORS GENERAL

The information included in Appendix III represents the Department of the Treasury's (Treasury) consolidated responses to Department of Homeland Security's (DHS) FISMA 2013 questions for Inspectors General. KPMG prepared responses to DHS questions based on an assessment of 15 information systems across 12 Treasury components, excluding the IRS. KPMG determined the overall status of each DHS question based on the magnitude of the aggregated findings under each category with OIG acceptance. TIGTA performed audit procedures over the IRS information systems and provided their answers to the Treasury OIG and KPMG for consolidation. These answers are included within the table below. The information provided by TIGTA has not been subjected to KPMG audit procedures and, accordingly, we express no opinion 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? If yes, 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 800-53: CA-7).
	Yes	**1.1.2.** Documented strategy and plans for continuous monitoring (NIST 800-37 Rev 1, Appendix G).
	Yes	**1.1.3.** Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST 800-53, NIST 800-53A).
	Yes	**1.1.4.** 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 800-53, NIST 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. **Comments – TIGTA:** The IRS's annual assessments of system security controls are predominantly manual. The IRS's strategy for automating continuous monitoring includes the implementation of a tool called Archer, which will be a central repository and analysis engine for assessment results, such as automated vulnerability scans. Archer is in its initial development phases

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? If yes, 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.

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? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	No	**2.1.2.** Defined standard baseline configurations. **Comments – Treasury OIG:** Fiscal Service did not document all required aspects of baseline configuration for a selected system. TIGTA did not identify standard baseline configurations. (See Prior Year FY 2012 Finding #10 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. During FY 2013, the IRS was in the process of implementing the Security Compliance Posture Monitoring and Reporting application, which is intended to provide the ability to assess compliance with baseline security controls in a SCAP-compliant format on an enterprisewide level; however, its implementation has been delayed
	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 vulnerability scanning tools and processes on all systems to ensure timely remediation of scan result deviations. Also, the IRS processes to share vulnerability information to system owners and administrators are still under development.
	Yes	**2.1.5.** For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings fully documented.
	No	**2.1.6.** Documented proposed or actual changes to the hardware and software configurations. **Comments – TIGTA:** The IRS has not yet fully implemented configuration and change management controls to ensure that proposed or actual changes to hardware and software configurations are documented and controlled. During FY 2013, the Enterprise Services organization was in the process of implementing the Enterprise Configuration Management System to provide an enterprise solution for configuration and change management.
	No	**2.1.7.** Process for the timely and secure installation of software patches. **Comments – TIGTA:** The IRS has not yet fully implemented a process to ensure timely and secure installation of software patches. During FY 2013, the IRS was in the process of evaluating tools that have the capability to perform automated patch management activities across a multitude of technologies and feed results to a centralized location. During the FY 2013 FISMA evaluation period, TIGTA and the Government Accountability Office (GAO) identified critical patches that were missing or installed in an untimely manner on IRS computers.

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? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	No	**2.1.8.** Software assessing (scanning) capabilities are fully implemented (NIST 800-53: RA-5, SI-2). **Comments – TIGTA:** Monthly vulnerability scans are not being 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 800-53: CM-4, CM-6, RA-5, SI-2). **Comments – TIGTA:** The IRS has not yet fully implemented 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. During the FY 2013 FISMA evaluation period, TIGTA and the GAO identified servers that were not consistently configured to have strong controls.
	No	**2.1.10.** Patch management process is fully developed, as specified in organization policy or standards (NIST 800-53: CM-3, SI-2). **Comments – TIGTA:** The IRS has not yet implemented a process to ensure timely and secure installation of software patches. During FY 2013, the IRS was in the process of evaluating tools that have the capability to perform automated patch management activities across a multitude of technologies and feed results to a centralized location. During FY 2013, TIGTA and the GAO identified critical patches that were missing or installed in an untimely manner on IRS computers.
		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.

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? If yes, 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 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)

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? If yes, besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes:
	No	**3.1.2.** Identifies all users, including Federal employees, contractors, and others who access organization systems. **Comments – TIGTA:** The IRS has not fully implemented unique user identification that complies with Homeland Security Presidential Directive-12 (HSPD-12). In addition, five of our 10 sampled systems did not have the NIST SP 800-53 AC-2 security control in place.
	No	**3.1.3.** Identifies when special access requirements (e.g., multi-factor authentication) are necessary. **Comments – TIGTA:** The IRS did not fully implement 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.
	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:** Although the IRS is working to achieve its goal of 85 percent mandatory PIV use by the end of Calendar Year 2013, considerable challenges still exist for achieving full compliance due to its legacy environment.
	Yes	**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).
	No	**3.1.7.** Ensures that the users are granted access based on needs and separation-of-duties principles. **Comments – Treasury OIG:** DO, Mint and TIGTA were unable to provide evidence that users access was granted access based on needs. (See Finding #1) **Comments – TIGTA:** During FY 2013, TIGTA and the GAO identified users that had been granted more access than needed and instances where the separation-of-duties principle was not enforced.

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? If yes, besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes:
	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:** During FY 2013, the IRS was still in the process of implementing tools to achieve automated asset discovery and asset management.
	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).
	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:** During FY 2013, TIGTA and the GAO identified systems that do not have controls in place to ensure that accounts are terminated or deactivated once access is no longer needed.
	Yes	**3.1.11.** Identifies and controls use of shared accounts.
		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 was unable to provide documentation evidencing administrators account creation dates. TIGTA was unable to provide documentation evidencing users and their last login dates and times. Fiscal Service was unable to provide documentation evidencing the users' last log-on dare or time. (See 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? If yes, 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 800-53: IR-1).
	No	**4.1.2.** Comprehensive analysis, validation, and documentation of incidents. **Comments – Treasury OIG:** OIG incorrectly documented reported incidents in error. (See Finding #2)

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? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	No	**4.1.3.** When applicable, reports to US-CERT within established timeframes (NIST 800-53, 800-61; and OMB M-07-16, M-06-19). **Comments – Treasury OIG:** Fiscal Service did not report incidents within required time frames. (See Finding #2) **Comments – TIGTA:** The IRS did not always report incidents involving Personally Identifiable Information to the US-CERT within established time frames due to resource constraints.
	Yes	**4.1.4.** When applicable, reports to law enforcement within established time frames (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 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 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? If yes, 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 800-37, Revision 1. **Comments – Treasury OIG:** TIGTA did not update risk management program with NIST 800-37, Rev.1 guidance (See Prior Year FY 2011 Finding #10)

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? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	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 800-37, Rev. 1. **Comments – Treasury OIG:** TIGTA did not update risk management program with NIST 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 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.
	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:** FinCEN did not adequately document the implementation of controls as required by NIST and Treasury guidance (See Finding #3)
	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.
	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:** Fiscal Service 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).

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? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	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.

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? If yes, 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:** OIG was unable to provide evidence of successful completion of security awareness training. (See Finding #5)
	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 did not track completions of specialized information technology security training by contractors during the FY 2013 FISMA evaluation period.
	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? If yes, 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 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.
	Yes	**7.1.6.** POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25).
	Yes	**7.1.7.** Costs associated with remediating weaknesses are identified (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? If yes, 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 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:** 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. In addition, virtual private network server components do not comply with password requirements.
	Yes	**8.1.4.** Telecommuting policy is fully developed (NIST 800-46, Section 5.1).
	Yes	**8.1.5.** If applicable, multifactor authentication is required for remote access (NIST 800-46, Section 2.2, 3.3).

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? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	Yes	**8.1.6.** Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.
	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 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? If yes, 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 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:** 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 #4 and Prior Year FY 2011 Finding #8)
	No	**9.1.4.** Testing of system-specific contingency plans. **Comments – Treasury OIG:** TIGTA did not perform contingency plan testing for the selected system. (See Finding #4)

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? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	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 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:** TIGTA did not perform contingency plan testing for the selected system. (See 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:** TIGTA did not perform contingency plan testing for the selected system. (See Finding #4)
	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? If yes, 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.

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? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes:
	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.
	Yes	**10.1.4.** The inventory identifies interfaces between these systems and organization-operated systems (NIST 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.
		10.2. 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? If yes, 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 800-53: SA-2).
	Yes	**11.1.4.** Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST 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) 2013, 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 the Treasury 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, 2013.
- 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 in the subset would not exceed the percentage of systems they represent in the Treasury inventory of information 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 the Treasury inventory of information systems as of May 16, 2013, we noted a total of 188 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 the 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	135	2	50	36	47
General Support Systems	53	0	23	2	28
Total	188	2	72	38	75

From the analysis above, it was determined that IRS systems make up 40% of the total population of Major Applications and General Support systems and Non-IRS systems make up 60%. When the IRS to Non-IRS weighting is applied to subset size of 25 from the total population, the resulting sizes for the IRS and Non-IRS subsets are 10 and 15, respectively.

We determined that Major Applications account for 73% of the population of the Non-IRS population and General Support Systems account for 27%. We further determined that systems designated as "Financial" and "Mixed Financial" in TAF account for 34% of all Non-IRS Major Applications and General Support Systems. Lastly, we determined that 33% of the Non-IRS Major Applications and General Support Systems are assigned a FIPS 199 System Impact Level of "High," while 67% 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"	3
Total Systems with a FIPS 199 System Impact Level of "Moderate"	12
Total Systems with a FIPS 199 System Impact Level of "Low"	0
Total Systems Designated as Financial	3

(**Note:** During the evaluation, one of the high financial systems was determined to be retiring in early FY 2014, so a moderate non-financial system was used to replace it.)

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 113 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	52	44%	5
CDFI Fund	2	2%	0 (See Note 1)
DO	24	20%	3
FinCEN	7	6%	1
Mint	9	8%	1
OCC	7	6%	1
OIG	1	1%	1 (See Note 2)
TIGTA	2	2%	1 (See Note 2)
TTB	3	3%	1 (See Note 2)
Total	113	100%	15

(**Note 1:** Per instructions from the OIG, we did not sample any systems from CDFI Fund, because their systems had been selected in the past 2 years.)

(**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
The Act	Title III of the E-government Act of 2002
ACIOCS	Associate Chief Information Officer for Cyber Security
AU	Audit and Accountability
BCP	Business Continuity Planning
BEP	Bureau of Engraving and Printing
BIA	Business Impact Analysis
BLSR	Fiscal Service Baseline Services Requirements
Bureaus	Bureaus/Offices
BPD	Bureau of the Public Debt
CA	Security Assessment and Authorization
CAT	Category
C&A	Certification and Accreditation
CDFI Fund	Community Development Financial Institutions Fund
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
CP	Contingency Planning
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	Bureau of the Fiscal Service
FISMA	Federal Information Security Management Act
FMS	Financial Management Service
FY	Fiscal Year
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
IG	Inspector General
IP	Internet Protocol
IR	Incident Response & Reporting

Acronym	Definition
IRS	Internal Revenue Service
ISSO	Information System Security Officer
IT	Information Technology
KPMG	KPMG LLP
Mint	United States Mint
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OTS	Office of Thrift Supervision
PIV	Personal Identity Verification
PL	Planning
POA&M	Plan of Action and Milestones
PL	Planning
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
Rev.	Revision
SC	System & Communications Protection
SI	System and Information Integrity
SIGTARP	Special Inspector General for the Troubled Asset Relief Program
SA	System and Services Acquisition
SOP	Standard Operating Procedure
SP	Special Publication
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
UPS	United Parcel Service
US-CERT	United States Computer Emergency Readiness Team
USGCB	United Stated Government Configuration Baseline

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 2

Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2013, (Reference No. 2013-20-128), September 27, 2013

THIS PAGE INTENTIONALLY LEFT BLANK

Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2013

September 27, 2013

Reference Number: 2013-20-128

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 2013

Highlights

Issued on September 27, 2013

Highlights of Reference Number: 2013-20-128 to the Department of the Treasury, Office of the Inspector General, Assistant Inspector General for Audit.

IMPACT ON TAXPAYERS

The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. The Federal Information Security Management Act (FISMA) was enacted to strengthen the security of information and systems within Federal Government agencies. Until the IRS takes steps to fully implement all 11 security program areas covered by FISMA, taxpayer data will remain vulnerable to inappropriate use, modification, or disclosure, possibly without being detected.

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's information security program for Fiscal Year (FY) 2013.

WHAT TIGTA FOUND

Based on our FY 2013 FISMA evaluation, TIGTA found that nine of 11 security program areas were generally compliant with the FISMA requirements. Six of the nine security program areas included all of the program attributes specified by the Department of Homeland Security's (DHS) *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*:

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

Three of the nine security program areas, while generally compliant, were not fully effective due to one program attribute that was missing or not working as intended:

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

However, two of the 11 security program areas were not compliant with FISMA requirements and did not meet the level of performance specified by the DHS's *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics* due to the majority of the DHS-specified attributes being missing or not working as intended:

- Configuration Management.
- Identity and Access Management.

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 DHS for the applicable FISMA evaluation period.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 27, 2013

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDIT
OFFICE OF THE INSPECTOR GENERAL
DEPARTMENT OF THE TREASURY

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2013 (Audit # 201320001)

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 2013. The Act requires the agency's Inspector General to perform an annual independent evaluation of the agency's information security program and practices to determine the effectiveness of such program and practices.

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 Alan R. Duncan, 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
CM	Continuous Monitoring
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
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 Internal Revenue Service (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. Otherwise, taxpayers could be exposed to invasion of privacy and financial loss or damage from identity theft or other financial crimes.

The Federal Information Security Management Act (FISMA) of 2002[1] was enacted to strengthen the security of information and systems within Federal agencies. Under the FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of the FISMA, related Office of Management and Budget (OMB) policies, and National Institute of Standards and Technology (NIST) procedures, standards, and guidelines.

One of the provisions of the FISMA requires the agencies to have an annual independent evaluation of their information security programs and practices performed by the agency Inspector General or an independent external auditor as determined by the Inspector General.[2] The OMB uses the information from the agencies and independent evaluations in its FISMA oversight capacity to assess agency-specific and Federal Governmentwide security performance, develop its annual security report to Congress, and assist in improving and maintaining adequate agency security performance.

In July 2010, the OMB delegated its responsibility to the Department of Homeland Security (DHS) for the collection of annual FISMA responses.[3] The DHS issued the *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics* on November 30, 2012, for Fiscal Year[4] (FY) 2013 FISMA responses. These reporting metrics specified the security program areas for the Inspectors General to evaluate and listed specific attributes that each security program area should include. Detailed information on our audit

[1] Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.
[2] The FISMA evaluation period for the Department of the Treasury is July 1, 2012, through June 30, 2013.
[3] In OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*, OMB delegated the responsibility for various operational aspects of Federal cyber security to the DHS, including overseeing the agencies' compliance with the FISMA and developing analyses for the OMB to assist in the development of the FISMA annual report.
[4] A 12-consecutive-month period ending on the last day of any month. The Federal Government's fiscal year begins on October 1 and ends on September 30.

objective, scope, and methodology is presented in Appendix I. Major contributors to this 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

The DHS *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics* that were issued on November 30, 2012, specified 11 information security program areas and a total of 98 attributes within the 11 areas for the Inspectors General to evaluate and determine compliance with FISMA requirements. The 11 information security program areas are as follows:

- Continuous Monitoring Management.
- Configuration Management.
- Identity and Access Management.
- Incident Response and Reporting.
- Risk Management.
- Security Training.
- Plan of Action and Milestones (POA&M).
- Remote Access Management.
- Contingency Planning.
- Contractor Systems.
- Security Capital Planning.

To complete our FISMA evaluation, we reviewed a representative judgmental sample[5] of 10 major IRS information systems. For each system in the sample, we assessed the risk management process, the annual testing of controls for continuous monitoring, the testing of information technology contingency plans, and the plan of action and milestones process. In addition, we evaluated the IRS's enterprise-level processes over configuration management, identity and access management, incident response and reporting, security training, remote access management, contractor systems, and security capital planning. During the FY 2013 FISMA evaluation period, we also completed seven audits, as shown in Appendix IV, which evaluated various aspects of information security at the IRS. We considered the results of these

[5] A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.

audits in our evaluation, as well as results from ongoing audits for which draft reports were issued to the IRS by August 8, 2013.

Based on our FY 2013 FISMA evaluation, we determined that nine of the 11 security program areas were generally compliant with the FISMA requirements. The following six security program areas included all of the program attributes specified by the DHS's *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*:

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

The following three security program areas, while generally compliant, were not fully effective due to one program attribute that was missing or not working as intended:

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

However, two security program areas were not compliant with FISMA requirements and did not meet the level of performance specified by the DHS's *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics* due to the majority of the DHS-specified attributes being missing or not working as intended:

- Configuration Management.
- Identity and Access Management

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

The following matrix[6] presents TIGTA's results for the 11 security program areas as specified by the DHS's *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*. We have provided comments to support the "no" responses. TIGTA's results will be

[6] Many abbreviations in this matrix are used as presented in the original document and are not defined therein. However, we have provided the definitions in the Abbreviations page after the Table of Contents of this report.

consolidated with the Department of the Treasury Office of Inspector General's results of non-IRS bureaus and reported to the OMB.

1: Continuous Monitoring

Status of Continuous Monitoring Program [check one: Yes or No]	Yes	**1.1.** Has the organization established an enterprisewide 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 and plans for continuous monitoring (NIST SP 800-37 Rev 1, Appendix G).
	Yes	**1.1.3.** 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 800-53A).
	Yes	**1.1.4.** 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. TIGTA Comments: The IRS's annual assessments of system security controls are predominantly manual. The IRS's strategy for automating continuous monitoring includes the implementation of a tool called Archer, which will be a central repository and analysis engine for assessment results, such as automated vulnerability scans. Archer is in its initial development phases.

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. During FY 2013, the IRS was in the process of implementing the Security Compliance Posture Monitoring and Reporting application, which is intended to provide the ability to assess compliance with baseline security controls in a SCAP-compliant format on an enterprisewide level; however, its implementation has been delayed.
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 vulnerability scanning tools and processes on all systems to ensure timely remediation of scan result deviations. Also, the IRS processes to share vulnerability information to system owners and administrators are still under development.
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. During FY 2013, the Enterprise Services organization was in the process of implementing the Enterprise Configuration Management System to provide an enterprise solution for configuration and change management.
No	**2.1.7.** Process for the timely and secure installation of software patches. TIGTA Comments: The IRS has not yet fully implemented a process to ensure timely and secure installation of software patches. During FY 2013, the IRS was in the process of evaluating tools that have the capability to perform automated patch management activities across a multitude of technologies and feed results to a centralized location. During the FY 2013 FISMA evaluation period, TIGTA and the Government Accountability Office (GAO) identified critical patches that were missing or installed in an untimely manner on IRS computers.
No	**2.1.8.** Software assessing (scanning) capabilities are fully implemented. (NIST SP 800-53: RA-5, SI-2) TIGTA Comments: Monthly vulnerability scans are not being 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 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. During the FY 2013 FISMA evaluation period, TIGTA and the GAO identified servers that were not consistently configured to have strong controls.
	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 yet implemented a process to ensure timely and secure installation of software patches. During FY 2013, the IRS was in the process of evaluating tools that have the capability to perform automated patch management activities across a multitude of technologies and feed results to a centralized location. During FY 2013, TIGTA and the GAO identified critical patches that were missing or installed in an untimely manner on IRS computers.
		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.

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 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: The IRS has not fully implemented unique user identification that complies with Homeland Security Presidential Directive-12 (HSPD-12). In addition, five of our 10 sampled systems did not have the NIST SP 800-53 AC-2 security control in place.
	No	**3.1.3.** Identifies when special access requirements (*e.g.*, multifactor authentication) are necessary. TIGTA Comments: The IRS did not fully implement 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: Although the IRS is working to achieve its goal of 85 percent mandatory PIV use by the end of Calendar Year 2013, considerable challenges still exist for achieving full compliance due to its legacy environment.
Yes	**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)
No	**3.1.7.** Ensures that the users are granted access based on needs and separation-of-duties principles. TIGTA Comments: During FY 2013, TIGTA and 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. (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: During FY 2013, the IRS was still in the process of implementing tools to achieve automated asset discovery and asset management.
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.)
No	**3.1.10.** Ensures that accounts are terminated or deactivated once access is no longer required. TIGTA Comments: During FY 2013, TIGTA and the GAO identified systems that do not have controls in place to ensure that accounts are terminated or deactivated once access is no longer needed.
Yes	**3.1.11.** Identifies and controls use of shared accounts.

		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 due to resource constraints.
	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 organizationwide 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 at 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.

6: Security Training

Status of Security Training Program [check one: Yes or No]	Yes	**6.1** Has the organization established a security training 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	**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 did not track completions of specialized information technology security training by contractors during the FY 2013 FISMA evaluation period.
	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.
	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: 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. In addition, virtual private network server components do not comply with password requirements.
	Yes	**8.1.4.** Telecommuting policy is fully developed. (NIST SP 800-46, Section 5.1)
	Yes	**8.1.5.** If applicable, multifactor authentication is required for remote access. (NIST SP 800-46, Section 2.2, Section 3.3)
	Yes	**8.1.6.** Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.
	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 re-authentication 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 enterprisewide 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 exercises 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 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 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 2013, the IRS maintained two contractor managed systems in the Trusted Agent FISMA, the U.S. Department of the Treasury's system for reporting FISMA data. The IRS also maintained a list of 130 contractor sites in FY 2013 that required annual security reviews because each handles or processes IRS information. The IRS Infrastructure and Security Review organization conducts reviews to ensure that security controls and standards are met and issues reports of findings to these contractors.
	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) 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 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 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 that was not noted in the questions above.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to provide an annual independent evaluation of the effectiveness of the IRS's information technology security program and practices, and to assess the progress made by the IRS in meeting the responsibilities established by the NIST and the OMB. The following 11 evaluative sections are taken directly from the DHS *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*, issued on November 30, 2012.

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.

To accomplish our objective, we reviewed a judgmental sample[1] of 10 major IRS information systems from a total of 75 major applications maintained in the Trusted Agent FISMA system as of April 11, 2013. We selected a judgmental sample because we did not plan to project the results. We conducted tests to determine the appropriate level of performance that the IRS has achieved for each of the security program areas. We also evaluated completed TIGTA work during the FISMA period, as well as audits from the GAO, and determined its applicability to the FISMA questions.

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 2013 Inspector General Federal Information Security Management Act Reporting Metrics*. The Department of the Treasury Office of Inspector General will combine

[1] A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.

our results for the IRS with its results for the non-IRS bureaus and submit the combined yes or no responses to OMB.

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
Charles Ekunwe, Senior Auditor
Bret Hunter, Senior Auditor
Mary Jankowski, Senior Auditor
Esther Wilson, Senior Auditor
Tina Wong, Senior Auditor

Appendix III

Report Distribution List

Principal Deputy Commissioner
Office of the Commissioner – Attn: Chief of Staff C
Office of the Deputy Commissioner for Services and Enforcement SE
Deputy Commissioner for Operations Support OS
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 Liaison: Director, Risk Management Division OS:CTO:SP:RM

Appendix IV

Treasury Inspector General for Tax Administration Information Technology Security-Related Reports Issued During the Fiscal Year 2013 Evaluation Period

1. TIGTA, Ref. No. 2012-20-099, *Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data* (Sept. 2012).
2. TIGTA, Ref. No. 2012-20-112, *An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers* (Sept. 2012).
3. TIGTA, Ref. No. 2012-20-109, *The Customer Account Data Engine 2 Database Was Initialized; However, Database and Security Risks Remain, and Initial Timeframes to Provide Data to Three Downstream Systems May Not Be Met* (Sept. 2012).
4. TIGTA, Ref. No. 2012-20-115, *Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected* (Sept. 2012).
5. TIGTA, Ref. No. 2013-20-016, *Significant Delays Hindered Efforts to Provide Continuous Monitoring of Security Settings on Computer Workstations* (Jan. 2013).
6. TIGTA, Ref. No. 2013-20-023, *Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process* (Feb. 2013).
7. TIGTA, Ref. No. 2013-20-030, *Integrated Financial System Updates Are Improving System Security, but Remaining Weaknesses Should Be Addressed* (Mar. 2013).