Audit Report

OIG-17-003

INFORMATION TECHNOLOGY: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2016 Performance Audit

November 9, 2016

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 9, 2016

MEMORANDUM FOR KODY KINSLEY
ASSISTANT SECRETARY FOR MANAGEMENT

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

FROM: Larissa Klimpel /s/
Acting Director, Cyber/Information Technology Audits

SUBJECT: Audit Report – *Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2016 Performance Audit*

We are pleased to transmit the following reports:

- *Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2016 Performance Audit*, dated November 7, 2016, (Attachment 1); and

- *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2016*, dated September 28, 2016 (Attachment 2).

The Federal Information Security Modernization Act of 2014 (FISMA) requires that Federal agencies have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices, and to report the results to the Office of Management and Budget (OMB). OMB delegated its responsibility to the Department of Homeland Security (DHS) for the collection of annual FISMA responses. FISMA also requires that the agency Inspector General (IG) or an independent external auditor perform the annual evaluation as determined by the IG.

To meet our FISMA requirements, we contracted with KPMG LLP (KPMG), an independent certified public accounting firm, to perform this year's annual FISMA audit of Treasury's unclassified systems, except for those of the Internal Revenue Service (IRS), which were evaluated by the Treasury Inspector General for Tax

Administration (TIGTA). Appendix III of the attached KPMG report includes *The Department of the Treasury's Consolidated Response to DHS's FISMA 2016 Questions for Inspectors General*. KPMG conducted its audit in accordance with generally accepted government auditing standards. In connection with our contract with KPMG, we reviewed its report and related documentation and inquired of its representatives.

In brief, KPMG reported that, consistent with applicable FISMA requirements, OMB policy and guidance, and the National Institute of Standards and Technology (NIST) standards and guidelines, Treasury's information security program and practices for its unclassified systems were established and have been maintained for the five Cybersecurity Functions and the eight FISMA program areas. However, KPMG identified six deficiencies within three of the Cybersecurity Functions and four of the FISMA program areas. Accordingly, KPMG made 44 recommendations to the responsible officials to address the identified deficiencies.

With respect to IRS's unclassified systems, TIGTA reported that IRS's information security program generally aligned with applicable FISMA requirements, OMB policy and guidance, and the NIST standards and guidelines. However, due to program attributes not yet implemented, IRS's information security program was not fully effective. TIGTA found that three security program areas failed to meet FISMA requirements overall.

If you have any questions or require further information, you may contact me at (202) 927-0361.

Attachments

cc: Jack Donnelly
Associate Chief Information Officer,
Cyber Security

ATTACHMENT 1

Department of the Treasury
Federal Information Security Modernization Act
Fiscal Year 2016 Performance Audit
November 9, 2016

THIS PAGE INTENTIONALLY LEFT BLANK

Department of the Treasury
Federal Information Security Modernization Act
Fiscal Year 2016 Performance Audit

November 7, 2016

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

Department of the Treasury
Federal Information Security Modernization Act Fiscal Year 2016 Performance Audit

Table of Contents

FISMA Performance Audit Report

Appendices

KPMG LLP
1676 International Drive
McLean, VA 22102

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

Re: Department of the Treasury's Federal Information Security Modernization Act Fiscal Year 2016 Performance Audit

Dear Mr. Thorson:

This report presents the results of our independent performance audit of the Department of the Treasury's (Treasury) information security program and practices for its unclassified systems. The Federal Information Security Modernization Act of 2014 (FISMA) requires Federal agencies, including the Treasury, to have an annual independent evaluation performed of their information security programs and practices to determine effectiveness of such programs and practices, and to report the results of the evaluations to the Office of Management and Budget (OMB). The Department of Homeland Security (DHS) is responsible for the operational aspects of Federal cyber security, such as establishing government-wide incident response and operating CyberScope to collect FISMA metrics. Appendix III, *Department of the Treasury's Consolidated Response to DHS' FISMA 2016 Questions for Inspectors General*, dated July 29, 2016 provides Treasury's response to the CyberScope questionnaire. We also considered applicable OMB policy and guidelines and the National Institute of Standards and Technology (NIST) standards and guidelines. FISMA requires that the agency Inspector General (IG) or an independent external auditor perform the annual evaluation as determined by the IG. The Treasury Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct an audit of Treasury's information security program and practices for its unclassified systems.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives for this audit were to assess the effectiveness of the Treasury's information security programs and practices; respond to DHS FISMA Questions on behalf of the Treasury OIG; and assess the implementation for a sample of security controls from NIST Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organization,* for 15 non-national security systems; and follow up on the status of prior-year FISMA findings. The assessment period was from July 1, 2015 to June 30, 2016. Additional details regarding the scope of our independent audit are included in Appendix I, *Objectives, Scope and Methodology*. The scope of our work did not include the Internal Revenue Service (IRS), as that bureau was evaluated by the Treasury Inspector General for Tax Administration (TIGTA). The TIGTA report is appended to this report and the findings

are included in Appendix III, *Department of the Treasury's Consolidated Response to DHS's FISMA 2016 Questions for Inspectors General*. Additional details regarding the scope of our independent performance audit are included in Appendix I, *Objectives, Scope, and Methodology*. Appendix II, *Status of Prior-Year Findings*, summarizes Treasury's progress in addressing prior-year recommendations. Appendix IV, *Approach to Selection of Subset of Systems*, describes how we selected systems for review. Appendix V contains a glossary of terms used in this report.

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, Treasury established and maintained its information security program and practices for its unclassified systems for the 5 Cybersecurity Functions[1] and 8 FISMA program areas[2]. However, the program was not fully effective as reflected in the 6 deficiencies within 3 of the 5 Cybersecurity Functions and within 4 of the 8 FISMA program areas that we identified during fieldwork as follows:

Cybersecurity Function: Identify:

1. Risk management activities were not compliant with policies at Community Development Financial Institutions (CDFI) Fund, OIG, and Departmental Offices (DO). (Risk Management)
2. Plan of Action and Milestones (POA&Ms) were not tracked in accordance with NIST and Treasury requirements at DO and Bureau of the Fiscal Service (Fiscal Service). (Risk Management)

Cybersecurity Function: Protect:

3. Configuration management plan was incomplete and missing key information regarding system baseline configurations at Fiscal Service. (Configuration Management)
4. Vulnerability scans were not being conducted in accordance with Treasury Directive Publication (TD P) 85-01 policies at Bureau of Engraving and Printing (BEP) and DO. (Configuration Management)
5. Account management activities were not compliant with policies at CDFI Fund, Alcohol and Tobacco Tax and Trade Bureau (TTB), OIG, DO, Fiscal Service and United States Mint (Mint). (Identity and Access Management)

Cybersecurity Function: Recover:

6. Contingency planning activities were not compliant with policies at DO, Mint, Financial Crimes Enforcement Network (FinCEN) and OIG. (Contingency Planning)

We made 44 recommendations related to these control deficiencies that, if effectively addressed by management, should strengthen the respective bureaus', offices', and Treasury's information security programs. In a written response, the Treasury Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO) agreed with our findings and recommendations (see *Management Response below).* Treasury's planned corrective actions are responsive to the intent of our

[1] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the FY 2016 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers (CIO) Council. In FY 2016 the eight IG FISMA Metric Domains were aligned with the five functions of identify, protect, detect, response, and recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

[2] As described in the DHS' *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.1.3*, the 8 FISMA Metric Domains are: risk management, contractor systems, configuration management, identity and access management, security and privacy training, information security continuous monitoring, incident response, and contingency planning.

recommendations. We will follow up on the status of all corrective actions as part of the FY 2017 independent evaluation.

During our audit, we noted some bureaus and offices self-identified weaknesses in NIST SP 800-53 Rev. 4 controls and documented them in 41 POA&Ms. We reviewed each self-identified weakness and noted that each weaknesses had a corrective action plan documented within a POA&M, and therefore, did not provide any additional recommendations (see *Self-identified Weaknesses*).

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

Sincerely,

KPMG LLP

November 7, 2016

BACKGROUND

Federal Information Security Modernization Act of 2014 (FISMA)

Federal Information Security Modernization Act of 2014, commonly referred to as FISMA, focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires Federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The act assigns specific responsibilities to agency heads and Inspector Generals (IGs) in complying with requirements of FISMA. The act is supported by the Office of Management and Budget (OMB), Department of Homeland Security (DHS), agency security policy, and risk-based standards and guidelines published by National Institute of Standards and Technology (NIST) related to information security practices.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of FISMA and related OMB policies and NIST procedures, standards, and guidelines. FISMA directs Federal agencies to report annually to the OMB Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. DHS is responsible for the operational aspects of Federal cyber security, such as establishing government-wide incident response and operating the tool to collect FISMA metrics. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG.

FY 2016 Inspector General FISMA Reporting Metrics

OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the FY 2016 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Office (CIO) Council. In FY 2016 the eight IG FISMA Metric Domains were aligned with the five NIST *Framework for Improving Critical Infrastructure Cybersecurity* functions:

Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FY 2016 IG FISMA Metric Domains

Cybersecurity Functions	FY 2016 IG FISMA Metric Domains
Identify	Risk Management Contractor Systems
Protect	Configuration Management Identity and Access Management Security and Privacy Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Last year, CIGIE, in coordination with OMB, DHS, NIST and other key stakeholders, introduced a maturity model for information security continuous monitoring, and this year, introduced a maturity model for incident response. According to the FY 2016 IG FISMA Reporting Metrics, the purpose of the CIGIE maturity models was to:

1) summarize the status of agencies' information security programs and their maturity on a 5-level scale;
2) provide transparency to agency CIOs, top management officials, and other interested readers of IG FISMA reports regarding what has been accomplished and what still needs to be implemented to improve the information security program; and
3) help ensure consistency across the IGs in their annual FISMA evaluations.

Furthermore, the FY 2016 IG FISMA Reporting Metrics outlined what was considered to be an "effective" FISMA program:

> Due to the different models being used in the FY 2016 IG FISMA assessment, questions are distributed differently based on whether the function area utilizes a full maturity model (Detect and Respond) or maturity model indicators (Identify, Protect, and Recover). For those function areas that utilize a full maturity model, there are questions associated with each level. For those function areas that rely on maturity model indicators, however, the scoring distribution focuses on the *Defined*, *Consistently Implemented*, and *Managed and Measurable* maturity levels. Agencies with programs that score at or above the *Managed and Measureable* for a NIST Framework Function have "effective" programs within that area in accordance with the effectiveness definition in NIST SP 800-53, Rev. 4, discussed above.

The introduction of 5-level scale is a deviation from previous DHS guidance over the CyberScope questions. As such, a year-on-year comparison of FISMA compliance is not possible due to the fundamental change in how CyberScope is scored and evaluated.

Department of the Treasury Bureaus/Offices (Bureaus)

The Department of the Treasury (Treasury) 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 consolidation of the legacy Bureau of the Public Debt (BPD), which 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. IT systems in support of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) are handled by DO.

6 **Financial Crimes Enforcement Network (FinCEN)** – Supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes. It also provides United States policy makers with strategic analyses of domestic and worldwide trends and patterns.

7 **Internal Revenue Service (IRS)** – Responsible for determining, assessing, and collecting internal revenue in the United States.

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

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

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

11 **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 2016 FISMA audit did not include the IRS, which was evaluated by TIGTA. The TIGTA report is appended to this report and the findings of that report are included in Appendix III, *Department of the Treasury's Consolidated Response to DHS's FISMA 2016 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 Office of the Chief Information Officer (OCIO) Cyber Security Program develops and implements IT security policies and provides policy compliance oversight for both unclassified and classified systems managed by each of Treasury's bureaus. The OCIO Cyber Security Program's mission focuses on the following areas:

1. **Cyber Security Policy** – Manages and coordinates Treasury's cyber security policy for sensitive (unclassified) systems throughout Treasury, assuring these policies and requirements are updated to address today's threat environment, and conducts program performance, progress monitoring, and analysis.
2. **Performance Monitoring and Reporting** – Implements collection of Federal and Treasury-specific security measures and reports those to national authorities and in appropriate summary or dashboard form to senior management, IT managers, security officials, and bureau officials. For example, this includes preparation and submission of the annual FISMA report and more frequent continuous monitoring information through CyberScope.
3. **Cyber Security Reviews** – Conducts technical and program reviews to help strengthen the overall cyber security posture of the Treasury and meet their oversight responsibilities.
4. **Enterprise-wide Security** – Works with Treasury's Government Security Operations Center to deploy new Treasury-wide capabilities or integrate those already in place, as appropriate, to strengthen the overall protection of the Treasury.
5. **Understanding Security Risks and Opportunities from New Technologies** – Analyzes new information and security technologies to determine risks (e.g., introduction of new vulnerabilities) and opportunities (e.g., new means to provide secure and original functionality for users). OCIO seeks to understand these technologies, their associated risks and opportunities, and share and use that information to Treasury's advantage.
6. **Treasury Computer Security Incident Response Capability (TCSIRC)** – Provides incident reporting with external reporting entities and conducts performance monitoring and analyses of the Computer Security Incident Response Center (CSIRC) within Treasury and each bureau's CSIRC.
7. **National Security Systems** – Manages and coordinates the Treasury-wide program to address the cyber security requirements of national security systems through the development of policy and program or technical security performance reviews.
8. **Cyber Security Sub-Council (CSS) of the CIO Council** – Operates to serve as the formal means for gaining bureau input and advice as new policies are developed, enterprise-wide activities are considered, and performance measures are developed and implemented; provides a structured means for information-sharing among the bureaus.

The Treasury CIO has tasked the Associate Chief Information Officer for Cyber Security (ACIOCS) with the responsibility of managing and directing the OCIO's Cyber Security program, as well as ensuring compliance with statutes, regulations, policies, and guidance. In this regard, Treasury Directive Publication (TD P) 85-01 Volume I, *Treasury Information Technology Security Program*, serves as the Treasury IT security policy to provide for information security for all information and information systems that support the mission of the Treasury, including those operated by another Federal agency or contractor on behalf of the Treasury. In addition, as OMB periodically releases updates/clarifications of FISMA or as NIST releases updates to publications, the ACIOCS and the Cyber Security Program have responsibility to interpret and release updated policy for the Treasury. The ACIOCS and the Cyber Security Program are also responsible for promoting and coordinating a Treasury IT security program, as well as monitoring and evaluating the status of Treasury's IT security posture and compliance with statutes, regulations, policies, and guidance. Lastly, the ACIOCS has the responsibility of managing Treasury's IT Critical Infrastructure Protection (CIP) program for Treasury IT assets.

Bureau CIOs

Organizationally, Treasury has established Treasury CIO and bureau-level CIOs. The CIOs are responsible for managing the IT security program for their respective bureau, as well as advising the bureau head on significant issues related to the bureau IT security program. The CIOs also have the responsibility for overseeing the development of procedures that comply with the Treasury OCIO's policy

and guidance and federal statutes, regulations, policy, and guidance. The bureau Chief Information Security Officers (CISO) are tasked by their respective CIOs to serve as the central point of contact for the bureau's IT security program, as well as to develop and oversee the bureau's IT security program. This includes the development of policies, procedures, and guidance required to implement and monitor the bureau IT security program.

Department of the Treasury – Bureau OCIO Collaboration

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

OVERALL AUDIT RESULTS

Consistent with applicable FISMA requirements, OMB policy and guidance, and the National Institute of Standards and Technology (NIST) standards and guidelines, the Treasury's information security program and practices for its unclassified systems were established and have been maintained for the 5 Cybersecurity functions and 8 FISMA program areas. The FISMA program areas are outlined in the *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.1.3* and were prepared by DHS' Office of Cybersecurity and Communications Federal Network Resilience. The 8 program areas are risk management, contractor systems, configuration management, identity and access management, security and privacy training, information security continuous monitoring, incident response, and contingency planning.[3] However, while the security program has been implemented across the Treasury for its non-IRS bureaus, the program was not fully effective as reflected in 6 findings within 4 of the 8 FISMA program areas.

We have made 44 recommendations that, if effectively addressed by management, should strengthen the respective bureau's, office's, and Treasury's information security programs. The *Findings* section of this report presents the detailed findings and associated recommendations. We noted 40 self-identified control weaknesses by 5 bureaus, which are in the *Self-Identified Weakness* section of the report. We will follow up on the status of all corrective actions as part of the FY 2017 independent evaluation.

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

In a written response to this report the Treasury CIO agreed with our findings and recommendations (See *Management Response)*

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

FINDINGS

1. Risk management activities were not compliant with policies at CDFI Fund, OIG, and DO.

TD P 85-01 Volume I requires Treasury bureaus to upload required artifacts into the Department's FISMA inventory management, reporting and tracking tool as the documents are completed. Additionally, TD P 85-01 Volume I requires bureaus to develop security plans for the information system that is consistent with the organization's enterprise structure and that is updated to address changes to the information system/environment of operation. Further, bureaus are required to conduct, document and update the risk assessment on a bureau defined frequency or whenever there are significant changes to the information system. This control falls under the identify Cybersecurity domain and the risk management FISMA program area. We noted the following:

- For the selected system, CDFI Fund management did not upload required documentation in the Department of Treasury's centralized FISMA inventory management tool. Management indicated that required documentation was not uploaded due to a lack of oversight and competing priorities. Additionally, CDFI Fund management did not fully document the controls that are shared responsibilities between CDFI Fund and TTB. For the controls where responsibility is shared, the system security plan (SSP) simply states to inspect the TTB and Cloud Provider SSPs. (*See recommendations #1 and #2.*)
- For the selected system, OIG management did not ensure that the SSP completely addressed NIST SP 800-53, Rev. 4, controls and control enhancements. Specifically, OIG management did not completely document the control requirement for 73 controls and control enhancements within the SSP, did not include 6 controls within the SSP, and did not consistently document within the SSP the selected system's control environment. Additionally, OIG management did not perform or document a formal risk assessment for the system since April 2013. Also, the accompanying system security control assessment did not include all NIST SP 800-53, Rev. 4, controls and control enhancements required for a Moderate system. OIG management indicated that the SSP was restructured during the recent Security Assessment and Authorization (SA&A) process and due to lack of oversight, management did not document controls and control enhancements appropriately. Finally, the risk assessment for the system was informally postponed due to the system recently moving to a new location. (*See recommendations #3, #4, #5, #6, and #7.*)
- For one of the selected systems, DO management did not document all of the NIST SP 800-53, Rev. 4, moderate controls and control enhancements in the SSP. DO policy requires management to use an approved template. Instead, DO management separately documented its security controls in the system Security Controls Requirements Compliance Matrix (SRCM). We noted that a selection of 12 controls and control enhancements in the SRCM were inadequately or inappropriately documented. For the second selected system, DO management did not update the SSP during the FISMA period, resulting in an SSP that does not reflect the implementation status of its controls or the current state of the system. DO management indicated that it transferred the control descriptions out of the SSP and into the SRCM in an attempt to centralize the controls after the most recent annual test. Due to human error, management did not adequately address control and control enhancement information in the SRCM. Additionally, due to lack of oversight, management did not conduct its review of the SSP to validate it included and adequately documented the NIST SP 800-53, Rev. 4, controls in the SSP and did not formally approve the plan. (*For the first system, see recommendations #8 and #9. For the second system, see recommendations #10, #11, and #12.*)

Failing to document a current baseline of security controls in the SSP may have a negative effect on subsequent security activities. Specifically, the bureaus and offices may not be able to implement, assess, authorize, and monitor the required NIST SP 800-53, Rev. 4, controls properly for the selected systems; therefore, the system security controls may not be sufficient to protect the confidentiality, integrity, and availability of sensitive bureau information. Additionally, by not uploading the required artifacts into the Department's FISMA inventory management tool, the OCIO has limited visibility into the security status of the system. Further, without a current risk assessment, bureaus may not be aware of potential security risks posed by the use of the system.

We recommend CDFI Fund management:

1. For the selected system, implement a process or mechanism to ensure all required documentation (e.g., SSP, Contingency Plan, Risk Assessments, etc.) is uploaded into the Department's FISMA inventory management tool on the frequency stipulated in TD P 85-01.

2. For the selected system, update the SSP to include CDFI Fund's control implementation.

We recommend OIG management:

3. For the selected system, ensure all controls/control enhancement sections and statuses that indicate the control implementation are fully documented in the SSP as required by NIST SP 800-53, Rev. 4.

4. For the selected system, conduct and document a formal risk assessment for the system in accordance with TD P 85-01.

5. For the selected system, develop a security assessment plan that describes the scope of the assessment to include, security controls and control enhancements, assessment procedures to be used to determine security control effectiveness and the assessment environment.

6. For the selected system, conduct a security control assessment based upon the security assessment plan.

7. For the selected system, document the results of the assessment in a security assessment report.

We recommend DO management:

8. For the first selected system, align the system documentation of minimum control requirements with the DO SSP template requirements.

9. For the first selected system, review the control implementation documentation to ensure that the NIST 800-53, Rev. 4, controls and control enhancements are fully documented in the SSP.

10. For the second selected system, ensure that the system's current SSP is being reviewed and updated according to NIST SP 800-53, Rev. 4, guidance.

11. For the second selected system, ensure descriptions of controls in place are reflective of inherited controls by the service provider.

12. For the second selected system, ensure implementation statuses are being updated to reflect the system more accurately.

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

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

- DO management did not regularly update and monitor progress towards remediating existing POA&Ms and did not close POA&Ms by the established milestones documented. For the first system, DO management had a total of 17 system POA&Ms that were past due and were not updated nor provided a justification of why they had not been closed during the FISMA reporting period of July 1, 2015 through June 30, 2016. For the second system, management had a total of 15 POA&Ms that were past due and did not update and revise these past due POA&Ms with any justification explaining why they had not been updated within established timeframes. DO management indicated that DO POA&Ms had not been updated due to Information System Security Officer (ISSO) turnover and the lag time for acquiring and onboarding a replacement. (*For the first system, see recommendations #13 and #14. For the second system, see recommendations #15 and #16.)*
- Fiscal Service management had one POA&M past due and did not update or provide a justification of why it was past due. Fiscal Service management indicated that due to competing priorities, management did not place an emphasis on monitoring and closing this POA&M on a timely basis. (*See recommendations #17 and #18.*)

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

We recommend that DO management:

13. For the first selected system, develop a process to ensure that POA&Ms are being monitored according to DO security policies and NIST guidance.

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

15. For the second selected system, develop a process to ensure that system POA&Ms are being monitored according to NIST guidance.

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

We recommend that Fiscal Service management:

17. For the selected system, develop a process to ensure that POA&Ms are being monitored according to Fiscal Service policies and NIST guidance.

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

3. Configuration management plan was incomplete and missing key information regarding system baseline configurations at Fiscal Service.

NIST SP 800-53, Rev. 4, requires that organizations develop, document, and maintain under configuration control, a current baseline configuration of the information system. This control falls under the protect Cybersecurity domain, and configuration management FISMA program area. We noted the following:

For the selected system, the configuration management plan (CMP) was incomplete and did not address controls and security requirements over the baseline configuration, which is essential to supporting system rollback procedures. In addition, the plan did not specify the responsibilities regarding the system baseline configuration, the retention and availability of previous baseline configurations, and the frequency that management should review the baseline. Fiscal Service management indicated that the system team was in a transition from one Federal Reserve Bank to another Federal Reserve Bank for application support this past year. In addition to the operational change, management did not notice the change in the configuration template and failed to complete the new section for baseline requirements. (*See recommendation #19.*)

By not documenting the required information regarding baseline configuration can cause confusion regarding which parties are responsible for the maintenance of the baseline, and the process by which the baseline is reviewed, updated and deployed. Therefore, these actions may not be performed.

We recommend that Fiscal Service management:

19. For the selected system, ensure that information security controls and requirements, including controls over the system baseline configuration, shared configuration management responsibilities, and the retention of previous baselines, are addressed adequately in the system CMP.

4. Vulnerability scans were not being conducted in accordance with TD P 85-01 policies at BEP and DO.

The TD P 85-01, Volume I, requires Treasury bureaus to scan for vulnerabilities in the information system and hosted applications every two weeks and when new vulnerabilities potentially affecting the system and applications are identified and reported. This control falls under the protect Cybersecurity domain and the configuration management FISMA program area. We noted the following:

- For the selected system, BEP management has a Federal Risk and Authorization Management Program (FedRAMP) authorized system that is hosted by a cloud service provider who performs vulnerability scans on its environment monthly instead of every two weeks as required by TD P 85-01. BEP Management stated that the accreditation package did not document the specific RA-5

Vulnerability Scanning frequency deviation as a risk acceptance. (*See recommendations #20 and #21.*)

- DO management did not conduct vulnerability scans for two months for the servers hosted at the Fiscal Service data center. Management did not perform vulnerability scans every two weeks as required by the TD P 85-01. Additionally, the DO *Information Technology Security Handbook* (DO P-910) defines the frequency of vulnerability scans to be conducted at least every thirty days, which does not comply with the biweekly frequency specified by TD P 85-01. DO management stated that as part of the new scanning policy, the system's internet protocol (IP) addresses were removed from the data center scan to be added to a new distinct system-specific scan. Due to human error, these IP addresses were never added into the new scan. (*See recommendations #22, #23, #24, and #25.*)

Not scanning the system for vulnerabilities could result in the system not being adequately patched to remediate known flaws. This may result in weaknesses that allow unauthorized access and/or bugs that jeopardize the confidentiality, integrity, and availability of the system environment and network.

We recommend that BEP management:

20. For the selected system, work with the Cloud Service Provider to increase the scanning frequency for the system components or create a formal risk acceptance for the reduced scanning frequency.

21. For the selected system, document the actions taken in the above step(s) in the SSP.

We recommend that DO management:

22. For the selected system, work with Fiscal Service to ensure the system server IP addresses are added to the scanning policy and ensure all future scans are performed at least every two weeks.

23. For the selected system, enhance vulnerability scanning procedures to ensure a lack a scans will be noted in the event of failure in the future.

24. At the bureau level, update the DO Information Technology Security Policy Handbook (DO P 910) to align with the vulnerability scan frequency of every two weeks, as specified by TD P 85-01.

25. At the bureau level, ensure all DO system's corresponding SSPs are updated to reflect the scanning frequency as TD P 85-01 and conduct vulnerability scans accordingly.

5. Account management activities were not compliant with policies at CDFI Fund, TTB, OIG, DO, Fiscal Service and Mint.

TD P 85-01 Volume I requires Treasury bureaus and offices to automatically disable inactive accounts after 120 days. Additionally, TD P 85-01 Volume I requires Treasury bureaus to receive a signed acknowledgement from individuals requiring access to the information system, and to review and update the rules of behavior on a bureau defined frequency. Access agreements are also required to reviewed, signed and updated at least annually. Finally, bureaus are required to create, enable, modify, disable, and remove information system accounts in accordance with organization-defined

procedures or conditions. This control falls under the protect Cybersecurity domain and the identity and access management FISMA program area. We noted the following:

- For the selected CDFI Fund system, 5 of 21 sampled user accounts had gone unused for more than 60 days and were not disabled as required by the Security Policy Handbook. Of these five accounts, three had never logged into the system after the account was created. CDFI Fund management indicated that the script being utilized to disable accounts automatically following 60 days of inactivity had flaws in identifying inactive accounts in certain scenarios (e.g., missing employee ID field, null last login date). In addition, management failed to review consistently the weekly disabled user report and remove inactive accounts. (*See recommendations #26, #27, and #28.*)
- For the selected TTB system, 3 of 8 sampled users for one subcomponent were inactive for more than 60 days and were not disabled automatically within the system, which does not adhere to the SSP. Additionally, we inspected the completed Rules of Behavior (ROB) for system users and noted that one user completed the ROB three months after the account was created, which does not comply with the SSP. For the users who were inactive for more than 60 days, TTB management stated that one of the users is a help desk technician and does not log into their account on a regular basis; rather, this user logs in as needed to assist users with technical issues. The second user is a Quality Assurance (QA) Manager who only logs in when a user needs assistance logging in. Additionally, the third account is a system admin account that is not regularly used, but an active account is required. For the user who did not sign the ROB in a timely manner, TTB stated that management did not initially assign the New User criteria to the account while the user was onboarding, which includes the requirement to sign the ROB. The New User criteria was subsequently assigned to the user once it was discovered that the user did not complete required training. (*See recommendations #29 and #30.*)
- For the selected OIG system, access authorizations and user agreements (e.g., Rules of Behavior ROB and Access Agreements) were not consistently documented, approved, and retained during the FY 2016 FISMA performance period. Specifically, 1 of 15 sampled access authorization email notifications was not retained; 2 of 15 sampled ROB/User Agreement forms were not retained for users given access to the system; and 5 of 15 sampled ROB/User Agreement forms were not signed by the ISSO. OIG management indicated that the account authorization process is a manual process initiated by the Human Resource (HR) department. Furthermore, the HR personnel who initiated the request for access, no longer worked for the bureau and the record was not retained elsewhere. Additionally, OIG management stated the ROB/Access Agreements for two of the sampled users had been lost. OIG management further stated the only required signature on the form is from the user; however, this requirement has not been documented in a policy. (*See recommendations #31 and #32.*)
- For the selected DO system, 71 out of 3,214 system user accounts had gone unused for more than 120 days and were not disabled as required by the SSP. DO management noted that the system utilizes a script to disable accounts that have been inactive for more than 90 days. This script, however, skips over certain Microsoft Active Directory (AD) Organizational Unit (OU) containers and account types. Therefore, some accounts will not be disabled. (*See recommendation #33.*)
- Management utilizes Non-Disclosure Agreements (NDAs) for users as a form of Rules of Behavior and Access Agreement for the first selected Fiscal Service system. Two of 15 sampled system users did not complete their NDAs in a timely manner (within 21 days as stated on the Fiscal Service NDA form). In addition, three of 15 sampled users were missing NDAs. For the second selected system, the SSP and Fiscal Service Baseline Security Requirements (BLSR) required management to disable system user accounts that are inactive for more than 120 days and that management should delete user accounts after 13 months of inactivity. Fiscal Service

management failed to disable or remove 285 out of 1,294 system users that were inactive for more than 120 days. In addition, 85 out of 1,294 users had not logged into their system accounts and were not disabled or removed. Fiscal Service management indicated that users did not complete or sign a NDA in a timely manner due to management oversight. Additionally, Fiscal Service management stated that when the system transitioned to a single sign-on (SSO) system for account management, the system management had requested that SSO system be configured to identify inactive users. However, the General Technical Manager did not update SSO system based on resource constraints. In addition, based on historical experience with other Fiscal Service systems that transitioned to SSO, there was a possibility that accounts in SSO system could be modified, suspended, and removed in error. (*For the first system, see recommendations #34. For the second system, see recommendations #35 and #36.*)

- For the selected Mint system, we noted that Mint retains the access authorizations in its Information Technology Service Management (ITSM) ticketing system for the selected system. We noted that 2 of the 8 sampled tickets only identified the customer requesting access and not the actual user who was granted access. Mint management required validation for the two users located at a Mint field office, and the Mint field office IT manager was unable to readily validate ticket information for two users through the ITSM ticketing system. The user listing provided included Customer Names from ITSM tickets however, the Customer Name was not always the actual user. To determine the user added, each ITSM ticket from the original listing had to be reviewed to identify and validate the user receiving approval for access. Mint management indicated that the process for validating user access approvals is manual, requiring the review of each ITSM ticket. (see recommendations #37 and #38)

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

We recommend that CDFI Fund management:

26. For the selected system, work with TTB to revise the inactive user script.

27. For the selected system, test and verify that the script is configured to disable all inactive users after 60 days of inactivity.

28. For the selected system, implement a periodic account review process that will identify any inactive users who have not been disabled.

We recommend TTB management:

29. For the selected system, perform a periodic review/analysis, as required by policy, of the accounts for the system to validate that no enabled accounts have gone unused for more than 60 days.

30. For the selected system, establish procedures to be performed by TTB management to ensure that users consistently complete the TTB Rules of Behavior and Access Agreements prior to granting users' access to the system.

We recommend OIG management:

31. For the selected system, establish a process for consistently completing the Rules of Behavior and Access Agreements and update policies to reflect this policy.

32. For the selected system, establish a process and a centralized location to store and retain completed forms.

We recommend DO management:

33. For the selected system, configure the system to disable user accounts automatically after 120 days of inactivity.

We recommend Fiscal Service management:

34. For the first system, establish a process to ensure that all system users are consistently completing a NDA within a timely manner, and a process to revoke accounts when a NDA is not completed.

35. For the second system, in the absence of a long-term system capability solution, obtain a formal risk acceptance waiver and perform manual monthly reviews of all system user accounts and disable or delete accounts that no longer need access.

36. For the second system, configure or acquire additional system capability to automatically disable user accounts in accordance with system and Fiscal Service defined frequency.

We recommend Mint management:

37. For the selected system, review established process and procedures for creation of ITSM tickets for user access requests to specifically identify users receiving access and not just the customers submitting ITSM tickets for user access to system. Furthermore, require that the actual individuals save a copy of their ITSM ticket email notification and email messages for their own access authorization requests for their records.

38. For the selected system, ensure that all current users have their completed ITSM ticket request for access authorizations on file.

6. Contingency planning activities were not compliant with policies at DO, Mint, FinCEN and OIG.

The TD P 85-01, Volume I, requires Treasury bureaus to test the contingency plan for the information system no less than annually using NIST SP 800-84, NIST SP 800-34 and other applicable guidance, and Business-unit Defined Tests and Exercises to determine the effectiveness of the plan and review the contingency plan test results and initiate corrective actions if needed. Additionally, TD P 85-01 requires that bureaus test backup information semi-annually for moderate systems to verify media reliability and information integrity. This control falls under the recover Cybersecurity domain and the contingency planning FISMA program area. We noted the following:

- DO's annual system contingency plan testing was not consistent with DO requirements. A PowerPoint presentation was presented to contingency team members explaining general contingency plan concepts. However, DO did not perform formal contingency planning testing

during the FISMA year, which is not consistent with DO P-910. DO management indicated that the ISSO interpreted the DO requirements to allow a PowerPoint presentation to be sufficient for contingency plan testing. Further, the ISSO interpreted the DO requirements for backup testing to be every other year instead of twice a year. (*See recommendations #39 and #40.*)

- Mint management did not approve and sign the contingency plan during the FISMA year. Mint management did not sign the contingency plan because a signature page was not included in the contingency plan template. (*See recommendation #41.*)
- FinCEN management did not conduct a contingency plan test and exercise for the system during the FISMA year. Further, management provided a contingency plan that was last reviewed and updated on December 11, 2015, but was not finalized or approved as of the end of the FISMA reporting period. FinCEN management indicated that there was a lack of oversight to ensure FinCEN contingency plans are updated and annually tested. (*See recommendations #42 and #43.*)
- For the selected OIG system, the backup integrity test was neither formally conducted nor documented during the FISMA performance period. OIG management noted that system backups were informally tested; therefore, documentation was not available to support the results of the test. (*See recommendation #44.*)

Failing to update, approve and test the contingency plan bureaus may be vulnerable to unknown weaknesses in its contingency plan procedures should a situation arise in which the plan must be implemented. Also, without documenting contingency plan approvals, key infrastructure personnel may implement contingency plan procedures that are either out of date or incorrect. Additionally, failing to test and document the integrity and reliability of information system backups increases the risk of unexpected data loss.

We recommend that DO management:

39. For the selected system, revise the Contingency Plan Test to adhere to DO P-910 and TD P 85-01 requirements for a moderate system and perform testing as required.

40. For the selected system, integrate testing on backups in coordination with Fiscal Services during contingency plan testing occurring twice a year.

We recommend that Mint management:

41. For the selected system, require that senior level officials document their approvals of the Contingency Plan by adding their signature to the Contingency Plan signature page following each annual plan update.

We recommend that FinCEN management:

42. For the selected system, ensure that the system Contingency Plans are tested on an annual basis and documented according to NIST guidance.

43. For the selected system, require that senior level officials document their approvals of the Contingency Plan by adding their signature to the Contingency Plan signature page following each plan update.

We recommend that OIG management:

44. For the selected system, conduct and document formal tests of backup information to ensure media reliability and information integrity on a semi-annual basis.

SELF-IDENTIFIED WEAKNESSES

During the FY 2016 Treasury FISMA performance audit, we noted 3 DO systems, 2 Fiscal Service systems, 1 FinCEN system, 1 Mint system, and 1 OCC system had in aggregate, 41 NIST SP 800-53, Rev. 4, controls that had weaknesses that were self-identified by the bureaus/offices. These self-identified weaknesses were associated with 41 open POA&Ms. We reviewed each self-identified weakness and noted that each weaknesses had a corrective action plan documented within a POA&M, and, therefore, did not provide any additional recommendations.

FY16 FISMA Self-Identified Weaknesses – Department of the Treasury

Bureau	System	NIST SP 800 53 Control	Weakness
DO	DO System #1	CA-3	POA&M #11087 ISAs for 1 system interconnection is expired.
DO	DO System #1	CM-2	POA&M #11084 Baseline configuration settings are not in compliance.
DO	DO System #2	AC-2	POA&M #8395: Account creation, modification, enabling, disabling, or removal of accounts is not automatically audited.
DO	DO System #2	AC-2	POA&M #8410: The system has no process by which the Organization Administrator is notified if general users transfer/resign, therefore neither the account nor passwords are updated.
DO	DO System #2	AU-6	POA&M #8411: Information system monitoring logs/alerts are not provided to DO.
DO	DO System #2	CA-5	POA&M #8397: Plan of Action and Milestones is not up to FISMA standards.
DO	DO System #2	CM-2 CM-6	POA&M #8398: Baseline configuration is outdated.
DO	DO System #2	CM-6 SI-2	POA&M #8419: Vulnerability scanning is only executed monthly and the application is only scanned when being promoted from development to production.
DO	DO System #2	CM-6	POA&M #8407: USB ports are not disabled on the servers.
DO	DO System #2	CM-2 CM-6 CM-8	POA&M #8418; Inventory reports are not provided monthly to the CISO.
DO	DO System #2	CP-4	POA&M #8420: CP Test results are documented but are not provided to the SO/ISSO.
DO	DO System #2	IA-2	POA&M #8399: System does not implement PIV enabled features. POA&M #8408: System does not employ multi-factor authentication.
DO	DO System #2	PL-4 PS-6	POA&M #8401: Third-party personnel are not required to sign a DO NDA nor a ROB.
DO	DO System #2	RA-5	POA&M #8400: System Incidents discovered by the third-party are not reported to DO.

Bureau	System	NIST SP 800 53 Control	Weakness
DO	DO System #2	SI-2	POA&M #8403: 2015 SA&A scanning effort identified numerous vulnerabilities.
DO	DO System #3	CA-3	POA&M #9277: Insufficient interconnection Security Agreements.
DO	DO System #3	CM-2	POA&M #10970: The systems Baseline Configurations not adequately documented.
DO	DO System #3	CM-6	POA&M #9286: Autocomplete HTML attribute not disabled for password field. POA&M #9287: Cacheable SSL Page Found. POA&M #9288: Missing HTTP only attribute in session cookie. POA&M #9289: Missing secure attribute in encrypted session (SSL) cookie. POA&M #9290: Permanent cookie contains sensitive session information. POA&M #9291: Query parameter in SSL request.
Fiscal Service	FS System #1	PL-4	POA&M #10642: The System SSP and SCM are out of date.
Fiscal Service	FS System #2	IA-2	POA&M #7273: Multifactor Authentication Not Being Utilized.
FinCEN	FinCEN System #1	CA-5	POA&M #9803: POA&Ms are not updated in a timely manner.
Mint	Mint System #1	AC-2	POA&M #10707: The systems users and roles have been granted predefined options.
Mint	Mint System #1	AU-2 AC-2	POA&M #10694: The system does not implement automated audit actions to include automatic notification of the ISSO.
Mint	Mint System #1	CM-6	POA&M #10702: Application server configuration settings do not meet established criteria. POA&M #10696: Oracle configuration settings do not meet established criteria.
Mint	Mint System #1	SI-2	POA&M #10699: The system does not have the latest patches/updates installed.
OCC	OCC System #1	AC-2	POA&M #9327, #9950, #9249: Account Creation Auditing.
OCC	OCC System #1	CA-5	POA&M #11206: POA&MS are not updated in a timely manner.
OCC	OCC System #1	CM-6	POA&M #10378, #9247, #9248: System Configuration Settings
OCC	OCC System #1	CM-8	POA&M #6400: System Inventory does not accurately reflect inventory of system components.
OCC	OCC System #1	AC-2	POA&M #9299 System is not configured to automatically deactivate inactive accounts.

MANAGEMENT RESPONSE TO THE REPORT

The following is the Treasury CIO's response, dated November 1, 2016, to the FY 2016 FISMA Performance Audit Report.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

November 1, 2016

MEMORANDUM FOR LARISSA KLIMPEL
ACTING DIRECTOR, INFORMATION TECHNOLOGY AUDIT

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

SUBJECT: Management Response to Draft Audit Report – "Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2016 Performance Audit"

Thank you for the opportunity to comment on the draft report entitled, *Department of the Treasury Federal Information Security Modernization Act [FISMA] Fiscal Year 2016 Performance Audit*. We are pleased the report states our security program is consistent with applicable FISMA requirements, the Office of Management and Budget (OMB) policy and the National Institute of Standards and Technology (NIST) standards and guidelines. We acknowledge there are FISMA program areas identified in the draft report that require security improvement.

We have carefully reviewed the draft report and agree with all findings and recommendations. Please refer to the attachment for further details on our planned corrective actions. We appreciate your noting that of those Bureaus' with self-identified weaknesses, each Plan of Action and Milestones (POA&M) had adequate corrective action plans established, and therefore, your auditors did not provide any additional recommendations. Finally, we value your recognition that due to fundamental changes on how Inspectors General (IG) score and evaluate agencies in 2016, a year-on-year comparison of FISMA compliance is not possible.

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

- Deployed Einstein 3 Accelerated (E3A) countermeasure Domain Name Services (DNS) Sinkhole architecture capable of adding advanced detection and prevention methods against malicious activity. This new capability aids Treasury's Government Security Operations Center (GSOC) Incident Response team in implementing more robust security measures across multiple domains.

- Established Treasury's Phishing Awareness Program to educate and protect users against the threat of sophisticated phishing attacks while enabling the Department to enhance its resilience against cybersecurity threats.

- Achieved an Initial Operating Capability for Phase 1 of the Continuous Diagnostics and Mitigation solution across five bureaus.

- Accomplished two full iterations of identification, prioritization, and categorization for Treasury's High Value information Assets (HVA) as required by OMB.

- Completed coordination and participation in Risk Vulnerability Assessment (RVA) activities with the Department of Homeland Security (DHS) per Binding Operational Directive 16-01.

- Reached Maturity Level-2 of the President's Management Council (PMC) Cybersecurity Assessment, and achieved Maturity Level-3 in one functional area.

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

Attachment

cc: Kody Kinsley, Assistant Secretary for Management
Jack Donnelly, Associate Chief Information Officer for Cyber Security
and Chief Information Security Officer

Management Response to KPMG Recommendations

KPMG Finding 1: Risk management activities were not compliant with policies at the Community Development Financial Institution (CDFI), Office of the Inspector General (OIG), and Departmental Offices (DO).

KPMG Recommendation 1: We recommend CDFI Fund management: For the selected system, implement a process or mechanism to ensure all required documentation (e.g., System Security Plan (SSP), Contingency Plan, Risk Assessments, etc.) is uploaded into the Department's Federal Information Security Modernization Act (FISMA) inventory management tool on the frequency stipulated in Treasury Directive Publication (TD P) 85-01.

> **Treasury's Response:** All system Security Assessment and Authorization (SA&A) documents have been uploaded to Treasury FISMA Inventory Management System (TFIMS). The TD P 85-01 TFIMS SA&A document upload controls are currently being adhered to. The completion date was August 20, 2016.
>
> **Responsible Official:** CDFI, Chief Information Officer

KPMG Recommendation 2: We recommend CDFI Fund management: For the selected system, update the SSP to include CDFI Fund's control implementation.

> **Treasury's Response:** The system SSP has been updated to reflect CDFI Fund's control implementation. The completion date was September 5, 2016.
>
> **Responsible Official:** CDFI, Chief Information Officer

KPMG Recommendation 3: We recommend OIG management: For the selected system, ensure all controls/control enhancement sections and statuses that indicate the control implementation are fully documented in the SSP as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4.

> **Treasury's Response:** The OIG management will review and update the OIG SSP in accordance with NIST SP 800-53. The target completion date is April 28, 2017.
>
> **Responsible Official:** OIG, Chief Information Officer

KPMG Recommendation 4: We recommend OIG management: For the selected system, conduct and document a formal risk assessment for the system in accordance with TD P 85-01.

> **Treasury's Response:** The OIG management will conduct a formal risk assessment for the selected system. The target completion date is April 28, 2017.
>
> **Responsible Official:** OIG, Chief Information Officer

KPMG Recommendation 5: We recommend OIG management: For the selected system, develop a security assessment plan that describes the scope of the assessment to include, security controls and control enhancements, assessment procedures to be used to determine security control effectiveness and the assessment environment.

Treasury's Response: The OIG will create a stand-alone security control assessment procedure in accordance with NIST SP 800-53. Target completion date is March 31, 2017.

Responsible Official: OIG, Chief Information Officer

KPMG Recommendation 6: We recommend OIG management: For the selected system, conduct a security control assessment based upon the security assessment plan.

Treasury's Response: The OIG management will create a stand-alone security control assessment procedure in accordance with NIST SP 800-53. Target completion date is March 31, 2017.

Responsible Official: OIG, Chief Information Officer

KPMG Recommendation 7: We recommend OIG management: For the selected system, document the results of the assessment in a security assessment report.

Treasury's Response: The OIG management will conduct a formal risk assessment for the selected system. Target completion date is March 31, 2017.

Responsible Official: OIG, Chief Information Officer

KPMG Recommendation 8: We recommend DO management: For the first selected system, align the system documentation of minimum control requirements with the system SSP template requirements.

Treasury's Response: The Office of DC Pension **(**ODCP) Information Systems Security Officer (ISSO) is in the process of converting the controls data from the Security Requirements Controls Matrix (SRCM) to the SSP template. The target completion date is November 30, 2016.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 9: We recommend DO management: For the first selected system, review the control implementation documentation to ensure that the NIST 800-53, Rev. 4, controls and control enhancements are fully documented in the SSP.

Treasury's Response: As part of the conversion from the SRCM to the SSP, the ODCP ISSO will review each NIST 800-53, Rev. 4 control in the system template to ensure that a response is provided for each on behalf of the system. The target completion date is November 30, 2016.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 10: We recommend DO management: For the second selected system, ensure that the system's current SSP is being reviewed and updated according to NIST SP 800-53, Rev. 4, guidance.

Treasury's Response: The selected system's SSP will be reviewed and updated regularly in accordance with NIST SP 800-53 Rev. 4 guidance. The target completion date is April 30, 2017.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 11: We recommend DO management: For the second selected system, ensure descriptions of controls in place are reflective of inherited controls by the service provider.

> **Treasury's Response:** The selected system's SSP will be updated to accurately describe the controls in place that are provided by the vendor. The target completion date is April 30, 2017.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Recommendation 12: We recommend DO management: For the second selected system, ensure implementation statuses are being updated to reflect the system more accurately.

> **Treasury's Response:** The SSP will be updated regularly with current statuses of control implementation. The target completion date is April 30, 2017.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Finding 2: Plan Of Actions & Milestones (POA&Ms) were not tracked in accordance with NIST and Treasury requirements at DO and Fiscal Service (FS).

KPMG Recommendation 13: We recommend DO management: For the first selected system, develop a process to ensure that POA&Ms are being monitored according to DO security policies and NIST guidance.

> **Treasury's Response:** The DO management has already begun to revise and update their POA&Ms processes and procedures to improve POA&Ms monitoring by having quarterly meetings with system owners and stakeholders. The completion date was October 14, 2016.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Recommendation 14: We recommend DO management: For the first selected system, ensure POA&Ms are updated with revised milestones and provide adequate justification for missed remediation dates.

> **Treasury's Response:** The DO management has already begun to revise and update their POA&M processes and procedures by updating specific fields in the inventory database such as the revised due dates and due dates comments field. The completion date was October 14, 2016.
>
> **Responsible Official:** DO, Chief Information Security Officer

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

> **Treasury's Response:** The POA&Ms are being updated quarterly (or less) in the inventory database system. Updates on actions affecting POA&Ms are being input as they are known. This is being done according to NIST guidance. The completion date was September 30, 2016.
>
> **Responsible Official:** DO, Chief Information Security Officer

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

Treasury's Response: The POA&Ms are being updated with revised milestones and are being provided adequate justification for missed remediation dates. The completion date was September 30, 2016.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 17: We recommend that FS management: For the selected system, develop a process to ensure that POA&Ms are being monitored according to FS policies and NIST guidance.

Treasury's Response: The FS agrees with the finding/recommendation as presented in the draft audit report. The FS will ensure that Fiscal Information Technology Mainframe (FITM) POA&Ms are being monitored according to NIST guidance. The target completion date is June 30, 2017.

Responsible Official: FS, Chief Information Officer

KPMG Recommendation 18: We recommend that FS management: For the selected system, ensure POA&Ms are updated with revised milestones and provide adequate justification for missed remediation dates.

Treasury's Response: The FS agrees with the finding/recommendation as presented in the draft audit report. The FS will ensure FITM POA&Ms are updated with revised milestones and provide adequate justification for missed remediation dates. The target completion date is June 30, 2017.

Responsible Official: FS, Chief Information Officer

KPMG Finding 3: Configuration Management Plan (CMP) was incomplete and missing key information regarding system baseline configurations at FS.

KPMG Recommendation 19: We recommend that FS management: For the selected system, ensure that information security controls and requirements, including controls over the system baseline configuration, shared configuration management responsibilities, and the retention of previous baselines, are addressed adequately in the system CMP.

Treasury's Response: The FS agrees with the finding/recommendation as presented in the draft audit report. The FS has revised the system CMP to address the controls over the system baseline configuration, shared configuration management responsibilities, and retention of previous baselines. Evidence to support this will be validated by the Bureau. The target completion date is January 31, 2017.

Responsible Official: FS, Chief Information Officer

KPMG Finding 4: Vulnerability scans were not being conducted in accordance with TD P 85-01 policies at Bureau of Engraving and Printing (BEP) and DO.

KPMG Recommendation 20: We recommend that BEP management: For the selected system, work with the Cloud Service Provider to increase the scanning frequency for the system components or create a formal risk acceptance for the reduced scanning frequency.

Treasury's Response: The BEP plans to update the accreditation and authority to operate documentation for the system after discussing the possibility of changing a Federal Risk and Authorization Program (FedRAMP) control objective to meet Treasury policy requirements to determine what, if any, cost would be incurred and whether the customization is permitted under the contract. If the control cannot be updated, then the accreditation package will be updated to document the risk, risk level, and mitigation strategy, as appropriate. The updated package will then be resubmitted to the authorizing official for review. The completion date was September 20, 2016.

Responsible Official: BEP, Chief Information Security Officer

KPMG Recommendation 21: We recommend that BEP management: For the selected system, document the actions taken in the above step(s) in the SSP.

Treasury's Response: The BEP plans to update the accreditation and authority to operate documentation for the system after discussing the possibility of changing a FedRAMP control objective to meet Treasury policy requirements to determine what, if any, cost would be incurred and whether the customization is permitted under the contract. If the control cannot be updated, then the accreditation package will be updated to document the risk, risk level, and mitigation strategy, as appropriate. The updated package will then be resubmitted to the authorizing official for review. The completion date was September 20, 2016.

Responsible Official: BEP, Chief Information Security Officer

KPMG Recommendation 22: We recommend that DO management: For the selected system, work with FS to ensure the system server IP addresses are added to the scanning policy and ensure all future scans are performed at least every two weeks.

Treasury's Response: The ISSO worked with the Bureau of the FS to investigate the reason why the selected systems were not included in the bi-weekly scans; once the issue was identified, the ISSO worked with the FS to have the selected systems scanning schedule re-established. The completion date was August 1, 2016.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 23: We recommend that DO management: For the selected system, enhance vulnerability scanning procedures to ensure a lack a scans will be noted in the event of failure in the future.

Treasury's Response: The Bureau of the FS, System Manager/Infrastructure ISSO receives the scan results for the system. In addition, the DO CISO has requested that the FS provide all future system scanning results to the DO CISO's office. ODCP is working with FS to comply with the DO CISO request. The target completion date is
November 30, 2016.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 24: We recommend that DO management: At the bureau level, update the DO Information Technology Security Policy Handbook (DO P 910) to align with the vulnerability scan frequency of every two weeks, as specified by TD P 85-01.

Treasury's Response: The DO management will revise the DO 910 to reflect the updated scan frequency of two weeks. The target completion date is June 30, 2017.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 25: We recommend that DO management: At the bureau level, ensure all DO system's corresponding SSPs are updated to reflect the scanning frequency as TD P 85-01 and conduct vulnerability scans accordingly.

Treasury's Response: The DO management will revise the system SSP to reflect the updated scan frequency of two weeks as part of the annual update. The target completion date is June 30, 2017.

Responsible Official: DO, Chief Information Security Officer

KPMG Finding 5: Account management activities were not compliant with policies at CDFI Fund, Tax and Trade Bureau (TTB), OIG, DO, FS and Mint.

KPMG Recommendation 26: We recommend that CDFI Fund management: For the selected system, work with TTB to revise the inactive user script.

Treasury's Response: The TTB has modified the inactive user script. The script is fully functional. CDFI Fund is currently reviewing all inactive users weekly. This update has been documented in the system SSP. The completion date was August 20, 2016.

Responsible Official: CDFI, Chief Information Officer

KPMG Recommendation 27: We recommend that CDFI Fund management: For the selected system, test and verify that the script is configured to disable all inactive users after 60 days of inactivity.

Treasury's Response: The TTB has modified the inactive user script. The script is fully functional. CDFI Fund is currently reviewing all inactive users weekly. This update has been documented in the system SSP. The completion date was August 20, 2016.

Responsible Official: CDFI, Chief Information Officer

KPMG Recommendation 28: We recommend that CDFI Fund management: For the selected system, implement a periodic account review process that will identify any inactive users who have not been disabled.

Treasury's Response: The TTB has modified the inactive user script. The script is fully functional. CDFI Fund is currently reviewing all inactive users weekly. This update has been documented in the system SSP. The completion date was August 20, 2016.

Responsible Official: CDFI, Chief Information Officer

KPMG Recommendation 29: We recommend TTB management: For the selected system, perform a periodic review/analysis, as required by policy, of the accounts for the system to validate that no enabled accounts have gone unused for more than 60 days.

Treasury's Response: To address the finding, TTB will modify the system SSP, Account Management control, to state:

- Inactive user accounts will be automatically disabled at 60 days.
- System authorizations will continue to be reviewed on an annual basis by their system owner and any invalid authorizations will be removed as a result of that review.
- Application specific authorizations for systems will not be automatically disabled unless the system owners determine otherwise.
- System authorizations will be removed when the user no longer requires access to the application. Target completion date is November 18, 2016.

Responsible Official: TTB, Chief Information Security Officer

KPMG Recommendation 30: We recommend TTB management: For the selected system, establish procedures to be performed by TTB management to ensure that users consistently complete the TTB Rules of Behavior and Access Agreements prior to granting users' access to the system.

Treasury's Response: Regarding the Rules of behavior finding, we will modify our procedures to require that new user Active Directory (Windows) accounts are set to automatically expire if the user has not completed the Rules of Behavior and Access Agreements within a specified amount of time. A warning will be sent to the IT Security Office, the Training Coordinator and the user's manager two days before expiration. If the user does not complete the Rules of Behavior or Access Agreements within the allotted time, the account will remain disabled until they will have completed the necessary forms using TLMS externally. Once the completion of the Rules of Behavior and Access Agreements has been verified, the user account will be enabled. The target completion date is November 18, 2016.

Responsible Official: TTB, Chief Information Security Officer

KPMG Recommendation 31: We recommend OIG management: For the selected system, establish a process for consistently completing the Rules of Behavior and Access Agreements and update policies to reflect this policy.

Treasury's Response: The OIG management will update separate OIG system Access Authorizations and User Agreements for OIG users, and contractors. The completion date was August 2, 2016.

Responsible Official: OIG, Chief Information Officer

KPMG Recommendation 32: We recommend OIG management: For the selected system, establish a process and a centralized location to store and retain completed forms.

Treasury's Response: The OIG management will update a separate OIG General Support System (GSS) Access Authorizations and User Agreements for OIG users, and contractors. The completion date was August 2, 2016.

Responsible Official: OIG, Chief Information Officer

KPMG Recommendation 33: We recommend DO management: For the selected system, configure the system to disable user accounts automatically after 120 days of inactivity.

Treasury's Response: The DO is currently revising system scripts and procedures to comply with the disabling of user accounts after 120 days of inactivity. In addition legitimate exceptions of accounts excluded from the scripts will be documented. The target completion date is June 30, 2017.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 34: We recommend FS management: For the first system, establish a process to ensure that all system users are consistently completing an NDA within a timely manner, and a process to revoke accounts when an NDA is not completed.

Treasury's Response: The FS will update access management procedures, enhance tracking, and train key personnel to remediate this finding. The target completion date is June 30, 2017.

Responsible Official: FS, Chief Information Officer

KPMG Recommendation 35: We recommend FS management: For the second system, in the absence of a long-term system capability solution, obtain a formal risk acceptance waiver and perform manual monthly reviews of all system user accounts and disable or delete accounts that no longer need access.

Treasury's Response: The FS will implement a manual monthly review to ensure accounts that have been inactive for 120 days are disabled or removed. A formal Risk Acceptance will also be pursued to document acceptance of any residual risk. The target completion date is June 30, 2017.

Responsible Official: FS, Chief Information Officer

KPMG Recommendation 36: We recommend FS management: For the second system, configure or acquire additional system capability to automatically disable user accounts in accordance with system and Fiscal Service defined frequency.

Treasury's Response: The system application accounts are stored in FS's application protocol and are shared accounts that are used for access to more than just the system. FS's application protocol password policy settings will lock / disable the account after 120 days of inactivity. FS will evaluate and determine an approach (if feasible) to an automated solution to disable user access (authorization) to system if the application is not accessed by the user for 120 days. The target completion date is June 30, 2017.

Responsible Official: FS, Chief Information Officer

KPMG Recommendation 37: We recommend Mint management: For the selected system, review established process and procedures for creation of Information Technology Service Management (ITSM) tickets for user access requests to specifically identify users receiving access and not just the customers submitting ITSM tickets for user access to system. Furthermore, require that the actual individuals save a copy of their ITSM ticket email notification and email messages for their own access authorization requests for their records.

Treasury's Response: Review and update existing processes and procedures for creation of ITSM tickets to specify customer requesting and the user receiving access to information systems and applications. The target completion date is January 30, 2017.

Responsible Official: Mint, Chief Information Security Officer

KPMG Recommendation 38: We recommend Mint management: For the selected system, ensure that all current users have their completed ITSM ticket request for access authorizations on file.

Treasury's Response: Ensure ITSM and Helpdesk include a designated Access Approval mailbox address on all access authorization emails to ensure efficient access. The target completion date is January 30, 2017.

Responsible Official: Mint, Chief Information Security Officer

KPMG Finding 6: Contingency planning activities were not compliant with policies at DO, Mint, Financial Crimes Enforcement Network (FinCEN) and OIG.

KPMG Recommendation 39: We recommend that DO management: For the selected system, revise the Contingency Plan (CP) Test to adhere to DO P-910 and TD P 85-01 requirements for a moderate system and perform testing as required.

Treasury's Response: The ISSO performed the FISMA year 2017 contingency plan test in a manner consistent with DO policy. Specifically, the ISSO conducted a back-up tape test. In addition, the ISSO is planning a CP tabletop exercise with the system's response team to ensure everyone understands their roles in the event the system's CP is initiated. The target completion date is March 30, 2017.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 40: We recommend that DO management: For the selected system, integrate testing on backups in coordination with FS during contingency plan testing occurring twice a year.

Treasury's Response: The ISSO has integrated back-up tape testing into the CP test schedule. The first back-up tape test will be included in the annual CP test and the second back-up take test will occur in the first or second quarter of each fiscal year. The target completion date is March 30, 2017.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 41: We recommend that Mint management: For the selected system, require that senior level officials document their approvals of the CP by adding their signature to the CP signature page following each annual plan update.

Treasury's Response: Update the CP template to add a signature page for senior level official(s) review and approval. The target completion date was October 14, 2016.

Responsible Official: Mint, Chief Information Security Officer

KPMG Recommendation 42: We recommend that FinCEN management: For the selected system, ensure that the system CP are tested on an annual basis and documented according to NIST guidance.

Treasury's Response: The FinCEN will ensure the system CP is approved by management and tested according to NIST guidance. The target completion date is April 30, 2017.

Responsible Official: FINCEN, Chief Information Security Officer

KPMG Recommendation 43: We recommend that FinCEN management: For the selected system, require that senior level officials document their approvals of the CP by adding their signature to the CP signature page following each plan update.

Treasury's Response: The FinCEN will ensure the system CP is approved by management and tested according to NIST guidance. The target completion date is April 30, 2017.

Responsible Official: FINCEN, Chief Information Security Officer

KPMG Recommendation 44: We recommend that OIG management: For the selected system, conduct and document formal tests of backup information to ensure media reliability and information integrity on a semi-annual basis.

Treasury's Response: The OIG management will develop and conduct a formal backup integrity test for the OIG system. The completion date was September 29, 2016.

Responsible Official: OIG, Chief Information Officer

APPENDIX I – OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives for this performance audit were to assess the effectiveness of the Department of the Treasury's (Treasury's) information security programs and practices for the period July 1, 2015 to June 30, 2016 for its unclassified systems and to evaluate Treasury's compliance with the Federal Information Security Modernization Act of 2014 (FISMA) and related information security policies, procedures, standards, and guidelines. Specifically, the objectives of this audit were to:

- Perform an assessment of the effectiveness 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).
- Assess the implementation for a sample of security controls from NIST SP 800-53 Revision 4 for 15 non-national security systems.
- Follow up on the status of prior-year FISMA findings.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) applicable to performance audits. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To accomplish our audit objectives, we evaluated security controls in accordance with applicable legislation; the DHS *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.1.3,* dated September 26, 2016; and the National Institute of Standards and Technology (NIST) standards and guidelines as outlined in the *Criteria* section. We reviewed Treasury's information security program for a program-level perspective and then examined how each bureau and office complied with the implementation of these policies and procedures.

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

PHASE A: Assessment of Department-Level Compliance

To gain an enterprise-level understanding, we assessed management, policies, and guidance for the overall Treasury-wide information security program per requirements defined in FISMA and DHS *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.1.3*, dated September 26, 2016 as well as Treasury guidelines developed in response to FISMA. This included program controls applicable to risk management, contractor systems, configuration management, identity and access management, security and privacy training, information security continuous monitoring, incident response, and contingency planning.

PHASE B: Assessment of Bureau and Office Level Compliance

To gain a bureau and office level understanding, we assessed the implementation of the guidance for the 11[4] bureau- and office-wide information security programs according to requirements defined in FISMA and DHS *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.1*.3, as well as Treasury guidelines developed in response to FISMA. This included program controls applicable to risk management, contractor systems,

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

configuration management, identity and access management, security and privacy training, information security continuous monitoring, incident response, and contingency planning.

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

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

We also tested a subset of 15 information systems from a total population of 113 non-IRS major applications and general support systems as of April 28, 2016.[5] 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 TIGTA.[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 Treasury's and bureaus' policies, procedures, and guidelines. Lastly, we evaluated selected security-related documents and records, including security assessment and authorization (SA&A) packages, configuration assessment results, and training records.

We performed our fieldwork from June 1, 2016 to July 31, 2016 at Treasury's headquarters offices in Washington, D.C., and bureau locations and data centers in Washington, D.C.; Hyattsville, Maryland; Kansas City, Missouri; East Rutherford, New Jersey; Merrifield, Virginia; Vienna, Virginia; Parkersburg, West Virginia. During our audit, we met with Treasury management to discuss our preliminary conclusions.

Criteria

We focused our FISMA audit approach on federal information security guidance developed by NIST and Office of Management and Budget (OMB). NIST Special Publications (SP) 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 TIGTA, rather than selecting a random sample of information systems that might exclude a Treasury bureau. We pulled the inventory again on July 08, 2016 and noted that there were no changes to the inventory.

[6] Our rotational system selection strategy precludes selecting systems reviewed within the past two years.

[7] Note (per *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.1.3*): 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

following is a listing of the criteria used in the performance of the fiscal year (FY) 2016 FISMA performance audit:

NIST Federal Information Processing Standard (FIPS) and/or SPs

- NIST FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- NIST FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance- Based Model*
- NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*
- NIST SP 800-60, Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*
- NIST SP 800-70, Rev. 3, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*

OMB Policy Directives

- OMB Circular A-130, *Management of Federal Information Resources*
- OMB Memorandum 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*
- OMB Memorandum 05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*
- OMB Memorandum 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*
- OMB Memorandum 15-01, *Fiscal Year 2014 – 2015 Guidance on Improving Federal Information Security and Privacy Management Practices*

Department of Homeland Security

- *DHS FY 2016 Inspector General Federal Information Security Management Act of 2014 Reporting Metrics Version 1.1.3*

Treasury Policy Directives

- Treasury Directive Publication (TD P) 15-71, Department of the Treasury Security Manual

FIPS 200 specifically requires it. Unless specified by additional implementing policy by OMB, guidance documents published by NIST generally allow agencies latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable and compliant with the guidance.

- TD P 85-01, Volume I, *Treasury Information Technology Security Program*

APPENDIX II – STATUS OF PRIOR-YEAR FINDINGS

In Fiscal Year (FY) 2015, FY 2012, and FY 2011 we conducted a FISMA Performance Audit in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. In Fiscal Year (FY) 2014 and FY 2013, we conducted a FISMA Evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation. As part of this year's FISMA Performance Audit we followed up on the status of the prior year findings. For the following prior-year performance audit findings, we evaluated the information systems to determine whether the recommendations have been implemented and whether the findings were closed by management. We inquired of Department of the Treasury (Treasury) personnel and inspected evidence to determine the status of the findings. If there was evidence that the recommendations had been sufficiently implemented, we validated the closed findings. If there was evidence that the recommendations had been only partially implemented or not implemented at all, we determined the finding to be open. We did not evaluate the status of any FY 2012 FISMA findings as they were already closed.

Prior Year Findings – 2015 Performance Audit

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2015 Finding #1 – Community Development Financial Institutions (CDFI) Fund Logical account management activities were not compliant with policies.	For a selected CDFI Fund system, the associated system security plan (SSP) stated user accounts are disabled after 120 days of inactivity. However, the CDFI Fund IT Security Policy Handbook (CDFI Fund P-910) stated that systems needed to be configured to automatically disable any user account after 90 days of inactivity. In addition, we noted that 9 user accounts had been inactive for more than 120 days and were still enabled within the system. For the selected system, management stated that a thorough review of the updated SSP was not performed to ensure that the SSP was in compliance with the CDFI Fund P-910. Furthermore, the security configurations for disabling inactive users were not appropriately implemented.	We recommend that CDFI Fund management: 1 For the selected system, update the SSP to require disabling of inactive user accounts after 90 days of inactivity as defined within the CDFI Fund IT Security Policy Handbook. 2 For the selected system, ensure the system is configured to automatically disable user accounts after 90 days of inactivity.	**Closed** We obtained and inspected the SSP and noted it was updated to include the requirement of disabling of inactive user accounts after 90 days of inactivity as defined within the CDFI Fund IT Security Policy Handbook. In addition, we obtained and inspected the script that is run showing that users are disabled after 60 days of inactivity and a copy of the email notification that is generated after the execution of the script showing users that have not logged in for over 60 days.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2015 Finding #1 – Bureau of the Fiscal Service (Fiscal Service) Logical account management activities were not compliant with policies.	For a selected Fiscal Service system, the system relied on a user account management tool for creating and managing access to system. The user account management tool did not automatically disable 3 inactive users with last login date greater than 120 days. Fiscal Service management indicated there was a programming issue with the account management tool, which caused some inactive user accounts not being disabled after 120 days. This programming issue only affected accounts originally provisioned by the legacy Bureau of the Public Debt user provisioning system.	We recommend that Fiscal Service management: 1 For the selected system, develop or acquire additional system capability to automatically disable user accounts that have been inactive for more than 120 days. 2 For the selected system, in the absence of a long-term system capability solution, perform manual monthly reviews of all system user accounts and disable or delete accounts that no longer need access.	**Closed** We obtained and inspected supporting documentation of the code change, evidence displaying that accounts are deactivated after 120 days, and evidence to show that a change request was completed to implement the code change.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2015 Finding #1 – Departmental Offices (DO) Logical account management activities were not compliant with policies.	For a selected DO system, the system was not configured to disable user accounts that have not logged in the system within 90 days. Rather, it uses a password reset configuration as a mitigating control to disable user's accounts who have not reset their passwords within 90 days. However, some system administrators had the "password inactive" setting for their administrator accounts configured to "never," which would only force a password change every 90 days but not lock the account. We noted 7 of the 11 system administrator's accounts that were inactive for more than 90 days were not disabled within the system. In addition, management did not adhere to the account management policies and procedures as documented in the system's SSP as follows: • 8 accounts were not documented as service accounts. • 4 new user accounts were created prior to obtaining the appropriate approvals. DO management was unaware that the mitigating control (i.e., password reset configuration) was not appropriately configured for all users to disable accounts once the password expired.	We recommend that DO management: 1 For the selected system, review the password reset configuration settings for all users on the servers to ensure they are configured to automatically disable user accounts who has not reset their passwords within 90 days. 2 For the selected system, perform a review/analysis of the administrative accounts for the system to validate no enabled accounts have gone unused for more than 90 days. 3 For the selected system, ensure all accounts are appropriately identified. 4 For the selected system, ensure the policies and procedures in place for appropriately approving and granting system access for new user accounts is followed.	**Closed** We obtained and inspected the password reset configuration settings for all users on the server and noted they are configured to automatically disable users who have not reset their passwords within 90 days. We obtained and inspected the a privileged user account review and noted they are performed no less than twice a year, and quarterly for DO Cyber data calls. Any accounts that are inactive for more than 90 days and/or no longer required were removed We obtained and inspected a listing of the accounts and noted that all accounts were appropriately identified as user accounts or service accounts. Additionally, we noted management had developed an account provisioning procedure as part of account management, which requires approvals by the Customer for requests to create information system accounts.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2015 Finding #1 – United States Mint (Mint) Logical account management activities were not compliant with policies.	For a selected Mint system, the help desk did not document or retain records for 4 of the sampled 25 new user access authorizations for the application. Mint management indicated that there was a need to increase support for a large increase in call center volume. During this time, they were receiving user account requests on a daily basis and were trying to setup the call center as quickly as possible, which resulted in some users not properly going through the formal ticketing process.	We recommend that Mint management, for the selected system, ensure access forms are completed, properly reviewed by the help desk prior to granting access, and centrally retained by the help desk.	**Open** We obtained and inspected the Account Control Policy and noted it was updated on January 25, 2016 and the enforcement requirements were modified. However, we were unable to obtain user access forms for two users and noted that the third-party vendor was unable to provide evidence of how the users were granted access to the environment.
Prior Year FY 2015 Finding #2 – CDFI Fund Did not implement all of the NIST SP 800-53, Rev. 4, security controls for some of their SSPs and ensure completeness in accordance with NIST guidance.	CDFI Fund's SSP for the selected system did not comply with all required NIST SP 800-53 Rev. 4 controls and enhancements. We noted either 12 controls and 21 control enhancements were missing or the implementation descriptions of the controls were not documented. Although the SSP was not compliant, we noted that the annual assessment for system was performed based on the updated NIST SP 800-53 Rev. 4. CDFI Fund management indicated a thorough review of the updated SSP was not performed. As such, all NIST SP 800-53 Rev. 4 applicable controls and control enhancements for this system were not included.	We recommend that CDFI Fund management, for the selected system, update the SSP to address and reference NIST SP 800-53 Rev. 4 controls and control enhancements, and ensure that the implementation description is specified for each control.	**Closed** We obtained and inspected the SSP and noted that it was updated to address and reference NIST SP 800-53, Rev. 4, controls and control enhancements, and included to implementation description for each control.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2015 Finding #2 – Mint Did not implement all of the NIST SP 800-53, Rev. 4, security controls for some of their SSPs and ensure completeness in accordance with NIST guidance.	Mint's SSP for the selected system that is managed by a third party cloud service provider (CSP) did not address all required NIST SP 800-53 Rev. 4 controls. We noted that 38 controls and 35 control enhancements were either missing or did not contain sufficient information to satisfy the control requirements. In addition, the SSP did not adequately address the following sections as outlined in the NIST SP 800-18: 1.3 Operation Status, 1.5 System Environment, 1.5.2 Encryption/PKI, 1.5.3 Network Configuration, 1.6 System Interconnection/Information Sharing, 1.6.2 Mobile Code, and 1.6.3 Ports, Protocols, & Services. Furthermore, control implementation statuses (i.e., implemented, not implemented, planned, inherited, not inherited, partially implemented, or compensated) were not documented for all NIST SP 800-53 Rev. 4 controls. Mint management stated that this was the first year of authorization for the selected system and that the SSP was not finalized because the third party CSP had limited resources to complete all required sections sufficiently in the time that was allotted.	We recommend that Mint management: 1 For the selected system, ensure that control implementation statements and statuses for all NIST SP 800-53 Rev. 4 controls and control enhancements are fully addressed in the SSP. 2 For the selected system, ensure that the following sections: 1.3 Operation Status, 1.5 System Environment, 1.5.2 Encryption/PKI, 1.5.3 Network Configuration, 1.6 System Interconnection/Information Sharing, 1.6.2 Mobile Code, 1.6.3 Ports, Protocols, & Services are consistent with guidance provided in the criteria and are fully documented.	**Partially Implemented/Open** We obtained and inspected the SSP and noted that it did not completely address all of the control implementation statements and statuses for all NIST SP 800-53, Rev. 4, controls and control enhancements. However, we noted in the SSP that the following sections had been updated and fully documented: 1.3 Operation Status, 1.5 System Environment, 1.5.2 Encryption/PKI, 1.5.3 Network Configuration, 1.6 System Interconnection/Information Sharing, 1.6.2 Mobile Code, 1.6.3 Ports, Protocols, & Services.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2015 Finding #2 – Office of the Comptroller of the Currency (OCC) Did not implement all of the NIST SP 800-53, Rev. 4, security controls for some of their SSPs and ensure completeness in accordance with NIST guidance.	OCC's SSP for the selected system did not address all required NIST SP 800-53 Rev. 4 controls, enhancements, and implementation descriptions. We noted 22 controls and 12 control enhancements did not fully address NIST SP 800-53 Rev. 4 controls. Furthermore, two control enhancements were missing from the SSP. OCC management indicated there were limitations in the application used to generate the SSP template and it did not include NIST SP 800-53 Rev. 4 controls, control enhancements, and implementation statuses.	We recommend that OCC management, for the selected system, update the SSP to address and reference NIST SP 800-53 Rev. 4 controls, control enhancements, and ensure that the implementation description is specified for each control	**Closed** We obtained and inspected the system' SSP and noted that the updated SSP included the required NIST SP 800-53, Rev. 4, controls, enhancements, and implementation descriptions for each specified control.
Prior Year FY 2015 Finding #3 – Alcohol and Tobacco Tax and Trade Bureau (TTB) Security program policy and procedures were not consistent with the NIST SP 800-53, Rev. 4 security controls.	The TD P 85-01 requires Treasury bureaus to ensure their policies and procedures are updated and reviewed to reflect the latest NIST guidance. This control falls under the risk management FISMA program area. Specifically, we noted the TTB security program policy and procedures incorrectly reference controls from the outdated NIST SP 800-53 Rev. 4 initial public draft version, dated February 2012. The policies and procedures do not include all required controls and control enhancements from the NIST SP 800-53 Rev. 4 final version, dated April 2013. We noted that 63 controls did not meet NIST SP-800-53 Rev. 4 requirements or were missing all, or part, of the control. TTB management indicated they were not aware that the security program policy and procedures did not address final NIST SP 800-53 Rev. 4 controls.	We recommend that TTB management, review and update the TTB security program policy and procedures to include all relevant controls and control enhancements procedures in the NIST SP 800-53 Rev. 4 final version.	**Closed** We obtained and inspected the SSP and noted that it had been updated and included all relevant controls and control enhancements procedures in the NIST SP 800-53, Rev. 4, final version.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2015 Finding #4 – DO POA&Ms were not tracked in accordance with NIST and Treasury requirements.	DO management did not document and track progress towards remediating existing POA&Ms and did not close POA&Ms by the established due date as documented in the POA&Ms for two selected systems. DO management had a total of 15 POA&Ms for one selected system and 6 POA&Ms for the other selected systems. None of the past due POA&Ms were updated with revised due dates or with any description in the "Status Comment" field explaining why they had not been closed. We also noted that there were seven closed POA&Ms for the first selected system did not include a remediation plan to describe the steps taken. DO Management indicated that due to competing priorities, DO management did not place emphasis on monitoring and closing POA&Ms on a timely basis. In cases where original POA&M due dates were not met management also did not revise the due dates or enter an explanation in the "Status Comment" field to explain why the original due date was missed.	We recommend that DO management: 1 For the first selected system, ensure that the POA&Ms are being monitored according to NIST guidance. 2 For the first selected system, ensure POA&Ms are updated with revised milestones and provide adequate justification for missed remediation dates. 3 For the first selected system, ensure POA&Ms document the remedial actions taken to correct the weaknesses or deficiencies for which the POA&M was created. 4 For the second selected system, ensure that the selected system's POA&Ms are remediated and updated according to NIST guidance. 5 For the second selected system, ensure POA&Ms are updated with revised milestones and provide adequate justification for missed remediation dates.	**Closed** For the first selected system, we inspected the Department's FISMA inventory management tool for all POA&Ms for the first system and noted that the POA&Ms were being monitored, updated, and revised according to NIST guidance by reviewing the timestamps for each of the POA&M entries. In addition, we noted that the POA&Ms documented the remedial actions taken to correct the deficiencies. For the second selected system, we inspected the Department's FISMA inventory management tool for all POA&Ms for the second system and noted that the POA&Ms were being updated, revised, and remediated in accordance to NIST guidance by reviewing the timestamps for each of the POA&M entries.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2015 Finding #4 – Financial Crimes Enforcement Network (FinCEN) POA&Ms were not tracked in accordance with NIST and Treasury requirements.	FinCEN management did not monitor progress towards remediating existing POA&Ms and did not close POA&Ms by the established milestones. As of June 30, 2015, FinCEN management had a total of 14 POA&M items that were past due and were not updated or provided with a justification for why they have not been closed. In addition, the selected system's POA&M report did not adequately outline the remedial actions with updated dates or the remediation plan. FinCEN management indicated that it is currently overhauling the system and that rather than spend limited resources fixing the old system, the POA&Ms will be addressed when the new system undergoes a formal security accreditation and authorization process.	We recommend that FinCEN management: 1 For the selected system, ensure that the POA&Ms are being monitored according to NIST guidance. 2 For the selected system, ensure POA&Ms are remediated accordingly with established milestones. If POA&Ms are not remediated, then POA&Ms should be updated with an adequate justification.	**Closed** We obtained and inspected evidence provided by FinCEN management that FinCEN closed 13 out of the 14 late POA&Ms and one (1) POA&M item has been updated with a new date completion. We further verified the status of the 14 POA&Ms for the selected system and noted all POA&M items were updated and included remedial action, effectiveness of remedial action, and updated dates.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2015 Finding #5 – Mint Contract with third-party cloud service provider did not address FedRAMP requirements.	The TD P 85-01 requires that all cloud systems shall comply with Federal Risk and Authorization Management Program (FedRAMP) guidelines. This control falls under the contractor systems FISMA program area. We noted the Mint's selected system is managed by a third-party cloud service provider (CSP); however, the CSP only provides application vulnerability scan reports and does not provide vulnerability scanning results of their infrastructure to the Mint. In addition, the Mint required the CSP to provide the Contingency Plan (CP). Furthermore, the CSP did not provide the following FISMA-related artifacts demonstrating compliance with NIST SP 800-53, Rev. 4: • Vulnerability scans for the months of January and May to ensure patches were occurring in a timely manner. • Security auditing tools' configuration settings were configured for a component of the selected system to capture auditable events as specified in accordance with the SSP. • User lists for two components of the selected system to capture the account creation date. • User lists for two components of the selected system to capture the last log-on date. In addition, one of the in-scope component's user list to capture both the last log-on date and enabled/disabled status.	We recommend that Mint management: 1 For the selected system, revisit the existing third-party CSP's contract and ensure the appropriate FedRAMP security clauses and requirements related to FISMA and NIST guidance are incorporated. 2 For the selected system, ensure that third-party CSP provides FISMA-related artifacts to demonstrate FISMA compliance to the Mint security compliance team. 3 For the selected system, remind the Mint contracting officer to ensure FedRAMP contract-specific clauses regarding compliance with FISMA and NIST are in place.	**Open** We obtained and inspected the extension letter related to this finding and noted that the due date was extended from April 30, 2016 to October 31, 2016, because the testing and evaluation of security controls for FedRAMP requirements will not take place until the current ATO expires on September 29, 2016.

Prior Year Findings – 2014 Evaluation

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #1 –Bureau of the Fiscal Service (Fiscal Service) Logical account management activities, such as access authorizations, were not in place or not consistently performed.	For a selected Fiscal Service system, Fiscal Service management did not retain supporting documentation of access approval for 1 of 25 administrative accounts. For this selected system, Fiscal Service did not have an effective process to retain evidence of access approval.	We recommend that Fiscal Service management, for the selected system, implement a new process to ensure that all administrative accounts are approved and that evidence of access approval is retained.	**Closed** We obtained and inspected the system's Account Recertification Standard and procedures and noted that requires administrative accounts to be approved and that evidence of access approval is required to be retained through the recertification process. Further, we obtained and inspected evidence that 10 users were removed since the last recertification process and evidence of access is retained.

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

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #3 – Mint Did not follow NIST guidance for SSPs	Mint's SSP for the selected system was last updated in May 2013, and has not been reviewed annually as required by Mint guidelines. Furthermore, the SSP utilized security controls from an outdated initial public draft version of the NIST SP 800-53, Rev. 4, which was released in February 2012. The Mint had not updated the SSP to include all of the required controls and enhancements from the final NIST SP 800-53, Rev. 4, version, dated April 2013. On March 30, 2012 the designated Mint security analyst reviewed the SSP and completed updates to reflect NIST SP 800-53, Rev. 4, initial public draft controls and enhancements. Mint management was aware that the SSP needed to be updated to reflect the final Rev. 4 controls. However, there were limited resources to update the SSP due to a transition in the IT contractor support in June 2013.	We recommend that Mint management: 1 For the selected systems, review and update the SSP to include all relevant controls from the NIST SP 800-53, Rev. 4, final version. 2 For the selected systems, ensure Rev. 4 controls and enhancements are implemented on the system and tested promptly	**Partially Implemented/Open** We inspected the selected system's SSP and noted that the SSP is includes all relevant Rev. 4 controls; however the implementation statuses were not identified. Mint was unable to provide evidence that all Rev. 4 controls in place for the selected system were assessed**.**
Prior Year FY 2014 Finding #5 – Bureau of Engraving and Printing (BEP) Bureau IT security and configuration management policies had not been updated or reviewed to address NIST and Treasury requirements	BEP management had not updated their IT security policies and procedures to incorporate the latest NIST SP 800-53, Rev. 4, controls. BEP management failure to stay compliant with NIST and Treasury policies was due to competing priorities with other IT initiatives. This was a self-reported finding and documented within BEP's enterprise-wide plan of action and milestones (POA&M), with an estimated completion date of December 15, 2014.	Based on the planned corrective actions for BEP, we are not making a recommendation.	**Open** BEP had not finished completing its corrective action during the course of this performance audit. We noted that the enterprise-wide POA&M due date to update the policies has been changed to December 31, 2016.

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #6 – Mint Did not update or review their contingency plan, or finalize their contingency plan test results	Contingency plan documentation for a selected Mint system had not been updated or reviewed since January 2009. Mint provided a 2014 disaster recovery exercise lessons-learned report, from February 2014; however, we noted this was still a draft version and had not been signed off by key contingency personnel.	We recommend that Mint management: 1 For the selected system, update the Contingency Plan. 2 For the selected system, ensure key contingency personnel sign-off annually on the contingency plan review and contingency plan test and exercise in a timely fashion after its completion.	**Closed** We obtained and inspected he system contingency plan and noted it was updated, signed, and finalized on September 1, 2015. We further noted it was signed timely after the contingency plan review contingency plan test and exercise was complete.

Prior Year Findings – 2013 Evaluation

Finding #	Prior Year Condition	Recommendation(s)	Status
Prior Year FY 2013 Finding #1 – Treasury Inspector General for Tax Administration (TIGTA) Logical account management activities were not in place or not consistently performed.	For a selected TIGTA system, TIGTA management was unable to provide a system-generated list showing last login dates and times. In addition, we were unable to obtain evidence of user authorization forms for the system. As a result, there was no evidence that user account management was in place and operating effectively. It was noted that this was a self-reported finding and was listed as a POA&M within the Trusted Agent FISMA (TAF) system with an estimated completion date of January 31, 2014.	Based on TIGTA's planned corrective actions, we are not making a recommendation.	**Open** TIGTA has not finished completing its corrective action. We noted that the POA&M due date has been revised to June 1, 2017.
Prior Year FY 2013 Finding #4 – TIGTA Contingency planning and testing controls were not fully implemented or operating as designed.	TIGTA did not fully implement contingency planning (planning and testing) controls as required by TD P 85-01 Volume I, NIST SP 800-53, Rev. 3, and NIST SP 800-34 guidance. While these controls do not affect normal, daily operations, they are invaluable in quickly recovering the system from a disaster or service interruption. Contingency plan documentation for a selected TIGTA system was not finalized within the FISMA year. This was a self-reported finding and documented within TIGTA's POA&M report on TAF, with an estimated completion date of December 31, 2013.	Based on TIGTA's planned corrective actions, we are not making a recommendation.	**Open** TIGTA has not finished completing its corrective action. We noted that the POA&M due date has been revised to June 1, 2017.

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. We noted that the POA&M due date has been revised to meet new milestones on December 31, 2016, May 31, 2017, and May 31, 2017.
Prior Year FY 2011 Finding #8 – TIGTA Contingency planning and testing and backup controls were not fully implemented or operating as designed.	The selected TIGTA system lacked sufficient documentation regarding the system's contingency plan and contingency plan testing. Specifically, the documentation did not include certain key software used. TIGTA management identified these weaknesses during a 2010 security assessment and established two POA&M items with scheduled completion dates of January 2012 and June 2012.	Based on TIGTA's planned corrective actions, we are not making a recommendation.	**Open.** TIGTA has not finished completing its corrective action. We noted that the POA&M due date has been revised to June 30, 2017.

Prior Year Findings – FY15 Self-Identified Weaknesses

Bureau	System	NIST SP 800 53 Control	Weakness	Status
BEP	BEP System #1	CA-6 CM-11 IA-2 MP-7 PL-2 PL-8 RA-2 RA-3 RA-5 SI-2	POA&M #R4001 (enterprise-wide): The system implementation for NIST SP 800-53 Rev. 4 is incomplete.	**Open** Management has not updated their overarching security policy (BEP 10-08.35) to align with NIST 800-53, Rev. 4.
DO	DO System #1	SI-2	POA&M #6861: Application supports Java SE Development Kit (JDK) 5.x and 6.x. Load balancers affected by multiple vulnerabilities.	**Open** DO has not finished completing its corrective action. We noted that the POA&M due date has been revised to December 2016.
	DO System #1	CM-6	POA&M #7788: System does not meet 90% compliance with the Center for Internet Security (CIS) Benchmark for its Linux servers	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that the finding was remediated.
	DO System #1	RA-5	POA&M #6736: Monthly vulnerability scan data (OS, Database and application levels) and Summary Reports are not provided to Treasury POA&M #7314: The database scanning tool used does not have the ability to update itself prior to running a new scan	**Partially Implemented/Open** POA&M 6736 is open POA&M 7314 is closed We obtained and examined supporting evidence in support of

Bureau	System	NIST SP 800 53 Control	Weakness	Status
				POA&M #7314 and noted that the corrective action plan was implemented and that this finding was remediated. We noted that the POA&M #6736 due date has been revised to December 30, 2016.
	DO System #1	IA-2	POA&M #6368: IA-2 Identification and Authentication: Partially Implemented. Two factor authentication has not been implemented for Remote Access by all users. POA&M #7328: The application can support authentication of Government employees via their PIV Card, but this capability isn't used.	**Open** DO has not finished completing its corrective action. We noted that the POA&M #6368 due date has been revised to January 30, 2017. We noted that the POA&M #7328 due date has been revised September 30, 2016.
	DO System #1	AU-2	POA&M #7412: The SSP doesn't identify what security events captured by the OS, Database and application and how the list of audited events support incident response efforts. Database auditing limited to capturing account logon/logoff.	**Open** DO has not finished completing its corrective action. We noted that the POA&M due date has been revised to September 30, 2016.
	DO System #1	AU-6	POA&M #7413: Application logs are not forwarded to the centralized log server for automated review, analysis and reporting.	**Open** DO has not finished completing its corrective action.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
				We noted that the POA&M due date has been revised to December 31, 2016.
	DO System #2	AC-2	POA&M #584: AC-2: Although accounts are reviewed on an annual basis, quarterly audits are not performed. In addition, the system does not automatically audit account management functions.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that the finding was remediated.
	DO System #2	CM-2	POA&M #576: CM-2: Although several secure hardening guides exist, the system only employs vendor-recommended settings. Additionally, the baseline is not documented. POA&M #6149: CM-2: Previously documented versions of baseline configurations are not documented.	**Partially Implemented/Open** POA&M 576 is open POA&M 6149 is closed We obtained and examined supporting evidence in support of POA&M #6149 and noted that the corrective action plan was sufficient to close the finding. We noted that the POA&M #576 due date has been revised to September 30, 2016.
	DO System #2	CM-6	POA&M #578: CM-6: The system does not employ any automated means to validate the configurations are maintained on a continual basis.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that the finding was remediated.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
	DO System #2	IA-2	POA&M #6151: (IA-2) Multi-factor authentication is not implemented. Only username and password are required for administrator accounts.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that the finding was remediated.
	DO System #2	SI-2	POA&M #575: SI-2: Numerous weaknesses were discovered during the vulnerability scanning conducted in conjunction with the FY 2013 SA&A effort. POA&M #8631: SI-2: Configuration scans revealed that numerous weaknesses were identified in June 2015. POA&M #8634: SI-2: The system does not have automated mechanisms to track the status of resolution for reported system flaws.	**Partially Implemented/Open** POA&M 575 is open POA&M 8631 is open POA&M 8634 is closed We obtained and examined supporting evidence in support of POA&M #8634 and validated that the corrective action plan was sufficient to close the finding. We noted that the POA&M #575 due date has been revised to September 1, 2016. We noted that the POA&M #8631 due date has been revised to September 1, 2016.
	DO System #3	AU-12	POA&M #7645: No application-level auditing capability for application.	**Open** DO has not finished completing its corrective action.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
				We noted that the POA&M due date has been revised to September 1, 2016.
	DO System #3	CP-4	POA&M #3508: Contingency plan testing cannot currently be performed, and emergency preparedness, with regard to system reconstitution, is insufficient.	**Open** DO has not finished completing its corrective action. We noted that the POA&M due date has been revised to September 1, 2016.
	DO System #3	CP-9	POA&M #3506: The disaster recovery site was not operational at the time of the assessment. This gives rise to multiple weaknesses: 1) The viability and integrity of backups cannot be ensured or validated; 2) Alternate storage viability cannot be validated; In addition, telecommunication services have not been established because the alternate site is not operational. As a result of this, the system cannot: - Test/examine emergency preparedness - Establish and validate Service Level Agreements (SLAs) - Identify points of failure	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that the finding was remediated.
Mint	Mint System #1	IA-2	POA&M #111: Two components privileged accounts do not have multifactor authentication enabled. Multifactor authentication supports stronger protections for identity and access of privileged users over remote network access methods such as the Internet as in the case of this application. Exposing application management interfaces publically is generally not best practice and multifactor authentication would lessen the risk of credential compromise due to vulnerabilities in other confidentiality controls.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that the finding was remediated.
FS	FS System #1	AC-2 AU-2	POA&M #3140: The system has neither implemented nor documented a procedure to incorporate the audit data from the General Support System (GSS) pertaining to the security of the	**Closed**

Bureau	System	NIST SP 800 53 Control	Weakness	Status
		AU-6 AU-12	system. These data should be reviewed, analyzed, and reported to support incident response. Without sufficient review, analysis, and reporting, security incidents may go undetected. POA&M #3141: The system relies on the GSS to collect audit events. During an observation conducted to review these audit processes, the GSS was unable to produce the logs containing the events noted in the SSP. The inability of the GSS to provide appropriate audit logs to the system will significantly hinder after-the-fact investigations of events and general risk management.	We obtained and examined supporting evidence in support of this finding and validated that the corrective action plan was sufficient to close the finding.
	FS System #1	CA-2	POA&M #8393: 2015 Continuous Monitoring Test Results were not provided for the system for 5/01/14 - 4/30/15.	**Closed** We obtained and examined supporting evidence in support of this finding and noted that the corrective actions were implemented and that the finding was remediated.
OCC	OCC System #1	AC-2 AU-2 AU-6 AU-12	POA&M #47: Component-level audit requirements have not yet been determined and documented. Lack of auditing for the following: Audit database management event and Audit database object management event. This finding is applicable to the multiple applications within the system.	**Open** OCC has not finished completing its corrective action. We determined that the prior year finding over POA&M #47 is still open since the lack of audit logging still exists.
	OCC System #1	CM-6	POA&M #3741: CM-6 Configuration Settings, CM-7 Least Functionality System vulnerability scans show numerous vulnerabilities due to unnecessary system services. The results of automated configuration management scans have shown a number of	**Open** OCC has not finished completing its corrective action.

Bureau	System	NIST SP 800 53 Control	Weakness	Status
			missing patches that are more than 60 days old. Based on this, it has been determined that while a flaw remediation process exists, it has failed to ensure that the system remains correctly configured and up to date.	We noted that the POA&M is due to be remediated in July 2016, after our FISMA reporting period.

APPENDIX III – DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS's FISMA 2016 QUESTIONS FOR INSPECTORS GENERAL

The information included in Appendix III represents Department of the Treasury's (Treasury) consolidated responses to Department of Homeland Security's (DHS) FISMA 2016 questions for Inspectors General. We prepared responses to DHS questions based on an assessment of 15 information systems across 12 Treasury components (IRS information was provided by TIGTA). For Risk Management, Contractor Systems, Configuration Management, Identity and Access Management, Security and Privacy Training, and Contingency Planning, we provided responses for each metric with either "Met" or "Not Met" using the available options from CyberScope. To determine if a metric was "Met" or "Not Met," we considered results across the 12 bureaus. If we determined that one or more bureaus had a finding related to the metric, we responded with "Not Met." For metrics with "Not Met," we provided explanations in the "Comment" areas. For the last metric in each of Risk Management, Contractor Systems, Configuration Management, Identity and Access Management, Security and Privacy Training, and Contingency Planning, CyberScope automatically determines whether the FISMA program areas are "Optimized," "Effective," or "Not Effective" based on the FISMA Metric Domain answers. The answers below are the outputs from CyberScope and the corresponding rating of "Optimized," "Effective," or "Not Effective." We obtained OIG and TIGTA acceptances for the responses to these FISMA Metric Domains.

Since both the Information Security Continuous Monitoring (ISCM) and Incident Response (IR) are based on DHS' maturity model, we included the five maturity levels for the presentational purposes. However, during the FISMA performance audit, we requested that Treasury management communicate its self-assessed maturity levels, and we then designed and executed test procedures to evaluate whether management's security program and practices over ISCM and IR operated at that self-assessed maturity level. The assessed maturity levels in this Appendix include the consolidated results of our testing across the bureaus and IRS.

Treasury Inspector general for Tax Administration (TIGTA) performed audit procedures over the IRS information systems and provided its answers to the Treasury OIG and KPMG for consolidation. TIGTA's answers are included within the table below, and denoted where its response changed the overall from a "Met" to a "Not Met." The information provided by TIGTA has not been subjected to KPMG audit procedures and, accordingly, we did not modify TIGTA's responses.

Since OMB, DHS, and CEGIE changed the FISMA IG reporting metrics and scoring methodology in FY 2016, a year-on-year comparison for FISMA compliance is not possible.

1: Identify – Risk Management		
Status of Risk Management Program [check one: Met or Not Met]	Met	**1.1** Has the organization established a risk management program that includes comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

1: Identify – Risk Management		
	Not Met	**1.1.1.** Identifies and maintains an up-to-date system inventory, including organization- and contractor-operated systems, hosting environments, and systems residing in the public, hybrid, or private cloud. (2016 CIO FISMA Metrics, 1.1; NIST Cybersecurity Framework (CF) ID.AM.1, NIST 800-53: PM-5) **Comments – Treasury OIG:** OCC has a self-identified weakness over system inventory for the selected system. (See Self-Identified Weaknesses Section: POA&M #6400)
	Met	**1.1.2.** Develops a risk management function that is demonstrated through the development, implementation, and maintenance of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39)
	Met	**1.1.3.** Incorporates mission and business process-related risks into risk-based decisions at the organizational perspective, as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39)
	Not Met	**1.1.4.** Conducts information system level risk assessments that integrate risk decisions from the organizational and mission/business process perspectives and take into account threats, vulnerabilities, likelihood, impact, and risks from external parties and common control providers. (NIST SP 800-37, Rev. 1, NIST SP 800-39, NIST SP 800-53: RA-3) **Comments – Treasury OIG:** OIG GSS Risk Assessment was not performed in accordance with Treasury and NIST guidance. (See Finding #1.) DO has a self-identified weakness over risk assessments for one of the four selected systems. (See Self-Identified Weaknesses Section: POA&M #8403.)
	Met	**1.1.5.** Provides timely communication of specific risks at the information system, mission/business, and organization-level to appropriate levels of the organization.
	Met	**1.1.6.** Performs comprehensive assessments to categorize information systems in accordance with Federal standards and applicable guidance. (FIPS 199, FIPS 200, FISMA, Cybersecurity Sprint, OMB M-16-04, President's Management Council (PMC) cybersecurity assessments)
	Met	**1.1.7.** Selects an appropriately tailored set of baseline security controls based on mission/business requirements and policies and develops procedures to employ controls within the information system and its environment of operation.
	Not Met	**1.1.8.** Implements the tailored set of baseline security controls as described in 1.1.7. **Comments – Treasury OIG:** CDFI fund, OIG and DO did not implement the NIST SP 800-53, Rev 4 security controls for some of their SSPs and ensure completeness in accordance with NIST guidance. (See Finding #1.) Mint did not implement the NIST SP 800-53, Rev. 4, security controls for some of their SSPs and ensure completeness in accordance with NIST guidance. (See Prior Year FY 2015 Finding #2 and Prior Year FY 2014 Finding #3.)

1: Identify – Risk Management		
	Not Met	**1.1.9.** Identifies and manages risks with system interconnections, including through authorizing system interconnections, documenting interface characteristics and security requirements, and maintaining interconnection security agreements. (NIST SP 800-53: CA-3) **Comments – Treasury OIG:** DO has a self-identified weakness over system interconnections for two of the selected systems. (See Self-Identified Weaknesses Section: POA&M #9277 and #11087.) **Comments – TIGTA**: During a prior review, TIGTA identified that the IRS did not have sufficient processes in place to ensure that interconnections in use at the IRS had proper authorization or security agreements. After the end of the FY 2016 FISMA evaluation period, the IRS informed us that it had completed all corrective actions. We have not verified those completed corrective actions.
	Not Met	**1.1.10.** Continuously assesses the security controls, including hybrid and shared controls, using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. **Comments – Treasury OIG:** OIG GSS Security Control Assessment not documented and performed in accordance with Treasury and NIST guidance. (See Finding #1.) Mint did not implement the NIST SP 800-53, Rev. 4, security controls for some of their SSPs and ensure completeness in accordance with NIST guidance. (See Finding #1, Prior Year FY 2015 Finding #2 and Prior Year FY 2014 #3.)
	Met	**1.1.11.** Maintains ongoing information system authorizations 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 (OMB M-14-03, NIST Supplemental Guidance on Ongoing Authorization).
	Not Met	**1.1.12.** Security authorization package contains system security plan, security assessment report, and POA&M that are prepared and maintained in accordance with government policies. (SP 800-18, SP 800-37) **Comments – Treasury OIG:** CDFI did not upload required documentation in the central document repository. OIG GSS Security Control Assessment not documented and performed in accordance with Treasury and NIST guidance. (See Finding #1.) Fiscal Service has a self-identified weakness over the updating of security authorization package documentation for one of the four selected systems. (See Self-Identified Weaknesses Section: POA&M #10642.)
	Not Met	**1.1.13.** POA&Ms are maintained and reviewed to ensure they are effective for correcting security weaknesses.

1: Identify – Risk Management		
		Comments – Treasury OIG: DO for two of the four selected systems, and Fiscal Service for one of the four selected systems, did not update POA&Ms in a timely manner. (See Finding #2) DO has self-identified weakness over POA&M for the selected system. (See Self-Identified Weaknesses Section: POA&M #8397.) FinCEN has self-identified weakness over POA&M for the selected system. (See Self-Identified Weaknesses Section: POA&M #9803.) OCC has self-identified weakness over POA&M for the selected system. (See Self-Identified Weaknesses Section: POA&M #11206.) **Comments – TIGTA**: The IRS did not consistently implement its policies and procedures to maintain and review POA&Ms to ensure that they were effective for correcting security weaknesses. • The IRS did not timely create POA&Ms for 24 (52 percent) of 46 weaknesses. The 46 weaknesses were the total number of weaknesses reported during the FY 2016 annual security assessment reviews for the 10 IRS systems we selected for the FY 2016 annual FISMA evaluation of the IRS. • The IRS closed five (40 percent) of 12 POA&Ms without sufficient support that the weaknesses were corrected. The 12 POA&Ms were the total number of POA&Ms closed by the 10 selected systems during the FY 2016 FISMA evaluation period. The IRS subsequently provided adequate documentation for three of the five to support that the weaknesses had been effectively corrected. The documentation subsequently provided by the IRS for the remaining two did not support that the weaknesses had been corrected. • In other audit work during FY 2016, TIGTA identified that 25 of 63 POA&Ms reviewed did not meet IRS POA&M standards to ensure effective and timely resolution of the weakness. We reviewed all 63 POA&Ms that had been prepared for security control weaknesses related to IRS's external file transfer solutions. Of the 25 POA&Ms that did not meet IRS policy standards, 22 POA&Ms did not contain sufficiently defined or detailed milestone actions to ensure timely resolution of the weakness and three POA&Ms did not address the weakness. The scheduled completion date for eight of the 22 POA&Ms lacking sufficient milestone actions had passed with the weaknesses remaining uncorrected. • The IRS Enterprise FISMA Dashboard reported that, as of June 30, 2016, 14 percent of the IRS's total open POA&Ms have passed scheduled completion dates and therefore are in late status. The IRS's goal was to have less than 10 percent of its open POA&Ms in late status. This indicates that the IRS has not yet consistently implemented its policies and procedures to ensure timely and effective correcting of security weaknesses. The IRS informed TIGTA that it has taken steps to remediate the POA&M consistency and accuracy issues by centralizing POA&M oversight and validation work under the IRS Enterprise FISMA Services office.

1: Identify – Risk Management		
	Not Met	**1.1.14.** Centrally tracks, maintains, and independently reviews/validates POA&M activities at least quarterly. (NIST SP 800-53 :CA-5; OMB M-04-25) **Comments – Treasury OIG:** DO for two of the four selected systems, and Fiscal Service one of the four selected systems, did not update POA&Ms in a timely manner. (See Finding #2.)
	Met	**1.1.15.** 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.
	Not Met	**1.1.16.** Implemented an insider threat detection and prevention program, including the development of comprehensive policies, procedures, guidance, and governance structures, in accordance with Executive Order 13587 and the National Insider Threat Policy. (PMC; NIST SP 800-53: PM-12) **Comments – TIGTA**: The IRS does not have an insider threat detection and prevention program. Although the IRS does not own or operate any classified national security information systems subject to Executive Order 13587, its own policy requires that it implement an insider threat program. In addition, the IRS is waiting for the Department of the Treasury, which is subject to Executive Order 13587, to release its Insider Threat Program to assist in identifying potential insider threats and establish reporting requirements and thresholds for the Treasury bureaus. However, the IRS indicated that its current resources and budget do not allow for a full-scale implementation of an insider threat program until 2027. As such, the IRS has taken a risk based decision to not meet this policy requirement at this time.
	Not Effective	**1.1.17.** Provide any additional information on the effectiveness (positive or negative) of the organization's Risk Management program that was not noted in the questions above. Based on all testing performed, is the Risk Management program effective? **Comments – Treasury OIG:** BEP had not updated or reviewed their bureau policies to address NIST and Treasury requirements. (See Prior Year FY 2014 Finding #5 and Self-Identified Weakness Section POA&M # R4001.) **Comments – TIGTA:** According to the new scoring methodology implemented by the DHS for the FY 2016 Inspector General FISMA Reporting Metrics, program areas must have met all attributes labeled as *Defined* and *Consistently Implemented* and half or more of the attributes labeled as *Managed and Measurable* to have an effective program. This program area did not meet all attributes at the level 3 *Consistently Implemented*.

1: Identify – Contractor Systems		
Status of Contractor Systems Program [check one: Met or Not Met]	Met	**1.2** Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including other government agencies, managed hosting environments, and systems and services residing in a cloud external to the organization that is inclusive of policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?
	Not Met	**1.2.1.** Establishes and implements a process to ensure that contracts/statements of work/solicitations for systems and services, include appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information. (FAR Case 2007-004, Common Security Configurations, FAR Sections 24.104, 39.101, 39.105, 39.106, 52.239-1; PMC, 2016 CIO Metrics 1.8, NIST 800-53, SA-4 FedRAMP standard contract clauses; Cloud Computing Contract Best Practices) **Comments – Treasury OIG:** DO has a self-identified weakness over incidents and information system monitoring alerts are not being reported by the third-party provider for one of the four selected systems. (See Self-Identified Weaknesses Section: POA&M #8400 and 8411) Mint's contract with their third-party cloud service provider did not address FedRAMP requirements and the CSP did not provide FISMA related artifacts to demonstrate FISMA compliance. (See Prior Year FY 2015 Finding #5.) **Comments – TIGTA:** The IRS has recently established a process for reviewing contracts for appropriate security clauses. In November 2015, the IRS instructed its contracting officers to conduct a 100 percent review of all new and existing information technology and service contracts to ensure that all applicable security clauses were included. In June 2016, the IRS instructed its contracting officers to implement codes in the IRS procurement system to indicate whether the contract had been reviewed and includes security clauses if appropriate. The IRS Procurement staff stated that the IRS intends to begin reviewing the progress made to ensure that all contracts include appropriate security clauses on a quarterly basis. As of June 30, 2016, the IRS reported the following results. • 808 contracts that have been reviewed contain appropriate security clauses. • 2,095 contracts that have been reviewed do not require security clauses. • 842 contracts that have been reviewed do not yet contain appropriate security clauses. • 1,844 contracts have not yet been reviewed. (All are active contracts with signed dates on or after July 1, 2016.)
	Met	**1.2.2.** Specifies within appropriate agreements how information security performance is measured, reported, and monitored on contractor- or other entity-operated systems. (CIO and CAO Council Best Practices Guide for Acquiring IT as a Service, NIST SP 800-35)

1: Identify – Contractor Systems		
	Met	**1.2.3.** Obtains sufficient assurance that the security controls of systems operated on the organization's behalf by contractors or other entities and services provided on the organization's behalf meet FISMA requirements, OMB policy, and applicable NIST guidelines. (NIST SP 800-53: CA-2, SA-9)
	Not Effective	**1.2.4.** Provide any additional information on the effectiveness (positive or negative) of the organization's Contractor Systems Program that was not noted in the questions above. Based on all testing performed, is the Contractor Systems Program effective?

2: Protect - Configuration Management		
Status of Configuration Management Program [check one: Met or Not Met]	Met*	**2.1.** Has the organization established a configuration management program that is inclusive of comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Comments – TIGTA:** The IRS established a configuration management program. However, we did note that it had not updated its configuration management policy and procedures within three years or when a significant change occurred as required.
	Not Met	**2.1.1.** Develops and maintains an up-to-date inventory of the hardware assets (i.e., endpoints, mobile assets, network devices, input/output assets, and SMART/NEST devices) connected to the organization's network with the detailed information necessary for tracking and reporting. (NIST CF ID.AM-1; 2016 CIO FISMA Metrics 1.5, 3.17; NIST 800-53: CM-8) **Comments – TIGTA:** Although the IRS has implemented an asset management solution as its official inventory solution, during the FY 2016 FISMA evaluation period, TIGTA reported the inventory being inaccurate and/or incomplete. Also, three of the 10 systems selected for the FISMA evaluation reported in their System Security Plans that NIST SP 800-53 security control CM-8, Information System Component Inventory, was not fully in place.

* TIGTA determined that IRM met this metric based on its testing; however, the bureau provided the clarifying comment.

2: Protect - Configuration Management		
	Not Met	**2.1.2.** Develops and maintains an up-to-date inventory of software platforms and applications used within the organization and with the detailed information necessary for tracking and reporting. (NIST 800-53: CM-8, NIST CF ID.AM-2) **Comments – Treasury OIG:** DO has a self-identified weakness over software inventory documentation for one of the four selected systems. (See Self-Identified Weaknesses Section: POA&M #8418.) **Comments – TIGTA:** Information deemed necessary for effective information system component inventories includes software license information. Within the last three years, TIGTA completed three audits relating to software license management and reported that the IRS was not adequately performing software license management, was not adhering to Federal requirements, and did not have specialized software license tools for developing and maintaining an enterprise-wide inventory. The IRS indicated that it is in the process of deploying a commercial-off-the-shelf software asset management framework to track and maintain its inventory of software in use across the IRS, expected to be completed by October 15, 2017.
	Not Met	**2.1.3.** Implements baseline configurations for IT systems that are developed and maintained in accordance with documented procedures. (NIST SP 800-53: CM-2; NIST CF PR.IP-1) **Comments – Treasury OIG:** Fiscal Service did not specify responsibilities regarding the system baseline configurations for one of the four selected systems. (See Finding #3.) DO has a self-identified weaknesses over baseline configurations for IT systems for three of the four selected systems. (See Self-Identified Weaknesses Section: POA&M #8398, #11084 and #10970.) OCC has self-identified weaknesses over baseline configurations for the selected system. (See Self-Identified Weaknesses Section: POA&M #9247, #9248, and #10378.) DO has a self-identified weakness over baseline configurations for one of the four selected systems. (See Prior-Year Findings – 2015 Self-Identified Weaknesses Section: POA&M #576.) **Comments – TIGTA:** The IRS has established and documented standard baseline configurations for its information technology systems; however, the IRS has not always maintained the configurations in accordance with its documented procedures. Four of the 10 systems selected for the FISMA evaluation reported in their System Security Plans that NIST SP 800-53 security control CM-2, Baseline Configuration, was not fully in place.

2: Protect - Configuration Management		
	Not Met	**2.1.4.** Implements and maintains standard security settings (also referred to as security configuration checklists or hardening guides) for IT systems in accordance with documented procedures. (NIST SP 800-53: CM-6; CIO 2016 FISMA Metrics, 2.3) **Comments – Treasury OIG:** Fiscal Service did not specify responsibilities regarding the system baseline configurations for one of the four selected systems. (See Finding #3.) DO has a self-identified weakness over baseline security control settings for three of the four selected systems. (See Self-Identified Weaknesses Section: POA&M #8407, #9286, #9287, #9288, #9289, #9290, #9291, and #11084.) Mint has a self-identified weakness over baseline configurations for the selected system. (See Self-Identified Weaknesses Section: POA&M #10696 and #10702.) **Comments – TIGTA:** The IRS has not always implemented and maintained standard security settings in accordance with documented procedures. All 10 System Security Plans of the systems selected for the FISMA evaluation showed that some or all of the required configuration settings for servers within their respective authorization boundaries were not implemented in accordance with IRS policy.
	Not Met	**2.1.5.** Assesses configuration change control processes, including processes to manage configuration deviations across the enterprise that are implemented and maintained. (NIST SP 800-53: CM-3, NIST CF PR.IP-3) **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. The GAO reported that the IRS did not document requests and approvals for all changes to the mainframe production system. TIGTA identified that the IRS did not always correct configuration vulnerabilities or apply patches on servers within the established time frames. Also, IRS security change management process and procedure documents are outdated and currently in the IRS's review process. Lastly, three of the 10 systems reported in their System Security Plans that NIST SP 800-53 security control CM-3, Configuration Change Control, was not fully in place.
	Met	**2.1.6.** Identifies and documents deviations from configuration settings. Acceptable deviations are approved with business justification and risk acceptance. Where appropriate, automated means that enforce and redeploy configuration settings to systems at regularly scheduled intervals are deployed, while evidence of deviations is also maintained. (NIST SP 800-53: CM-6, Center for Internet Security Controls (CIS) 3.7)

2: Protect - Configuration Management		
	Not Met	**2.1.7.** Implemented SCAP certified software assessing (scanning) capabilities against all systems on the network to assess both code-based and configuration-based vulnerabilities in accordance with risk management decisions. (NIST SP 800-53: RA-5, SI- 2; CIO 2016 FISMA Metrics 2.2, CIS 4.1) **Comments – Treasury OIG:** DO has a self-identified weakness over vulnerability scanning for one of the four selected systems. (See Prior-Year Findings – 2015 Self-Identified Weaknesses Section: POA&M #6736.) **Comments – TIGTA:** The IRS has not implemented Security Content Automation Protocol certified software assessing (scanning) capabilities against all systems on the network. In addition, the 10 systems selected for review reported in their System Security Plans that eight and four systems, respectively, did not have NIST SP 800-53 security controls RA-5, Vulnerability Management, and SI-2, Flaw Remediation, fully in place.
	Not Met	**2.1.8.** Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2) **Comments – Treasury OIG:** BEP's contract with their third-party cloud service provider did not align with the Treasury Department's vulnerability scanning frequency requirements. DO policy does not align with the Treasury Department's vulnerability scanning frequency requirements. DO vulnerability scans were not performed for parts of the FISMA year for one of the four selected systems. (See Finding #4.) DO has a self-identified weakness over vulnerability scanning for one of the four selected systems. (See Self-Identified Weaknesses Section: POA&M #8419.) DO has a self-identified weakness over configuration management and timely patching for two of the four selected systems. (See Self-Identified Weaknesses Section: POA&M #575, #6861, #8631.) OCC has a self-identified weakness over configuration settings for the selected system. (See Prior-Year Findings – 2015 Self-Identified Weaknesses Section: POA&M #3741.) **Comments – TIGTA:** The IRS has not yet fully implemented configuration related vulnerability scanning tools and processes on all systems to ensure timely remediation of scan result deviations. During the FY 2016 FISMA evaluation period, TIGTA reported that the IRS was not timely remediating high-risk vulnerabilities and POA&Ms did not meet standards. Also, a significant number (six, eight, and four systems, respectively) of the 10 systems selected for review reported in their System Security Plans that they did not have NIST SP 800-53 security controls CM-6, RA-5, and SI-2 fully in place.

2: Protect - Configuration Management		
	Not Met	**2.1.9.** Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01) **Comments – Treasury OIG:** Mint has a self-identified weakness over patch management for the selected system. (See Self-Identified Weaknesses Section: POA&M #10699.) **Comments – TIGTA:** The IRS has developed a comprehensive patch management standard operating procedure. However, the IRS indicated that a patch implementation standard operating procedure is currently being developed to include the tools that will be used for patch installation, standardize processes for common patching activities, and to ensure that patch deployment timelines meet the IRS policy. Both TIGTA and the GAO continue to report on weaknesses in the IRS patch management process. For instance, the IRS did not always ensure that critical security patch updates were applied to its systems in a timely manner. Also, the IRS continues to run outdated and unsupported software on its systems.
	Not Effective	**2.1.10.** Provide any additional information on the effectiveness (positive or negative) of the organization's Configuration Management Program that was not noted in the questions above. Based on all testing performed, is the Configuration Management Program effective? **Comments – Treasury OIG:** DO has a self-identified weakness over audit logging capabilities for two of the four selected systems. (See Prior-Year Findings – 2015 Self-Identified Weaknesses Section: POA&M #7412, #7413, and #7645.) OCC has a self-identified weakness over audit logging capabilities for the selected system. (See Prior-Year – 2015 Self-Identified Weaknesses Section: POA&M #47.) **Comments – TIGTA:** According to the new scoring methodology implemented by the DHS for the FY 2016 Inspector General FISMA Reporting Metrics, program areas must have met all attributes labeled as *Defined* and *Consistently Implemented* and half or more of the attributes labeled as *Managed and Measurable* to have an effective program. This program area did not meet all attributes at the level 2 *Defined*.

2: Protect - Identity and Access Management		
Status of Identity and Access Management Program [check one: Met or Not Met]	Met	**2.2.** Has the organization established an identity and access management program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?
	Not Met	**2.2.1.** Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements, participate in required training prior to being granted access, and recertify access agreements on a predetermined interval. (NIST 800-53: PL-4, PS-6) **Comments– OIG:** Fiscal Service, OIG, TTB did not consistently enforce signed rules of behavior (ROB) or access agreements for their users prior to granting access. (See Finding #5.) DO has a self-identified weakness over access agreements for one of the four selected systems. (See Self-Identified Weaknesses Section: POA&M #8401.) **Comments – TIGTA:** While the IRS has an enterprisewide process to register and grant users access to information systems, during the FY 2016 FISMA evaluation period, TIGTA reported that an IRS office did not use the process to register and grant users access to a system, and therefore appropriate access agreements were not signed. In addition, the System Security Plans for the 10 systems selected for review also reported occurrences of access granted to systems without proper authorization.
	Not Met	**2.2.2.** Ensures that all users are only granted access based on least privilege and separation-of-duties principles. **Comments – Treasury OIG:** Mint have a self-identified weakness the granting of users and roles for one of the selected systems. (See Self-Identified Weaknesses Section: POA&M #10707.) Mint was unable to provide evidence that users' access was granted access based on needs. (See Prior-Year FY 2015 Finding #1.) **Comments – TIGTA:** TIGTA identified 27 systems that did not support that users were granted access based on least privilege, due to incomplete, inaccurate, and outdated documentation for user access. In addition, TIGTA reported that the IRS's standard process to annually recertify that the users have a continued business need for access to the system was not used for users with elevated privileges. Also, during the FY 2016 FISMA evaluation period, the GAO identified users that the IRS allowed to have excessive privileges to systems. Lastly, the system security plans for the 10 IRS systems selected for review reported that 50 percent did not have NIST SP 800-53 security control AC-5, Separation of Duties, fully in place and 50 percent did not have NIST SP 800-53 security control AC-6, Least Privilege, fully in place.

2: Protect - Identity and Access Management		
	Met	**2.2.3.** Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. networking devices, such as load balancers and intrusion detection/prevention systems, and other input/output devices such as faxes and IP phones).
	Not Met	**2.2.4.** Implements PIV for physical access in accordance with government policies. (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11) **Comments – Treasury OIG:** Fiscal Service has a self-identified weakness over PIV use for physical access for one of the selected systems. (See Self-Identified Weaknesses Section: POA&M #7273.) **Comments – TIGTA:** The IRS has implemented the required Homeland Security Presidential Directive 12 and FIPS 201 access control systems in only 61 percent of the buildings that require them. The projected completion of the remaining 39 percent of the buildings is in FY 2019 (if funded).
	Not Met	**2.2.5.** Implements PIV or a NIST Level of Assurance (LOA) 4 credential for logical access by all privileged users (system, network, database administrators, and others responsible for system/application control, monitoring, or administration functions). (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.5.1) **Comments – Treasury OIG:** DO has a self-identified weakness over PIV use for logical access for one of the selected systems. (See Self-Identified Weaknesses Section: POA&M #8399 and #8408.) DO has a self-identified weaknesses over multi-factor authentication for two of the four selected system (See Prior-Year Findings – 2015 Self-Identified Weaknesses Section: POA&M #6368 and #7328.) **Comments – TIGTA:** The IRS reported that all privileged users are required to log on to the IRS network with PIV cards. Work is ongoing to ensure privileged access to systems using PIV cards and to replace aging systems and retire software that do not support PIV card access. As of June 29, 2016, the IRS had enabled a privileged access solution that allowed 1,901 (62 percent) of 3,084 privileged users to log on to privileged accounts using PIV cards.
	Met	**2.2.6.** Enforces PIV or a NIST LOA 4 credential for logical access for at least 85% of non-privileged users. (*Cybersecurity* Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.4.1)

2: Protect - Identity and Access Management		
	Not Met	**2.2.7.** Tracks and controls the use of administrative privileges and ensures that these privileges are periodically reviewed and adjusted in accordance with organizationally defined timeframes. (2016 CIO FISMA Metrics 2.9, 2.10; OMB M-16-04, CIS 5.2) **Comments – Treasury OIG:** DO has a self-identified weakness over tracking of administrative privileges for one of the selected systems. (See Self-Identified Weaknesses Section: POA&M #8410.) DO and OCC have a self-identified weakness over the effectiveness of their account management auditing for one of the selected systems. (See Self-Identified Weaknesses Section: POA&M #8395, #9327, #9950, and #9249d.). **Comments – TIGTA:** During the FY 2016 FISMA evaluation period, TIGTA and the GAO identified deficiencies in this control, reporting that the IRS had not properly limited the use of administrative privileges or ensured that these privileges were periodically reviewed and adjusted in accordance with policy. The IRS's current system to review privileged access does not require revalidation on a semi-annual basis in accordance with IRS policy. The IRS indicated it is working to correct this deficiency.
	Not Met	**2.2.8.** Ensures that accounts are terminated or deactivated once access is no longer required or after a period of inactivity, according to organizational policy. **Comments – Treasury OIG:** It was noted that CDFI, TTB, and DO all do not automatically terminate or suspend user accounts that have been inactive for longer than 120 days. (See Finding #5.) Mint has a self-identified weakness over automatic account termination for one of the selected systems. (See Self-Identified Weaknesses Section: POA&M #10694.) OCC has a self-identified weakness over automatic account termination for the selected system. (See Self-Identified Weaknesses Section: POA&M #9299.) **Comments – TIGTA:** During the FY 2016 FISMA evaluation period, 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.
	Not Met	**2.2.9.** Identifies, limits, and controls the use of shared accounts. (NIST SP 800-53: AC-2) **Comments – TIGTA:** During the FY 2016 FISMA evaluation period, TIGTA and the GAO identified improper use of shared accounts; for example, use of generic administrator accounts and passwords.
	Met	**2.2.10.** All users are uniquely identified and authenticated for remote access using Strong Authentication (multi-factor), including PIV. (NIST SP 800-46, Section 4.2, Section 5.1, NIST SP 800-63)

2: Protect - Identity and Access Management		
	Met	**2.2.11.** Protects against and detects unauthorized remote access connections or subversion of authorized remote access connections, including through remote scanning of host devices. (CIS 12.7, 12.8, FY 2016 CIO FISMA metrics 2.17.3, 2.17.4, 3.11, 3.11.1)
	Met	**2.2.12.** Remote access sessions are timed-out after 30 minutes of inactivity, requiring user re-authentication, consistent with OMB M-07-16.
	Met	**2.2.13.** Enforces a limit of consecutive invalid remote access logon attempts and automatically locks the account or delays the next logon prompt. (NIST 800-53: AC-7)
	Met	**2.2.14.** Implements a risk-based approach to ensure that all agency public websites and services are accessible through a secure connection through the use and enforcement of https and strict transport security. (OMB M-15-13)
	Not Effective	**2.2.15.** Provide any additional information on the effectiveness (positive or negative) of the organization's Identity and Access Management Program that was not noted in the questions above. Based on all testing performed is the Identity and Access Management Program effective? **Comments – Treasury OIG:** TIGTA was unable to provide documentation evidencing the users' last log-on date or time for one selected system and did not formally document account management activities for another prior year selected system. (See Prior-Year FY 2013 Finding #1 and Prior-Year FY 2011 Finding #1.) **Comments – TIGTA:** According to the new scoring methodology implemented by the DHS for the FY 2016 Inspector General FISMA Reporting Metrics, program areas must have met all attributes labeled as *Defined* and *Consistently Implemented* and half or more of the attributes labeled as *Managed and Measurable* to have an effective program. This program area did not meet all attributes at the level 3 *Consistently Implemented*.

2: Protect - Security and Privacy Training		
Status of Security Training Program [check one: Met or Not Met]	Met	**2.3.** Has the organization established a security and privacy awareness and training program, including comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

2: Protect - Security and Privacy Training		
	Met*	**2.3.1.** Develops training material for security and privacy awareness training containing appropriate content for the organization, including anti-phishing, malware defense, social engineering, and insider threat topics. (NIST SP 800-50, 800-53: AR-5, OMB M-15-01, 2016 CIO Metrics, PMC, National Insider Threat Policy (NITP)) **Comments – TIGTA:** The IRS's information systems security awareness training includes basic appropriate content, but it should be further developed to meet the specific requirements relating to insider threats. The IRS said that it plans to update information systems security training for FY 2017.
	Met	**2.3.2.** Evaluates the skills of individuals with significant security and privacy responsibilities and provides additional security and privacy training content or implements human capital strategies to close identified gaps. (NIST SP 800-50)
	Met	**2.3.3.** Identifies and tracks status of security and privacy awareness training for all information system users (including employees, contractors, and other organization users) requiring security awareness training with appropriate internal processes to detect and correct deficiencies. (NIST 800-53: AT-2)
	Met	**2.3.4.** Identifies and tracks status of specialized security and privacy training for all personnel (including employees, contractors, and other organization users) with significant information security and privacy responsibilities requiring specialized training.
	Met	**2.3.5.** Measures the effectiveness of its security and privacy awareness and training programs, including through social engineering and phishing exercises. (PMC, 2016 CIO FISMA Metrics 2.19, NIST SP 800-50, NIST SP 800-55)
	Effective	**2.3.6.** Provide any additional information on the effectiveness (positive or negative) of the organization's Security and Privacy Training Program that was not noted in the questions above. Based on all testing performed is the Security and Privacy Training Program effective?

3: Detect - Information Security Continuous Monitoring Management – Level 1 Ad-hoc		
Status of ISCM Program Maturity [check one: Met or Not Met]		3.1.1 ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.

* TIGTA determined that IRM met this metric based on its testing; however, the bureau provided the clarifying comment.

3: Detect - Information Security Continuous Monitoring Management – Level 1 Ad-hoc		
	Met	**3.1.1.1.** ISCM stakeholders and their responsibilities have not been fully defined and communicated across the organization. (People)
	Met*	**3.1.1.2.** The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Key personnel do not possess knowledge, skills, and abilities to successfully implement an effective ISCM program. (People) **Comments – TIGTA:** The IRS stated that an assessment it completed for all its information technology organization covered the ISCM program areas.
	Met	**3.1.1.3.** The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions. (People)
	Met	**3.1.1.4.** The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. (People)
	Met	**3.1.1.5.** ISCM processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. (Processes)
	Met	**3.1.1.6.** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. (Processes)
	Met	**3.1.1.7.** The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. (Processes)
	Met	**3.1.1.8.** The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes. (Processes)
	Met	**3.1.1.9.** The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. Use of ISCM technologies in the following areas is ad-hoc. - Patch management - License management - Information management - Software assurance

* TIGTA determined that IRM met the metric based on its testing; however, the bureau provided the clarifying comment.

3: Detect - Information Security Continuous Monitoring Management – Level 1 Ad-hoc		
		- Vulnerability management - Event management - Malware detection - Asset management - Configuration management - Network management - Incident management (Technology) **Comments – TIGTA:** While the IRS is still in the process of implementing its ISCM program required by the OMB, the IRS indicated that the related ISCM activities are currently being performed and are supported by numerous tools within the enterprise.
	Met	**3.1.1.10.** The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. (Technology)

3: Detect - Information Security Continuous Monitoring Management – Level 2 Defined		
Status of ISCM Program Maturity [check one: Met or Not Met]		**3.2.1.** The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide.
	Not Met	**3.2.1.1.** ISCM stakeholders and their responsibilities have been defined and communicated across the organization. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement ISCM activities. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**3.2.1.2.** The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. In addition, the organization has developed a plan for

3: Detect - Information Security Continuous Monitoring Management – Level 2 Defined		
		closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective ISCM program. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**3.2.1.3.** The organization has defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. However, ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**3.2.1.4.** The organization has defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. However, ISCM activities are not consistently integrated with the organization's risk management program. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**3.2.1.5.** ISCM processes have been fully defined for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. However, these processes are inconsistently implemented across the organization. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**3.2.1.6.** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**3.2.1.7.** The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control

3: Detect - Information Security Continuous Monitoring Management – Level 2 Defined		
		ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**3.2.1.8.** The organization has a defined process for capturing lessons learned on the effectiveness of its ISCM program and making necessary improvements. However, lessons learned are not consistently shared across the organization and used to make timely improvements to the ISCM program. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Met	**3.2.1.9.** The organization has identified and fully defined the ISCM technologies it plans to utilize in the following automation areas. In addition, the organization has developed a plan for implementing ISCM technologies in these areas: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. However, the organization has not fully implemented technology is these automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some ISCM activities, the tools may not be interoperable. (Technology) **Comments – TIGTA:** The IRS has defined and documented in its ISCM Program Plan its ISCM technologies related to vulnerability management, asset management, configuration management, and incident management. The remaining domains have yet to be documented.
	Met	**3.2.1.10.** The organization has defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. However, the organization does not consistently implement the technologies that will enable it to manage an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. (Technology)

3: Detect - Information Security Continuous Monitoring Management – Level 3 Consistently Implemented		
Status of ISCM Program Maturity [check one: Met or Not Met]		**3.3.1.** In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions, consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**3.3.1.1.** ISCM stakeholders and their responsibilities have been identified and communicated across the organization, and stakeholders have adequate resources (people, processes, and technology) to effectively implement ISCM activities. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS has defined and documented the ISCM roles and responsibilities in its ISCM Program Plan; however, at this time, not all ISCM stakeholders have adequate resources (people and technology) to implement their defined responsibilities.
	Not Met	**3.3.1.2.** The organization has fully implemented its plans to close any gapes in skills, knowledge, and resources required to successfully implement an ISCM program. Personnel possess the required knowledge, skills, and abilities to effectively implement the organization's ISCM program. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.3.1.3.** ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.

3: Detect - Information Security Continuous Monitoring Management – Level 3 Consistently Implemented		
	Not Met	**3.3.1.4.** ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS has defined and documented how ISCM activities integrate with organizational risk tolerance, the threat environment, and the business/mission requirements within the ISCM Program Plan. However, ISCM activities are not yet consistently integrated with the organization's risk management program
	Not Met	**3.3.1.5.** ISCM processes are consistently performed across the organization in the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**3.3.1.6.** The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**3.3.1.7.** The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting. ISCM measures provide information on the effectiveness of ISCM processes and activities. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.

3: Detect - Information Security Continuous Monitoring Management – Level 3 Consistently Implemented		
		Comments – TIGTA: The IRS has identified and defined the performance measures and requirements within the ISCM Program Plan. The measures are consistently collected, analyzed, and used appropriately across the IRS. However, the metrics providing comprehensive information on the effectiveness of ISCM processes and activities are not collected and analyzed.
	Not Met	**3.3.1.8.** The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The ISCM Program Plan is thoroughly reviewed by all affected stakeholders, and a comprehensive update is preformed to ensure that different processes and activities making up ISCM are updated appropriately. However, consistently sharing lessons learned to make timely improvements to the ISCM program has not occurred.
	Not Met	**3.3.1.9.** The organization has consistently implemented its defined technologies in all of the following ISCM automation areas. ISCM tools are interoperable to the extent practicable. - Patch management - License management - Information management - Software assurance - Vulnerability management - Event management - Malware detection - Asset management - Configuration management - Network management - Incident management. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.

3: Detect - Information Security Continuous Monitoring Management – Level 3 Consistently Implemented		
		Comments – TIGTA: The IRS has not met this metric.
	Not Met	**3.3.1.10.** The organization can produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS stated that it has defined the continuous diagnostics and mitigation tool requirements for inventory automation that will produce an accurate point-in-time inventory, but it has not implemented the tool yet.

3: Detect - Information Security Continuous Monitoring Management – Level 4 Managed and Measurable		
Status of ISCM Program Maturity [check one: Met or Not Met]		**3.4.1.** In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.
	Not Met	**3.4.1.1.** The organization's staff is consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of the organization's ISCM program. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.4.1.2.** Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the ISCM program. (People)

3: Detect - Information Security Continuous Monitoring Management – Level 4 Managed and Measurable		
		Comments – Treasury OIG: We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.4.1.3.** Staff are assigned responsibilities for developing and monitoring ISCM metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the ISCM program. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.4.1.4.** The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing ISCM. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS has not yet implemented the continuous diagnostics and mitigation tool suite needed to generate the data that will assist the IRS in analyzing quantitative and qualitative performance measures across the organization.
	Not Met	**3.4.1.5.** Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.4.1.6.** The organization is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains. (Processes)

3: Detect - Information Security Continuous Monitoring Management – Level 4 Managed and Measurable		
		Comments – Treasury OIG: We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.4.1.7.** The organization uses its ISCM metrics for determining risk response actions including risk acceptance, avoidance/rejection, or transfer. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.4.1.8.** ISCM metrics are reported to the organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.4.1.9.** ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.4.1.10.** The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing ISCM. (Technology)

3: Detect - Information Security Continuous Monitoring Management – Level 4 Managed and Measurable		
		Comments – Treasury OIG: We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.4.1.11.** The organization's ISCM performance measures include data on the implementation of its ISCM program for all sections of the network from the implementation of technologies that provide standard calculations, comparisons, and presentations. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.4.1.12.** The organization utilizes a SIEM tool to collect, maintain, monitor, and analyze IT security information, achieve situational awareness, and manage risk. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.

3: Detect - Information Security Continuous Monitoring Management – Level 5 Optimized		
Status of ISCM Program Maturity [check one: Met or Not Met]		**3.5.1.** In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape. **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.

3: Detect - Information Security Continuous Monitoring Management – Level 5 Optimized		
	Not Met	**3.5.1.1.** The organization's assigned personnel collectively possess a high skill level to perform and update ISCM activities on a near real-time basis to make any changes needed to address ISCM results based on organization risk tolerance, the threat environment, and business/mission requirements. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.5.1.2.** The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity and practices. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.5.1.3.** On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.5.1.4.** The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.5.1.5.** Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format. (Processes)

3: Detect - Information Security Continuous Monitoring Management – Level 5 Optimized		
		Comments – Treasury OIG: We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.5.1.6.** The organization has institutionalized the implementation of advanced cybersecurity technologies in near real-time. (Technology) **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**3.5.1.7.** The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its ISCM program. r. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.

4: Respond – Incident Response – Level 1 Ad-hoc		
Status of Incident Response Program Maturity [check one: Met or Not Met]		**4.1.1.** Incident response program is not formalized and incident response activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines).
	Met	**4.1.1.1.** Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have not been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. (People)
	Met	**4.1.1.2.** The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. Key personnel do not possess the knowledge, skills, and abilities to successfully implement an effective incident response program. (People)

4: Respond – Incident Response – Level 1 Ad-hoc		
	Met	**4.1.1.3.** The organization has not defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. (People)
	Met	**4.1.1.4.** The organization has not defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. (People)
	Met	**4.1.1.5.** Incident response processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting to internal and external stakeholders using standard data elements and impact classifications within timeframes established by US-CERT. (Processes)
	Met	**4.1.1.6.** The organization has not fully defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. (Processes)
	Met	**4.1.1.7.** The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. (Processes)
	Met	**4.1.1.8.** The organization has not defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. (Processes)
	Met	**4.1.1.9.** The organization has not identified and defined the incident response technologies needed in one or more of the following areas and relies on manual/procedural methods in instances where automation would be more effective. Use of incident response technologies in the following areas is ad-hoc. - Web application protections, such as web application firewalls - Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools - Aggregation and analysis, such as security information and event management (SIEM) products - Malware detection, such as anti-virus and antispam software technologies - Information management, such as data loss prevention - File integrity and endpoint and server security tools. (Technology)
	Met	**4.1.1.10.** The organization has not defined how it will meet the defined Trusted Internet Connection (TIC) security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. (Technology)

4: Respond – Incident Response – Level 1 Ad-hoc		
	Met	**4.1.1.11.** The organization has not defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks. (Technology)
	Met	**4.1.1.12.** The organization has not defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. (Technology)

4: Respond – Incident Response – Level 2 Defined		
Status of Incident Response Program Maturity [check one: Met or Not Met]		**4.2.1.** The organizational has formalized its incident response program through the development of comprehensive incident response policies, plans, and procedures consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, incident response policies, plans, and procedures are not consistently implemented organization-wide.
	Met	**4.2.1.1.** Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement incident response activities. Further, the organization has not verified roles and responsibilities as part of incident response testing. (People)
	Met	**4.2.1.2.** The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective incident response program. (People)
	Met	**4.2.1.3.** The organization has defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. However, the organization does not consistently utilize its threat vector taxonomy and incident response information is not always shared with individuals with significant security responsibilities and other stakeholders in a timely manner. (People)
	Not Met	**4.2.1.4.** The organization has defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. However, incident response activities are not consistently integrated with these areas. (People)

4: Respond – Incident Response – Level 2 Defined		
		Comments – Treasury OIG: We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Met	**4.2.1.5.** Incident response processes have been fully defined for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. However, these processes are inconsistently implemented across the organization. (Processes)
	Met	**4.2.1.6.** The organization has fully defined, but not consistently implemented, its processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. (Processes)
	Not Met	**4.2.1.7.** The organization has identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. (Processes) **Comments – Treasury OIG**: We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.2.1.8.** The organization has defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. However, lessons learned are not consistently captured and shared across the organization and used to make timely improvements to security controls and the incident response program. (Processes) **Comments – Treasury OIG**: We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Met	**4.2.1.9.** The organization has identified and fully defined the incident response technologies it plans to utilize in the following areas: - Web application protections, such as web application firewalls - Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools - Aggregation and analysis, such as security information and event management (SIEM) products. However, the organization has not ensured that security and event data are aggregated and correlated from all relevant sources and sensors. - Malware detection such as Anti-virus and antispam software technologies - Information management such as data loss prevention - File integrity and endpoint and server security tools

4: Respond – Incident Response – Level 2 Defined		
		However, the organization has not fully implemented technologies in these areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures. (Technology)
	Met	**4.2.1.10.** The organization has defined how it will meet the defined TIC security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. However, the organization has not ensured that the TIC 2.0 provider and agency managed capabilities are consistently implemented. (Technology)
	Met	**4.2.1.11.** The organization has defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its networks. (Technology)
	Not Met	**4.2.1.12.** The organization has defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. However, the organization has not established, and does not consistently maintain, a comprehensive baseline of network operations and expected data flows for users and systems. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.

4: Respond – Incident Response – Level 3 Consistently Implemented		
Status of Incident Response Program Maturity [check one: Met or Not Met]		**4.3.1.** In addition to the formalization and definition of its incident response program (Level 2), the organization consistently implements its incident response program across the agency, in accordance with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, data supporting metrics on the effectiveness of the incident response program across the organization are not verified, analyzed, and correlated.
	Not Met	**4.3.1.1.** Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined, communicated, and consistently implemented across the organization (Level 2). Further, the organization has verified roles and responsibilities of incident response stakeholders as part of incident response testing. (People)

4: Respond – Incident Response – Level 3 Consistently Implemented		
		Comments – Treasury OIG: We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.3.1.2.** The organization has fully implemented its plans to close any gaps in the skills, knowledge, and resources needed to effectively implement its incident response program. Incident response teams are periodically trained to ensure that knowledge, skills, and abilities are maintained. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The skills gap assessment conducted by the IRS indicated a skills proficiency gap when comparing the IRS CSIRC personnel to the industry standard level of technical proficiency. In addition, the staffing assessment showed 2.6 percent of the requisite staffing was considered unmet. The IRS indicated that these staffing and skills gaps have been addressed by augmenting Federal employees with contractors. TIGTA is currently engaged in an audit of the CSIRC organization and intends to further assess this assertion to ensure that the combined skill set and staffing level is sufficient to protect the IRS network from increasingly sophisticated adversaries.
	Not Met	**4.3.1.3.** The organization consistently utilizes its defined threat vector taxonomy and shares information with individuals with significant security responsibilities and other stakeholders in a timely fashion to support risk-based decision making. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.3.1.4.** Incident response activities are integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.3.1.5.** Incident response processes are consistently implemented across the organization for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. (Processes)

4: Respond – Incident Response – Level 3 Consistently Implemented		
		Comments – Treasury OIG: We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Met	**4.3.1.6.** The organization has ensured that processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents are implemented consistently across the organization. (Processes)
	Not Met	**4.3.1.7.** The organization is consistently capturing qualitative and quantitative performance metrics on the performance of its incident response program. However, the organization has not ensured that the data supporting the metrics was obtained accurately and in a reproducible format or that the data is analyzed and correlated in ways that are effective for risk management. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.3.1.8.** The organization is consistently collecting and capturing lessons learned and incident data on the effectiveness of its incident response program and activities. However, lessons learned may not be shared across the organization in a timely manner and used to make timely improvements to the incident response program and security measures. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.3.1.9.** The rigor, intensity, scope, and results of incident response activities (i.e. preparation, detection, analysis, containment, eradication, and recovery, reporting and post incident) are comparable and predictable across the organization. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.3.1.10.** The organization has consistently implemented its defined incident response technologies in the following areas: - Web application protections, such as web application firewalls - Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools - Aggregation and analysis, such as security information and event management (SIEM) products. The organization ensures that security and event data are aggregated and correlated from all relevant sources and sensors - Malware detection, such as anti-virus and antispam software technologies

4: Respond – Incident Response – Level 3 Consistently Implemented		
		- Information management, such as data loss prevention - File integrity and endpoint and server security tools In addition, the tools are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.3.1.11.** The organization has consistently implemented defined TIC security controls and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Met	**4.3.1.12.** The organization is utilizing DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving their networks. (Technology)
	Not Met	**4.3.1.13.** The organization has fully implemented technologies to develop and maintain a baseline of network operations and expected data flows for users and systems. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.

4: Respond – Incident Response – Level 4 Managed and Measurable		
Status of Incident Response Program Maturity [check one: Met or Not Met]		**4.4.1.** In addition to being consistently implemented (Level 3), incident response activities are repeatable and metrics are used to measure and manage the implementation of the incident response program, achieve situational awareness, and control ongoing risk. In addition, the incident response program adapts to new requirements and government-wide priorities.
	Not Met	**4.4.1.1.** Incident response stakeholders are consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and are collecting, analyzing, and reporting data on the effectiveness of the organization's incident response program. (People)

4: Respond – Incident Response – Level 4 Managed and Measurable		
		Comments – Treasury OIG: We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.4.1.2.** Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the incident response program. (People) **Comments – Treasury OIG**: We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.4.1.3.** Incident response stakeholders are assigned responsibilities for developing and monitoring incident response metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the incident response program. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.4.1.4.** The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing incident response. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.4.1.5.** Data supporting incident response measures and metrics are obtained accurately, consistently, and in a reproducible format. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.4.1.6.** Incident response data, measures, and metrics are analyzed, collected, and presented using standard calculations, comparisons, and presentations. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.4.1.7.** Incident response metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. (Processes)

4: Respond – Incident Response – Level 4 Managed and Measurable		
		Comments – Treasury OIG: We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.4.1.8.** The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.
	Not Met	**4.4.1.9.** The organization's incident response performance measures include data on the implementation of its incident response program for all sections of the network. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met.

4: Respond – Incident Response – Level 5 Optimized		
Status of Incident Response Program Maturity [check one: Met or Not Met]	Not Met	**4.5.1.** In addition to being managed and measurable (Level 4), the organization's incident response program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements, and a changing threat and technology landscape.
	Not Met	**4.5.1.1.** The organization's assigned personnel collectively possess a high skill level to perform and update incident response activities on a near real-time basis to make any changes needed to address incident response results based on organization risk tolerance, the threat environment, and business/mission requirements. (People) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**4.5.1.2.** The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity practices. (Processes)

4: Respond – Incident Response – Level 5 Optimized		
		Comments – Treasury OIG: We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**4.5.1.3.** On a near real-time basis, the organization actively adapts its incident response program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a near real-time manner. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**4.5.1.4.** The incident response program is fully integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**4.5.1.5.** The incident response program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact. (Processes) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**4.5.1.6.** The organization has institutionalized the implementation of advanced incident response technologies in near real-time. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.

4: Respond – Incident Response – Level 5 Optimized		
	Not Met	**4.5.1.7.** The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its incident response program. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.
	Not Met	**4.5.1.8.** The organization uses simulation based technologies to continuously determine the impact of potential security incidents to its IT assets and adjusts incident response processes and security measures accordingly. (Technology) **Comments – Treasury OIG:** We agree with the self-assessment from the bureaus and offices that this metric has not been met. **Comments – TIGTA:** The IRS did not meet this metric.

5: Recover - Contingency Planning		
Status of Contingency Planning Program [check one: Met or Not Met]	Met	**5.1** Has the organization established an enterprise-wide business continuity/disaster recovery program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?
	Not Met	**5.1.1.** Develops and facilitates recovery testing, training, and exercise (TT&E) programs. (FCD1, NIST SP 800-34, NIST SP 800-53) **Comments – Treasury OIG:** TIGTA has a self-identified weakness over the development of a TT&E program for one of the selected systems. (See Prior Year FY 2013 Finding #4 and Prior Year FY 2011 Finding #8)
	Met	**5.1.2.** Incorporates the system's Business Impact Analysis and Business Process Analysis into analysis and strategy toward development of the organization's Continuity of Operations Plan, Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). (NIST SP 800-34)
	Not Met	**5.1.3.** Develops and maintains documented recovery strategies, plans, and procedures at the division, component, and IT infrastructure levels. (NIST SP 800-34)

5: Recover - Contingency Planning		
		Comments – Treasury OIG: FinCEN did not get document approvals of their contingency plan. Mint did not approve and sign the contingency plan during the FISMA year for one of the selected systems. TIGTA did not fully implement contingency planning and testing controls for one system and one prior year system did not have a new operating system integrated into its contingency plan. (See Finding #6, Prior Year FY 2013 Finding #4 and Prior Year FY 2011 Finding #8)
	Met	**5.1.4.** BCP and DRP are in place and ready to be executed upon if necessary. (FCD1, NIST SP 800-34, 2016 CIO FISMA Metrics 5.3, PMC)
	Not Met	**5.1.5.** Tests BCP and DRP for effectiveness and updates plans as necessary. (2016 CIO FISMA Metrics, 5.4) **Comments – Treasury OIG:** DO's annual system contingency plan testing was not consistent with DO requirements for one of the selected systems. FinCEN and TIGTA not perform contingency plan testing for the selected system. (See Finding #6 and Prior Year FY 2013 Finding #4)
	Not Met	**5.1.6.** Tests system-specific contingency plans, in accordance with organizationally defined timeframes, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4) **Comments – Treasury OIG:** DO's annual system contingency plan testing was not consistent with DO requirements for one of the selected systems. FinCEN and TIGTA not perform contingency plan testing for the selected system. (See Finding #6 and Prior Year FY 2013 Finding #4) DO had a self-identified weakness over contingency plan testing for one the selected systems. (See Prior Year – 2015 Self-Identified Weaknesses Section: POA&M #3508)
	Not Met	**5.1.7.** Develops after-action reports that address issues identified during contingency/disaster recovery exercises in order to improve contingency/disaster recovery processes. (FCD1, NIST SP 800-34) **Comments – Treasury OIG:** DO has a self-identified weakness over after-action reports for one of the selected systems. (See Self-Identified Weaknesses Section: POA&M #8420) TIGTA did not perform contingency plan testing for the selected system (See Prior Year FY 2013 Finding #4)
	Met	**5.1.8.** Determines alternate processing and storage sites based upon risk assessments which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized, and are not subject to the same physical and/or cybersecurity risks as the primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-6, CP-7)
	Not Met	**5.1.9.** Conducts backups of information at the user- and system-levels and protects the confidentiality, integrity, and availability of backup information at storage sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-9, NIST CF, PR.IP-4, NARA guidance on information systems security records)

5: Recover - Contingency Planning		
		Comments – Treasury OIG: DO and OIG did not formally conduct or document backup integrity testing for one of the selected systems. (See Finding #6)
	Met	**5.1.10.** Contingency planning that considers supply chain threats.
	Not Effective	**5.1.11.** Provide any additional information on the effectiveness (positive or negative) of the organization's Contingency Planning Program that was not noted in the questions above. Based on all testing performed is the Contingency Planning Program effective?

APPENDIX IV – APPROACH TO SELECTION OF SUBSET OF SYSTEMS

In fiscal year (FY) 2016, a risk-based approach was employed to determine the subset of Department of the Treasury (Treasury) information systems for the FISMA audit. The universe for this subset only included major business applications and general support systems with a security classification of "moderate" or "high." We used the system inventory contained within the Treasury FISMA management tracking tool as the population for this subset. However, we did not validate the completeness and accuracy of the inventory in the Treasury FISMA management tracking tool.

Based on historical trends in Treasury's systems inventory and past reviews, we used a subset size of 25 from the total population of Treasury major applications and general support systems with a security classification of "Moderate" or "High." Based on the systems 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, 2016.
- Whether the system was identified in a previous FISMA audits or evaluations within the past two years.

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

Based on our analysis of Treasury's inventory of information systems as of April 8, 2016, we noted a total of 179 major applications and general support systems with a security classification of moderate or high are contained within the Treasury-wide inventory. The following table provides our analysis of the composition of Treasury's inventory of major applications and general support systems.

	Total	**IRS Financial Systems**	**IRS Non-Financial Systems**	**Non-IRS Financial Systems**	**Non-IRS Non-Financial Systems**
Major Applications	122	2	39	34	47
General Support Systems	57	0	25	1	31
Total	179	2	64	35	78

Consistent with prior performance audits or evaluations, KPMG selected 15 non-IRS systems per the OIG's direction. TIGTA selected 10 IRS systems for a total of 25 systems.

We determined that Major Applications account for 72 percent of the population of the Non-IRS population and General Support Systems account for 28 percent. We further determined that systems designated as "Financial" in the Treasury FISMA management tracking tool, account for 31% of all Non-IRS Major Applications and General Support Systems. Lastly, we determined that 30 percent of the Non-IRS Major Applications and General Support Systems are assigned a FIPS 199 System Impact Level of "High," while 70 percent are assigned a FIPS 199 System Impact Level of "Moderate."

Based on these factors, we determined the following proposed composition for the subset of Non-IRS Major Applications and General Support Systems for the FY 2016 FISMA audit:

Total Selected	15
Total Major Applications	11
Total General Support Systems	4
Total Systems with a FIPS 199 System Impact Level of "High"	5
Total Systems with a FIPS 199 System Impact Level of "Moderate"	10
Total Systems with a FIPS 199 System Impact Level of "Low"	0
Total Systems Designated as Financial	5

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

Bureau	Total Systems	Percentage of Total Non-IRS Population	Total Number of Non-IRS Systems to be Select
BEP	6	5%	1
Fiscal Service	42	37%	4
CDFI Fund	3	3%	1 (See Note 1)
DO	31	27%	4
FinCEN	6	5%	1
Mint	12	11%	1
OCC	7	6%	1
OIG	1	1%	1 (See Note 1)
TIGTA	2	2%	0 (See Note 2)
TTB	3	3%	1 (See Note 1)
Total	113	100%	15

(**Note 1:** Using this methodology initially did not yield a system being selected at these agencies. However, using our risk-based methodology, KPMG elected to select one system for each of these agencies and decrease the number of selected systems for the Fiscal Service and the Mint.)
(**Note 2:** One of the bureau's systems had been selected in FY 2014 and the remaining system is scheduled for decommission at the end of 2016.)

APPENDIX V – GLOSSARY OF TERMS

Acronym	Definition
AC	Access Control
ACIOCS	Associate Chief Information Officer for Cyber Security
AT	Awareness and Training
AU	Audit and Accountability
ATO	Authority to Operate
BCP	Business Continuity Planning
BEP	Bureau of Engraving and Printing
BIA	Business Impact Analysis
BLSR	Baseline Security Requirements
BPD	Bureau of the Public Debt
CA	Security Assessment and Authorization
CAT	Category
CDFI Fund	Community Development Financial Institutions Fund
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CM	Configuration Management
COR	Contracting Officer Representative
CP	Contingency Plan
CSIRC	Computer Security Incident Response Center
CSP	Cloud Service Provider
CSS	Cyber Security Sub-Council
DHS	Department of Homeland Security
DO	Departmental Offices
DRP	Disaster Recovery Plan
FCD	Federal Continuity Directive
FedRAMP	Federal Risk and Authorization Management Program
FinCEN	Financial Crimes Enforcement Network
FIPS	Federal Information Processing Standards
Fiscal Service	The Bureau of the Fiscal Service
FISMA	Federal Information Security Modernization Act of 2002
FMS	Financial Management Service
FY	Fiscal Year
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
IG	Inspector General
IR	Incident Response
IRS	Internal Revenue Service

Acronym	Definition
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
ISSO	Information Systems Security Officer
IT	Information Technology
KPMG	KPMG LLP
Mint	United States Mint
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestone
PL	Planning
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
Rev.	Revision
ROB	Rules of Behavior
SA	System and Services Acquisition
SA&A	Security Assessment and Authorization
SC	System and Communication Protection
SCM	Security Controls Matrix
SIGTARP	Special Inspector General for the Troubled Asset Relief Program
SO	System Owner
SP	Special Publication
SSP	System Security Plan
TARP	Troubled Asset Relief Program
TCSIRC	Treasury Computer Security Incident Response Capability
TD P	Treasury Directive Publication
TIGTA	Treasury Inspector General for Tax Administration
Treasury	Department of the Treasury
TTB	Alcohol and Tobacco Tax and Trade Bureau
TT&E	Test, Training & Exercise
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 2

Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2016
September 28, 2016

THIS PAGE INTENTIONALLY LEFT BLANK

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2016

September 28, 2016

Reference Number: 2016-20-092

.

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

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION – FEDERAL INFORMATION SECURITY MODERNIZATION ACT REPORT FOR FISCAL YEAR 2016

Highlights

Final Report issued on September 28, 2016

Highlights of Reference Number: 2016-20-092 to the Department of the Treasury, Office of the Inspector General, Assistant Inspector General for Audit.

IMPACT ON TAXPAYERS

The Federal Information Security Modernization Act of 2014 (FISMA) focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. As a custodian of taxpayer information, the IRS has an obligation to protect this sensitive information against unauthorized access or loss in accordance with FISMA requirements.

WHY TIGTA DID THE AUDIT

As part of the FISMA legislation, the Offices of Inspector Generals are required to perform an annual independent evaluation of each Federal agency's information security programs and practices. This report presents the results of TIGTA's FISMA evaluation of the IRS for Fiscal Year 2016.

WHAT TIGTA FOUND

The IRS's information security program was generally in alignment with FISMA requirements, but it was not fully effective due to program attributes not yet implemented. Based on the Department of Homeland Security's (DHS) scoring methodology for the Fiscal Year 2016 FISMA evaluation period, three Cybersecurity Framework functions (*Identify*, *Protect*, and *Detect*) were rated as "not effective" and two security functions (*Respond* and *Recover*) were rated as "effective." Within the Cybersecurity Framework functions, three security program areas (*Contractor Systems, Security and Privacy Training,* and *Contingency Planning*) met all the FISMA performance attributes specified by the DHS. The security program area *Risk Management* met most of the performance attributes. Based on the maturity model issued in the Fiscal Year 2016 FISMA evaluation period, the security program area *Incident Response* was rated at level four on a scale of one to five.

However, significant improvements are needed in three program areas that were rated as "not effective" and were missing many performance attributes specified by the DHS for meeting FISMA requirements. These security program areas were *Information Security Continuous Monitoring*, *Configuration Management*, and *Identity and Access Management*.

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

WHAT TIGTA RECOMMENDED

TIGTA does not include recommendations as part of its annual FISMA evaluation and reports on only the level of performance achieved by the IRS using the guidelines issued by the DHS for the applicable FISMA evaluation period.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 28, 2016

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

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Report – Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2016 (Audit # 201620001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Modernization Act[1] (FISMA) evaluation of the Internal Revenue Service (IRS) for Fiscal Year 2016. The FISMA requires Federal agencies to have an annual independent evaluation performed of their information security programs and practices and to report the results of the evaluation to the Office of Management and Budget. Our overall objective was to assess the effectiveness of the IRS's information security program and practices for the period July 1, 2015, to June 30, 2016, and to evaluate the IRS's compliance with the FISMA and related information security policies, procedures, standards, and guidelines.

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

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

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

Table of Contents

Abbreviations

CF	Cybersecurity Framework
CIO	Chief Information Officer
DHS	Department of Homeland Security
FCD1	Federal Continuity Directive 1
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAO	Government Accountability Office
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PMC	President's Management Council
POA&M	Plan of Action and Milestones
SP	Special Publication
TIC	Trusted Internet Connection
TIGTA	Treasury Inspector General for Tax Administration
US-CERT	United States Computer Emergency Readiness Team

Background

The Federal Information Security Modernization Act of 2014,[1] commonly referred to as the FISMA, focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. The FISMA requires Federal agencies to develop, document, and implement an agencywide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. It assigns specific responsibilities to agency heads and Inspectors General in complying with requirements of the FISMA. The FISMA is supported by the Office of Management and Budget (OMB), Department of Homeland Security (DHS), agency security policy, and risk-based standards and guidelines published by the National Institute of Standards and Technology (NIST) related to information security practices.

As a custodian of taxpayer information, the IRS is responsible for implementing appropriate security controls to protect the confidentiality of this sensitive information against unauthorized access or loss in accordance with FISMA requirements.

The Internal Revenue Service (IRS) collects and maintains a significant amount of personal and financial information on each taxpayer. As a custodian of taxpayer information, the IRS is responsible for implementing appropriate security controls to protect the confidentiality of this sensitive information against unauthorized access or loss in accordance with FISMA requirements. Under the FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of the FISMA and related OMB policies and NIST procedures, standards, and guidelines. The FISMA directs Federal agencies to report annually to the OMB Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with the FISMA. The DHS is responsible for the operational aspects of Federal cybersecurity, such as establishing governmentwide incident response and operating the tool to collect FISMA metrics. In addition, the FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to the OMB. The FISMA states that the independent evaluation is to be performed by the agency Inspector General or an independent external auditor as determined by the Inspector

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

General. The OMB uses annual FISMA metrics to assess the implementation of agency information security capabilities and to measure overall program effectiveness in reducing risks.

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

The DHS issued the *Fiscal Year (FY)*[2] *2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*[3] with three significant changes from the prior year.

1) The DHS organized the FY 2016 Inspector General FISMA Reporting Metrics around the five information security functions outlined in the NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework (CF)):[4] *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*. Eight security program areas evaluated in prior FISMA evaluations were aligned within the CF functions and include *Risk Management*, *Contractor Systems*, *Configuration Management*, *Identity and Access Management*, *Information Security Continuous Monitoring*, *Incident Response*, *Security and Privacy Training*, and *Contingency Planning*.

2) The DHS implemented a new scoring methodology. Agencies are allotted points for each CF function area based on their achievement of a five-level scale of maturity. The scale, from lowest to highest, includes: *Ad Hoc* (Level 1), *Defined* (Level 2), *Consistently Implemented* (Level 3), *Managed and Measurable* (Level 4), and *Optimized* (Level 5).

   Agencies with programs that score at or above the *Managed and Measureable* level for a CF function are considered to have "effective" programs within that area in accordance with the definition of effectiveness in NIST Special Publication (SP) 800-53.[5] To score

[2] Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
[3] DHS, *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (Version 1.1.2, Sep. 2016).
[4] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, Feb. 2014).
[5] The Inspector General FISMA metrics leverage NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013, updated Jan. 2015), which defines security control effectiveness as the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies.

at or above the *Managed and Measurable* level, all metrics designated *Defined* and *Consistently Implemented* must be met, plus half or more of metrics designated as *Managed and Measureable* must be met. See Figure 1 for a description of these maturity levels.

3) The DHS, in coordination with other key stakeholders, continued the effort begun in 2015 to develop specific maturity models for various security program areas. In addition to the *Information Security Continuous Monitoring* maturity model, which was included in the FY 2015 Inspector General FISMA Reporting Metric, the FY 2016 Inspector General FISMA Reporting Metrics included a maturity model for the *Incident Response* program area.

Figure 1: DHS Maturity Level Descriptions

Maturity Level	Maturity Level Description
Level 1: ***Ad-Hoc***	For the **Identify**, **Protect**, **and Recover** function areas, has not met at least half of all metrics designated as *Defined*. For the **Detect** and **Respond** function areas, has not met at least half of all metrics designated in the *Ad-Hoc* level.
Level 2: ***Defined***	For the **Identify**, **Protect**, **and Recover** function areas, has met half or greater of all metrics designated as *Defined*. For the **Detect** and **Respond** function areas, has met all metrics designated in the *Ad-Hoc* level and half or greater of the metrics designated in the *Defined* level.
Level 3: ***Consistently Implemented***	For all function areas, met all metrics designated at the *Defined* level and half or greater of the metrics designated at the *Consistently Implemented* level.
Level 4: ***Managed and Measurable***	For all function areas, met all metrics designated in the *Consistently Implemented* level and half or greater of the metrics designated at the *Managed and Measurable* level.
Level 5: **Optimized**	For all function areas, met all metrics designated in the *Managed and Measurable* and *Optimized* levels.

Source: DHS's FY 2016 Inspector General FISMA Reporting Metrics.

This review was performed at, and with information obtained from, the IRS Information Technology organization's Office of Cybersecurity in New Carrollton, Maryland, during the period May through August 2016. This report covers the period from July 1, 2015, through June 30, 2016. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The Information Security Program Is Generally Aligned With the Federal Information Security Modernization Act, but It Is Not Fully Effective Due to Program Attributes Not Yet Implemented

To determine the effectiveness of the IRS's information security program, we evaluated whether the IRS had implemented the attributes that the DHS had specified for each security function area. We based our work, in part, on a representative subset of 10 IRS information systems and the implementation status of key security controls. We also considered the results of TIGTA and Government Accountability Office (GAO) reports issued during the FY 2016 FISMA evaluation period that contained results applicable to the FISMA questions, as listed in Appendix IV.

The IRS has established an information security program that is generally aligned with applicable FISMA requirements, OMB policy and guidance, and the NIST standards and guidelines. However, due to program attributes not yet implemented, the IRS's information security program is not fully effective. Based on the DHS's scoring methodology for the FY 2016 FISMA evaluation period, three CF functions are rated as "not effective" and two security functions are rated as "effective," as shown in Figure 2.

Figure 2: Security Function Effectiveness Based on Implementation of DHS-Specified Attributes

Cybersecurity Framework Security Function	FY 2016 Inspector General FISMA Reporting Metric Domains	Effective Security Function
Identify	• *Risk Management* (met 13 of 16 attributes) • *Contractor Systems* (met all attributes)	No
Protect	• *Configuration Management* (did not meet a majority of attributes) • *Identity and Access Management* (did not meet a majority of attributes) • *Security and Privacy Training* (met all attributes)	No
Detect	• *Information Security Continuous Monitoring* (maturity model level of two)	No
Respond	• *Incident Response* (maturity model level of four)	Yes
Recover	• *Contingency Planning* (met all attributes)	Yes

Source: TIGTA's evaluation of security program attributes as presented in Figure 3, which determined whether security functions were rated "effective" or "not effective."

Some security program areas met all or most attributes

Three security program areas met all performance attributes specified by the DHS.

- ***Contractor Systems***

  The *Contractor Systems* security program area met all performance attributes specified by the DHS, despite being aligned with the *Identify* function that was scored as "not effective."

- ***Security and Privacy Training***

  The *Security and Privacy Training* program area met all performance attributes specified by the DHS, despite being aligned with the *Protect* function that was scored as "not effective."

- ***Contingency Planning***

  The *Contingency Planning* security program area, aligned with the *Recover* function, met all performance attributes specified by the DHS.

One security program area, *Risk Management*, needed improvement on three of 16 attributes.

- ***Risk Management***
  - The IRS did not have sufficient processes in place to ensure that system interconnections in use at the IRS had proper authorization or security agreements. (Metric 1.1.9) During a prior review, TIGTA identified[6] that the IRS did not have sufficient processes in place to ensure that interconnections in use at the IRS had proper authorization or security agreements. After the end of the FY 2016 FISMA evaluation period, the IRS informed us that it had completed all corrective actions. We have not verified those completed corrective actions.
  - Plans of Action and Milestones (POA&M) were not always maintained and reviewed to ensure that they were effective for correcting security weaknesses. (Metric 1.1.13) The IRS informed us that it has taken steps to remediate the POA&M consistency and accuracy issues by centralizing POA&M oversight and validation work under the IRS Enterprise FISMA Services office.
  - The IRS has not yet implemented an insider threat detection and prevention program. (Metric 1.1.16)

[6] TIGTA, Ref. No. 2015-20-087, *Improvements Are Needed to Ensure That External Interconnections Are Identified, Authorized, and Secured* (Sept. 2015).

One security program area, *Incident Response*, was rated at level four on the scale of one to five.

- ***Incident Response***

  The IRS has formalized its incident response program through the development of comprehensive incident response policies, plans, and procedures consistent with FISMA, NIST standards, and OMB guidance. Based on the maturity model issued in the FY 2016 Inspector General FISMA Reporting Metrics for this program area, the IRS's incident response program has achieved a maturity level of four, *Managed and Measurable*, on the scale of one to five. The IRS successfully demonstrated all nine of the level four attributes. However, TIGTA provided a comment on one metric (Metric 4.3.1.2) related to ensuring that key incident response personnel have the appropriate knowledge, skills, and abilities to successfully operate this mission-critical program.

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

Significant improvements are needed in three program areas that were rated as "not effective" and were missing many performance attributes specified by the DHS for meeting FISMA requirements.

- ***Information Security Continuous Monitoring (ISCM)***

  The *Information Security Continuous Monitoring* program area is at a maturity level of two (*Defined*) on the DHS's scale of one to five. The OMB requires Federal agencies to implement an ISCM program that automates asset management and maintains secure configuration of assets in real time. In July 2014, the Department of the Treasury decided to adopt a uniform approach to ISCM across the Treasury and to use the toolset selected by the DHS to meet the program requirements. The DHS is in the process of procuring a standard set of cybersecurity tools and services for use by Federal agencies. This toolset will include sensors that perform automated searches for known cyber flaws and send the results to dashboards that inform system managers in real time of cyber risks that need remediation. When implemented, ISCM is intended to provide security automation in 11 domains: Vulnerability Management, Patch Management, Event Management, Incident Management, Malware Detection, Asset Management, Configuration Management, Network Management, License Management, Information Management, and Software Assurance. The IRS is working in concert with the DHS's implementation phases, and currently performs ISCM-related activities using numerous templates and tools deployed within the enterprise.

- ***Configuration Management***

  The *Configuration Management* program area did not meet the majority of the attributes specified by the DHS. The IRS has established standard baseline configurations for information systems and system components. In addition, the IRS uses automated compliance tools to scan for improper configurations, vulnerabilities, and software flaws. However, deficiencies continue to exist in ensuring baseline configurations are maintained and reported vulnerabilities are corrected timely. In addition, the IRS is still working to expand a standard automated process to deploy operating system patches Service-wide. Eventually, the IRS's *Configuration Management* program area will benefit from the implementation of ISCM, which intends to use automation to produce an accurate inventory of devices and software on the IRS network and to automate configuration management of these devices and software in near real time.

- ***Identity and Access Management***

  The *Identity and Access Management* program area did not meet a majority of the attributes specified by the DHS. The IRS has made progress in implementing use of personal identity verification (PIV) cards for network and remote access in compliance with Homeland Security Presidential Directive 12,[7] but more work is needed to enforce PIV card access to systems and for physical access to IRS facilities.

  Also, the IRS has not consistently implemented controls to ensure that:

  - Users are not granted more access than they need.
  - The use of administrative privileges is tracked and periodically reviewed.
  - Accounts are terminated when no longer required.
  - The use of shared accounts is controlled.

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

The details of our yes/no responses to the FY 2016 Inspector General FISMA Reporting Metrics for the various program areas are contained in Figure 3.

[7] Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, was signed by President Bush on August 27, 2004. This directive established a new standard for issuing and maintaining identification badges for Federal employees and contractors entering Government facilities and accessing computer systems. The intent was to improve security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Agencies are required to use PIV badges (also referred to as SmartID cards) to access computer systems (logical access).

Figure 3: TIGTA's Responses to the DHS's FY 2016 Inspector General FISMA Reporting Metrics

1.0 Identify **Status of Risk Management Program**	**Maturity Model Indicator**	***Risk Management* (*Identify*)**
Yes	Level 2: Defined	**1.1** Has the organization established a risk management program that includes comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?
Yes	Level 2: Defined	**1.1.1** Identifies and maintains an up-to-date system inventory, including organization- and contractor-operated systems, hosting environments, and systems residing in the public, hybrid, or private cloud. (FY 2016 CIO FISMA Metrics 1.1, NIST CF ID.AM.1, NIST SP 800-53: PM-5)[8]
Yes	Level 3: Consistently Implemented	**1.1.2** Develops a risk management function that is demonstrated through the development, implementation, and maintenance of a comprehensive governance structure and organizationwide risk management strategy as described in NIST SP 800-37. (NIST SP 800-39)[9]
Yes	Level 3: Consistently Implemented	**1.1.3** Incorporates mission and business process-related risks into risk-based decisions at the organizational perspective, as described in NIST SP 800-37. (NIST SP 800-39)
Yes	Level 3: Consistently Implemented	**1.1.4** Conducts information system–level risk assessments that integrate risk decisions from the organizational and mission/business process perspectives and take into account threats, vulnerabilities, likelihood, impact, and risks from external parties and common control providers. (NIST SP 800-37, Rev. 1, NIST SP 800-39, NIST SP 800-53: RA-3)
Yes	Level 4: Managed and Measurable	**1.1.5** Provides timely communication of specific risks at the information system, mission/business, and organization-level to appropriate levels of the organization.

[8] DHS and Executive Office of the President of the United States, *FY 2016 CIO FISMA Metrics* (Version 1.00, Oct. 2015). Note: CIO is Chief Information Officer.
[9] NIST, NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (Feb. 2010, updated June 2014). NIST, NIST SP 800-39 Rev. 1, *Managing Information Security Risk: Organization, Mission, and Information System View* (Mar. 2011).

1.0 Identify **Status of Risk Management Program**	**Maturity Model Indicator**	***Risk Management* (*Identify*)**
Yes	Level 3: Consistently Implemented	**1.1.6** Performs comprehensive assessments to categorize information systems in accordance with Federal standards and applicable guidance. (Federal Information Processing Standards (FIPS) 199, FIPS 200, the FISMA, Cybersecurity Sprint, OMB M-16-04, President's Management Council (PMC) cybersecurity assessments)[10]
Yes	Level 2: Defined	**1.1.7** Selects an appropriately tailored set of baseline security controls based on mission/business requirements and policies and develops procedures to employ controls within the information system and its environment of operation.
Yes	Level 3: Consistently Implemented	**1.1.8** Implements the tailored set of baseline security controls as described in 1.1.7.
No	Level 4: Managed and Measurable	**1.1.9** Identifies and manages risks with system interconnections, including through authorizing system interconnections, documenting interface characteristics and security requirements, and maintaining interconnection security agreements. (NIST SP 800-53: CA-3) **TIGTA Comments:** During a prior review, TIGTA identified[11] that the IRS did not have sufficient processes in place to ensure that interconnections in use at the IRS had proper authorization or security agreements. After the end of the FY 2016 FISMA evaluation period, the IRS informed us that it had completed all corrective actions. We have not verified those completed corrective actions.
Yes	Level 3: Consistently Implemented	**1.1.10** Continuously assesses the security controls, including hybrid and shared 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.

[10] NIST, FIPS Pub. 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004). NIST, FIPS Pub. 200, *Minimum Security Requirements for Federal Information and Information Systems* (Mar. 2006). OMB, OMB M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* (Oct. 2015).
[11] TIGTA, Ref. No. 2015-20-087, *Improvements Are Needed to Ensure That External Interconnections Are Identified, Authorized, and Secured* (Sept. 2015).

1.0 Identify **Status of Risk Management Program**	**Maturity Model Indicator**	***Risk Management* (*Identify*)**
Yes	Level 4: Managed and Measurable	**1.1.11** Maintains ongoing information system authorizations 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 (OMB M-14-03, NIST *Supplemental Guidance on Ongoing Authorization*).[12]
Yes	Level 4: Managed and Measurable	**1.1.12** Security authorization package contains system security plan, security assessment report, and POA&M that are prepared and maintained in accordance with government policies. (NIST SP 800-18, NIST SP 800-37)[13]
No	Level 3: Consistently Implemented	**1.1.13** POA&Ms are maintained and reviewed to ensure they are effective for correcting security weaknesses. **TIGTA Comments:** The IRS did not consistently implement its policies and procedures to maintain and review POA&Ms to ensure that they were effective for correcting security weaknesses. • The IRS did not timely create POA&Ms for 24 (52 percent) of 46 weaknesses. The 46 weaknesses were the total number of weaknesses reported during the FY 2016 annual security assessment reviews for the 10 IRS systems we selected for the FY 2016 annual FISMA evaluation of the IRS. • The IRS closed five (40 percent) of 12 POA&Ms without sufficient support that the weaknesses were corrected. The 12 POA&Ms were the total number of POA&Ms closed by the 10 selected systems during the FY 2016 FISMA evaluation period. The IRS subsequently provided adequate documentation for three of the five to support that the weaknesses had been effectively corrected. The documentation subsequently provided by the IRS for the remaining two did not support that the weaknesses had been corrected. • In other audit work during FY 2016, TIGTA identified that 25 of 63 POA&Ms reviewed did not meet IRS POA&M standards to ensure effective and timely resolution of the weakness. We reviewed all 63 POA&Ms that had been prepared for security control weaknesses related to IRS's external file transfer solutions. Of the 25 POA&Ms that did not meet IRS policy standards, 22 POA&Ms did not contain sufficiently defined or detailed milestone actions to ensure timely resolution of the weakness and three POA&Ms did not address the

[12] OMB, OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems* (Nov. 2013). NIST, *Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management* (June 2014).
[13] NIST, NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems* (Feb. 2006).

1.0 Identify **Status of Risk Management Program**	**Maturity Model Indicator**	***Risk Management* (*Identify*)**
		weakness. The scheduled completion date for eight of the 22 POA&Ms lacking sufficient milestone actions had passed with the weaknesses remaining uncorrected. • The IRS Enterprise FISMA Dashboard reported that, as of June 30, 2016, 14 percent of the IRS's total open POA&Ms have passed scheduled completion dates and therefore are in late status. The IRS's goal was to have less than 10 percent of its open POA&Ms in late status. This indicates that the IRS has not yet consistently implemented its policies and procedures to ensure timely and effective correcting of security weaknesses. The IRS informed us that it has taken steps to remediate the POA&M consistency and accuracy issues by centralizing POA&M oversight and validation work under the IRS Enterprise FISMA Services office.
Yes	Level 4: Managed and Measurable	**1.1.14** Centrally tracks, maintains, and independently reviews/validates POA&M activities at least quarterly. (NIST SP 800-53: CA-5, OMB M-04-25)[14]
Yes	Level 4: Managed and Measurable	**1.1.15** 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.
No	Level 3: Consistently Implemented	**1.1.16** Implemented an insider threat detection and prevention program, including the development of comprehensive policies, procedures, guidance, and governance structures, in accordance with Executive Order 13587 and the National Insider Threat Policy.[15] (PMC, NIST SP 800-53: PM-12) **TIGTA Comments:** The IRS does not have an insider threat detection and prevention program. Although the IRS does not own or operate any classified national security information systems subject to Executive Order 13587, its own policy requires that it implement an insider threat program. In addition, the IRS is waiting for the Department of the Treasury, which is subject to Executive Order 13587, to release its Insider Threat Program to assist in identifying potential insider threats and establish reporting requirements and thresholds for the Treasury bureaus. However, the IRS indicated that its current resources and budget do not allow for a full-scale implementation of

[14] OMB, OMB M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* (Aug. 2004).
[15] Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (Oct. 2011). The White House, Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 2012).

1.0 Identify **Status of Risk Management Program**	**Maturity Model Indicator**	***Risk Management* (*Identify*)**
		an insider threat program until 2027. As such, the IRS has taken a risk-based decision to not meet this policy requirement at this time.
Not Effective		**1.1.17** Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Based on all testing performed, is the risk management program effective? **TIGTA Comments:** According to the new scoring methodology implemented by the DHS for the FY 2016 Inspector General FISMA Reporting Metrics, program areas must have met all attributes labeled as *Defined* and *Consistently Implemented* and half or more of the attributes labeled as *Managed and Measurable* to have an effective program. This program area did not meet all attributes at the level 3 *Consistently Implemented*.

1.0 Identify **Status of Contractor Systems Program**	**Maturity Model Indicator**	***Contractor Systems* (*Identify*)**
Yes	Level 2: Defined	**1.2** Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including other government agencies, managed hosting environments, and systems and services residing in a cloud external to the organization that is inclusive of policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?
Yes	Level 3: Consistently Implemented	**1.2.1** Establishes and implements a process to ensure that contracts/statements of work/solicitations for systems and services, include appropriate information security and privacy requirements and material disclosures, Federal Acquisition Regulation clauses, and clauses on protection, detection, and reporting of information. (Federal Acquisition Regulation Case 2007-004, Common Security Configurations,[16] Federal Acquisition Regulation Sections 24.104, 39.101, 39.105, 39.106, and 52.239-1, PMC, FY 2016 CIO FISMA Metrics 1.8, NIST SP 800-53: SA-4, Federal Risk and Authorization Management Program standard contract clauses, Cloud Computing Contract Best Practices) **TIGTA Comments:** The IRS has recently established a process for reviewing contracts for appropriate security clauses. In November 2015, the

[16] Federal Acquisition Regulation, FAR Case 2007-004, Common Security Configurations (Mar. 2008)

1.0 Identify **Status of Contractor Systems Program**	**Maturity Model Indicator**	***Contractor Systems* (*Identify*)**
		IRS instructed its contracting officers to conduct a 100 percent review of all new and existing information technology and service contracts to ensure that all applicable security clauses were included. In June 2016, the IRS instructed its contracting officers to implement codes in the IRS procurement system to indicate whether the contract had been reviewed and includes security clauses if appropriate. The IRS Procurement staff stated that the IRS intends to begin reviewing the progress made to ensure that all contracts include appropriate security clauses on a quarterly basis. As of June 30, 2016, the IRS reported the following results. • 808 contracts that have been reviewed contain appropriate security clauses. • 2,095 contracts that have been reviewed do not require security clauses. • 842 contracts that have been reviewed do not yet contain appropriate security clauses. • 1,844 contracts have not yet been reviewed. (All are active contracts with signed dates on or after July 1, 2016.)
Yes	Level 3: Consistently Implemented	**1.2.2** Specifies within appropriate agreements how information security performance is measured, reported, and monitored on contractor- or other entity-operated systems. (CIO and Chief Acquisition Officers Councils' Best Practices Guide for Acquiring IT As a Service, NIST SP 800-35)[17]
Yes	Level 3: Consistently Implemented	**1.2.3** Obtains sufficient assurance that the security controls of systems operated on the organization's behalf by contractors or other entities and services provided on the organization's behalf meet FISMA requirements, OMB policy, and applicable NIST guidelines. (NIST SP 800-53: CA-2 and SA-9)
Effective		**1.2.4** Provide any additional information on the effectiveness (positive or negative) of the organization's contractor systems program that was not noted in the questions above. Based on all testing performed, is the contractor systems program effective?

[17] CIO and Chief Acquisition Officers Councils, *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service* (Feb. 2012). Note: IT is Information Technology.

2.0 Protect **Status of Configuration Management Program**	**Maturity Model Indicator**	***Configuration Management* (*Protect*)**
Yes	Level 2: Defined	**2.1** Has the organization established a configuration management program that is inclusive of comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **TIGTA Comments:** The IRS established a configuration management program. However, we did note that it had not updated its configuration management policy and procedures within three years or when a significant change occurred as required.
No	Level 2: Defined	**2.1.1** Develops and maintains an up-to-date inventory of the hardware assets (*i.e.*, endpoints, mobile assets, network devices, input/output assets, and SMART/NEST devices) connected to the organization's network with the detailed information necessary for tracking and reporting. (NIST CF ID.AM-1, FY 2016 CIO FISMA Metrics 1.5 and 3.17, NIST SP 800-53: CM-8) **TIGTA Comments:** Although the IRS has implemented an asset management solution as its official inventory solution, during the FY 2016 FISMA evaluation period, TIGTA reported the inventory being inaccurate and/or incomplete. Also, three of the 10 systems selected for the FISMA evaluation reported in their System Security Plans that NIST SP 800-53 security control CM-8, Information System Component Inventory, was not fully in place.
No	Level 2: Defined	**2.1.2** Develops and maintains an up-to-date inventory of software platforms and applications used within the organization and with the detailed information necessary for tracking and reporting. (NIST SP 800-53: CM-8, NIST CF ID.AM-2) **TIGTA Comments:** Information deemed necessary for effective information system component inventories includes software license information. Within the last three years, TIGTA completed three audits relating to software license management and reported that the IRS was not adequately performing software license management, was not adhering to Federal requirements, and did not have specialized software license tools for developing and maintaining an enterprisewide inventory. The IRS indicated that it is in the process of deploying a commercial-off-the-shelf software asset management framework to track and maintain its inventory of software in use across the IRS, expected to be completed by October 15, 2017.

2.0 Protect **Status of Configuration Management Program**	**Maturity Model Indicator**	***Configuration Management* (*Protect*)**
No	Level 3: Consistently Implemented	**2.1.3** Implements baseline configurations for information technology systems that are developed and maintained in accordance with documented procedures. (NIST SP 800-53: CM-2, NIST CF PR.IP-1) **TIGTA Comments:** The IRS has established and documented standard baseline configurations for its information technology systems; however, the IRS has not always maintained the configurations in accordance with its documented procedures. Four of the 10 systems selected for the FISMA evaluation reported in their System Security Plans that NIST SP 800-53 security control CM-2, Baseline Configuration, was not fully in place.
No	Level 3: Consistently Implemented	**2.1.4** Implements and maintains standard security settings (also referred to as security configuration checklists or hardening guides) for information technology systems in accordance with documented procedures. (NIST SP 800-53: CM-6, FY 2016 CIO FISMA Metrics 2.3) **TIGTA Comments:** The IRS has not always implemented and maintained standard security settings in accordance with documented procedures. All 10 System Security Plans of the systems selected for the FISMA evaluation showed that some or all of the required configuration settings for servers within their respective authorization boundaries were not implemented in accordance with IRS policy.
No	Level 4: Managed and Measurable	**2.1.5** Assesses configuration change control processes, including processes to manage configuration deviations across the enterprise that are implemented and maintained. (NIST SP 800-53: CM-3, NIST CF PR.IP-3) **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. The GAO reported that the IRS did not document requests and approvals for all changes to the mainframe production system. TIGTA identified that the IRS did not always correct configuration vulnerabilities or apply patches on servers within the established time frames. Also, IRS security change management process and procedure documents are outdated and currently in the IRS's review process. Lastly, three of the 10 systems reported in their System Security Plans that NIST SP 800-53 security control CM-3, Configuration Change Control, was not fully in place.
Yes	Level 4: Managed and Measurable	**2.1.6** Identifies and documents deviations from configuration settings. Acceptable deviations are approved with business justification and risk acceptance. Where appropriate, automated means that enforce and redeploy configuration settings to systems at regularly scheduled intervals are deployed, while evidence of deviations is also maintained. (NIST SP 800-53: CM-6, Center for Internet Security Controls 3.7)

2.0 Protect **Status of Configuration Management Program**	**Maturity Model Indicator**	***Configuration Management* (*Protect*)**
No	Level 4: Managed and Measurable	**2.1.7** Implemented Security Content Automation Protocol certified software assessing (scanning) capabilities against all systems on the network to assess both code-based and configuration-based vulnerabilities in accordance with risk management decisions. (NIST SP 800-53: RA-5 and SI-2, FY 2016 CIO FISMA Metrics 2.2, Center for Internet Security Controls 4.1) **TIGTA Comments:** The IRS has not implemented Security Content Automation Protocol certified software assessing (scanning) capabilities against all systems on the network. In addition, the 10 systems selected for review reported in their System Security Plans that eight and four systems, respectively, did not have NIST SP 800-53 security controls RA-5, Vulnerability Management, and SI-2, Flaw Remediation, fully in place.
No	Level 3: Consistently Implemented	**2.1.8** Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST SP 800-53: CM-4, CM-6, RA-5, and SI-2) **TIGTA Comments:** The IRS has not yet fully implemented configuration-related vulnerability scanning tools and processes on all systems to ensure timely remediation of scan result deviations. During the FY 2016 FISMA evaluation period, TIGTA reported that the IRS was not timely remediating high-risk vulnerabilities and POA&Ms did not meet standards. Also, a significant number (six, eight, and four systems, respectively) of the 10 systems selected for review reported in their System Security Plans that they did not have NIST SP 800-53 security controls CM-6, RA-5, and SI-2 fully in place.
No	Level 4: Managed and Measurable	**2.1.9** Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3 and SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01) **TIGTA Comments:** The IRS has developed a comprehensive patch management standard operating procedure. However, the IRS indicated that a patch implementation standard operating procedure is currently being developed to include the tools that will be used for patch installation, standardize processes for common patching activities, and to ensure that patch deployment timelines meet the IRS policy. Both TIGTA and the GAO continue to report on weaknesses in the IRS patch management process. For instance, the IRS did not always ensure that critical security patch updates were applied to its systems in a timely manner. Also, the IRS continues to run outdated and unsupported software on its systems.

2.0 Protect **Status of Configuration Management Program**	**Maturity Model Indicator**	***Configuration Management* (*Protect*)**
Not Effective		**2.1.10** Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above. Based on all testing performed, is the configuration management program effective? **TIGTA Comments:** According to the new scoring methodology implemented by the DHS for the FY 2016 Inspector General FISMA Reporting Metrics, program areas must have met all attributes labeled as *Defined* and *Consistently Implemented* and half or more of the attributes labeled as *Managed and Measurable* to have an effective program. This program area did not meet all attributes at the level 2 *Defined*.

2.0 Protect **Status of Identity and Access Management Program**	**Maturity Model Indicator**	***Identity and Access Management* (*Protect*)**
Yes	Level 2: Defined	**2.2** Has the organization established an identity and access management program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?
No	Level 3: Consistently Implemented	**2.2.1** Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements, participate in required training prior to being granted access, and recertify access agreements on a predetermined interval. (NIST SP 800-53: PL-4 and PS-6) **TIGTA Comments:** While the IRS has an enterprisewide process to register and grant users access to information systems, during the FY 2016 FISMA evaluation period, TIGTA reported that an IRS office did not use the process to register and grant users access to a system, and therefore appropriate access agreements were not signed. In addition, the System Security Plans for the 10 systems selected for review also reported occurrences of access granted to systems without proper authorization.

2.0 Protect **Status of Identity and Access Management Program**	**Maturity Model Indicator**	***Identity and Access Management* (*Protect*)**
No	Level 3: Consistently Implemented	**2.2.2** Ensures that all users are only granted access based on least privilege and separation-of-duties principles. **TIGTA Comments:** TIGTA identified 27 systems that did not support that users were granted access based on least privilege, due to incomplete, inaccurate, and outdated documentation for user access. In addition, TIGTA reported that the IRS's standard process to annually recertify that the users have a continued business need for access to the system was not used for users with elevated privileges. Also, during the FY 2016 FISMA evaluation period, the GAO identified users that the IRS allowed to have excessive privileges to systems. Lastly, the system security plans for the 10 IRS systems selected for review reported that 50 percent did not have NIST SP 800-53 security control AC-5, Separation of Duties, fully in place and 50 percent did not have NIST SP 800-53 security control AC-6, Least Privilege, fully in place.
Yes	Level 3: Consistently Implemented	**2.2.3** Distinguishes hardware assets that have user accounts (*e.g.*, desktops, laptops, servers) from those without user accounts (*e.g.*, networking devices, such as load balancers and intrusion detection/prevention systems, and other input/output devices such as faxes and Internet Protocol phones).
No	Level 3: Consistently Implemented	**2.2.4** Implements PIV for physical access in accordance with government policies. (Homeland Security Presidential Directive 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11)[18] **TIGTA Comments:** The IRS has implemented the required Homeland Security Presidential Directive 12 and FIPS 201 access control systems in only 61 percent of the buildings that require them. The projected completion of the remaining 39 percent of the buildings is in FY 2019 (if funded).

[18] NIST, FIPS Pub. 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors* (Aug. 2013). Note: FIPS 201-2 superseded FIPS 201 (FIPS 201-1). OMB, OMB M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 2005). OMB, OMB M-07-06, *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials* (Jan. 2007). OMB, OMB M-08-01, *HSPD-12 Implementation Status* (Oct. 2007). OMB, OMB M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors* (Feb. 2011).

2.0 Protect **Status of Identity and Access Management Program**	**Maturity Model Indicator**	***Identity and Access Management (Protect)***
No	Level 3: Consistently Implemented	**2.2.5** Implements PIV or a NIST Level of Assurance 4 credential for logical access by all privileged users (system, network, database administrators, and others responsible for system/application control, monitoring, or administration functions). (Cybersecurity Sprint, OMB M-16-04, PMC, FY 2016 CIO FISMA Metrics 2.5.1) **TIGTA Comments:** The IRS reported that all privileged users are required to log on to the IRS network with PIV cards. Work is ongoing to ensure privileged access to systems using PIV cards and to replace aging systems and retire software that do not support PIV card access. As of June 29, 2016, the IRS had enabled a privileged access solution that allowed 1,901 (62 percent) of 3,084 privileged users to log on to privileged accounts using PIV cards.
Yes	Level 3: Consistently Implemented	**2.2.6** Enforces PIV or a NIST Level of Assurance 4 credential for logical access for at least 85 percent of nonprivileged users. (Cybersecurity Sprint, OMB M-16-04, PMC, FY 2016 CIO FISMA Metrics 2.4.1)
No	Level 4: Managed and Measurable	**2.2.7** Tracks and controls the use of administrative privileges and ensures that these privileges are periodically reviewed and adjusted in accordance with organizationally defined time frames. (FY 2016 CIO FISMA Metrics 2.9 and 2.10, OMB M-16-04, Center for Internet Security Controls 5.2) **TIGTA Comments:** During the FY 2016 FISMA evaluation period, TIGTA and the GAO identified deficiencies in this control, reporting that the IRS had not properly limited the use of administrative privileges or ensured that these privileges were periodically reviewed and adjusted in accordance with policy. The IRS's current system to review privileged access does not require revalidation on a semi-annual basis in accordance with IRS policy. The IRS indicated it is working to correct this deficiency.
No	Level 4: Managed and Measurable	**2.2.8** Ensures that accounts are terminated or deactivated once access is no longer required or after a period of inactivity, according to organizational policy. **TIGTA Comments:** During the FY 2016 FISMA evaluation period, TIGTA and the GAO identified systems that do not have controls in place to ensure that accounts are terminated or deactivated once access is no longer needed.
No	Level 3: Consistently Implemented	**2.2.9** Identifies, limits, and controls the use of shared accounts. (NIST SP 800-53: AC-2) **TIGTA Comments:** During the FY 2016 FISMA evaluation period, TIGTA and the GAO identified improper use of shared accounts; for example, use of generic administrator accounts and passwords.

2.0 Protect **Status of Identity and Access Management Program**	**Maturity Model Indicator**	***Identity and Access Management* (*Protect*)**
Yes	Level 3: Consistently Implemented	**2.2.10** All users are uniquely identified and authenticated for remote access using Strong Authentication (multi-factor), including PIV. (NIST SP 800-46: Section 4.2 and Section 5.1, NIST SP 800-63)[19]
Yes	Level 3: Consistently Implemented	**2.2.11** Protects against and detects unauthorized remote access connections or subversion of authorized remote access connections, including through remote scanning of host devices. (Center for Internet Security Controls 12.7 and 12.8, FY 2016 CIO FISMA Metrics 2.17.3, 2.17.4, 3.11, and 3.11.1)
Yes	Level 4: Managed and Measurable	**2.2.12** Remote access sessions are timed out after 30 minutes of inactivity, requiring user reauthentication, consistent with OMB M-07-16.[20]
Yes	Level 3: Consistently Implemented	**2.2.13** Enforces a limit of consecutive invalid remote access logon attempts and automatically locks the account or delays the next logon prompt. (NIST SP 800-53: AC-7)
Yes	Level 3: Consistently Implemented	**2.2.14** Implements a risk-based approach to ensure that all agency public websites and services are accessible through a secure connection through the use and enforcement of https and strict transport security. (OMB M-15-13)[21]
Not Effective		**2.2.15** Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Based on all testing performed, is the identity and access management program effective? **TIGTA Comments:** According to the new scoring methodology implemented by the DHS for the FY 2016 Inspector General FISMA Reporting Metrics, program areas must have met all attributes labeled as *Defined* and *Consistently Implemented* and half or more of the attributes labeled as *Managed and Measurable* to have an effective program. This program area did not meet all attributes at the level 3 *Consistently Implemented*.

[19] NIST, NIST SP 800-46 Rev. 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016). NIST, NIST SP 800-63-2, *Electronic Authentication Guideline* (Aug. 2013). NIST SP 800-63-2 supersedes NIST SP 800-63-1.
[20] OMB, OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 2007).
[21] OMB, OMB M-15-13, *Policy to Require Secure Connections across Federal Websites and Web Services* (June 2015).

2.0 Protect **Status of Security and Privacy Training Program**	**Maturity Model Indicator**	***Security and Privacy Training (Protect)***
Yes	Level 2: Defined	**2.3** Has the organization established a security and privacy awareness and training program, including comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?
Yes	Level 3: Consistently Implemented	**2.3.1** Develops training material for security and privacy awareness training containing appropriate content for the organization, including anti-phishing, malware defense, social engineering, and insider threat topics. (NIST SP 800-50, NIST SP 800-53: AR-5, OMB M-15-01, FY 2016 CIO FISMA Metrics, PMC, National Insider Threat Policy)[22] **TIGTA Comments:** The IRS's information systems security awareness training includes basic appropriate content, but it should be further developed to meet the specific requirements relating to insider threats. The IRS said that it plans to update information systems security training for FY 2017.
Yes	Level 3: Consistently Implemented	**2.3.2** Evaluates the skills of individuals with significant security and privacy responsibilities and provides additional security and privacy training content or implements human capital strategies to close identified gaps. (NIST SP 800-50)
Yes	Level 3: Consistently Implemented	**2.3.3** Identifies and tracks the status of security and privacy awareness training for all information system users (including employees, contractors, and other organization users) requiring security awareness training with appropriate internal processes to detect and correct deficiencies. (NIST SP 800-53: AT-2)
Yes	Level 3: Consistently Implemented	**2.3.4** Identifies and tracks the status of specialized security and privacy training for all personnel (including employees, contractors, and other organization users) with significant information security and privacy responsibilities requiring specialized training.
Yes	Level 4: Managed and Measurable	**2.3.5** Measures the effectiveness of its security and privacy awareness and training programs, including through social engineering and phishing exercises. (PMC, FY 2016 CIO FISMA Metrics 2.19, NIST SP 800-50, NIST SP 800-55)[23]

[22] NIST, NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (Oct. 2003). OMB, OMB M-15-01, *Fiscal Year 2014–2015 Guidance on Improving Federal Information Security and Privacy Management Practices* (Oct. 2014).
[23] NIST, NIST SP 800-55 Rev. 1, *Performance Measurement Guide for Information Security* (July 2008).

2.0 Protect **Status of Security and Privacy Training Program**	**Maturity Model Indicator**	***Security and Privacy Training (Protect)***
Effective		**2.3.6** Provide any additional information on the effectiveness (positive or negative) of the organization's security and privacy training program that was not noted in the questions above. Based on all testing performed, is the security and privacy training program effective?

3.0 Detect **Status of Information Security Continuous Monitoring Program**	**Maturity Model Indicator**	***Information Security Continuous Monitoring***
	Level 1: Ad-Hoc	**Definition** **3.1.1 (Definition)** The ISCM program is not formalized and ISCM activities are performed in a reactive manner, resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, NIST SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.[24]
Met	Level 1: Ad-Hoc	**People** **3.1.1.1 (People)** ISCM stakeholders and their responsibilities have not been fully defined and communicated across the organization.
Met	Level 1: Ad-Hoc	**3.1.1.2 (People)** The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Key personnel do not possess knowledge, skills, and abilities to successfully implement an effective ISCM program. **TIGTA Comments:** The IRS stated that an assessment it completed for all its information technology organization covered the ISCM program areas.
Met	Level 1: Ad-Hoc	**3.1.1.3 (People)** The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions.

[24] NIST, NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (Sept. 2011).

3.0 Detect **Status of Information Security Continuous Monitoring Program**	**Maturity Model Indicator**	***Information Security Continuous Monitoring***
Met	Level 1: Ad-Hoc	**3.1.1.4 (People)** The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements.
Met	Level 1: Ad-Hoc	**Processes** **3.1.1.5 (Processes)** ISCM processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security-related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program.
Met	Level 1: Ad-Hoc	**3.1.1.6 (Processes)** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used.
Met	Level 1: Ad-Hoc	**3.1.1.7 (Processes)** The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk.
Met	Level 1: Ad-Hoc	**3.1.1.8 (Processes)** The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes.
Met	Level 1: Ad-Hoc	**Technology** **3.1.1.9 (Technology)** The organization has not identified and defined the ISCM technologies needed in one of more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. Use of ISCM technologies in the following areas is ad-hoc. • Patch management • License management • Information management • Software assurance • Vulnerability management • Event management • Malware detection • Asset management • Configuration management

3.0 Detect **Status of Information Security Continuous Monitoring Program**	**Maturity Model Indicator**	***Information Security Continuous Monitoring***
		• Network management • Incident management **TIGTA Comments:** While the IRS is still in the process of implementing its ISCM program required by the OMB, the IRS indicated that the related ISCM activities are currently being performed and are supported by numerous tools within the enterprise.
Met	Level 1: Ad-Hoc	**3.1.1.10 (Technology)** The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.
	Level 2: Defined	**Definition** **3.2.1 (Definition)** The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, NIST SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organizationwide.
Met	Level 2: Defined	**People** **3.2.1.1 (People)** ISCM stakeholders and their responsibilities have been defined and communicated across the organization. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement ISCM activities.
Not Met	Level 2: Defined	**3.2.1.2 (People)** The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective ISCM program. **TIGTA Comments:** The IRS did not identify skill and requirement gaps (if any) to effectively implement an ISCM program in accordance with OMB M-14-03.
Met	Level 2: Defined	**3.2.1.3 (People)** The organization has defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. However, ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions.

3.0 Detect **Status of Information Security Continuous Monitoring Program**	**Maturity Model Indicator**	***Information Security Continuous Monitoring***
Met	Level 2: Defined	**3.2.1.4 (People)** The organization has defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. However, ISCM activities are not consistently integrated with the organization's risk management program.
Met	Level 2: Defined	**Processes** **3.2.1.5 (Processes)** ISCM processes have been fully defined for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security-related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. However, these processes are inconsistently implemented across the organization.
Met	Level 2: Defined	**3.2.1.6 (Processes)** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used.
Met	Level 2: Defined	**3.2.1.7 (Processes)** The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization.
Met	Level 2: Defined	**3.2.1.8 (Processes)** The organization has a defined process for capturing lessons learned on the effectiveness of its ISCM program and making necessary improvements. However, lessons learned are not consistently shared across the organization and used to make timely improvements to the ISCM program.

3.0 Detect **Status of Information Security Continuous Monitoring Program**	**Maturity Model Indicator**	***Information Security Continuous Monitoring***
Not Met	Level 2: Defined	**Technology** **3.2.1.9 (Technology)** The organization has identified and fully defined the ISCM technologies it plans to utilize in the following automation areas. In addition, the organization has developed a plan for implementing ISCM technologies in these areas: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. However, the organization has not fully implemented technology is these automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some ISCM activities, the tools may not be interoperable. **TIGTA Comments:** The IRS has defined and documented in its ISCM Program Plan its ISCM technologies related to vulnerability management, asset management, configuration management, and incident management. The remaining domains have yet to be documented.
Met	Level 2: Defined	**3.2.1.10 (Technology)** The organization has defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. However, the organization does not consistently implement the technologies that will enable it to manage an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.
	Level 3: Consistently Implemented	**Definition** **3.3.1 (Definition)** In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions consistent with NIST SP 800-53, NIST SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.

3.0 Detect **Status of Information Security Continuous Monitoring Program**	**Maturity Model Indicator**	***Information Security Continuous Monitoring***
Not Met	Level 3: Consistently Implemented	**People** **3.3.1.1 (People)** ISCM stakeholders and their responsibilities have been identified and communicated across the organization, and stakeholders have adequate resources (people, processes, and technology) to effectively implement ISCM activities. **TIGTA Comments:** The IRS has defined and documented the ISCM roles and responsibilities in its ISCM Program Plan; however, at this time, not all ISCM stakeholders have adequate resources (people and technology) to implement their defined responsibilities.
Not Met	Level 3: Consistently Implemented	**3.3.1.2 (People)** The organization has fully implemented its plans to close any gaps in skills, knowledge, and resources required to successfully implement an ISCM program. Personnel possess the required knowledge, skills, and abilities to effectively implement the organization's ISCM program. **TIGTA Comments:** The IRS did not meet this metric.
Met	Level 3: Consistently Implemented	**3.3.1.3 (People)** ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations.
Not Met	Level 3: Consistently Implemented	**3.3.1.4 (People)** ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements. **TIGTA Comments:** The IRS has defined and documented how ISCM activities integrate with organizational risk tolerance, the threat environment, and the business/mission requirements within the ISCM Program Plan. However, ISCM activities are not yet consistently integrated with the organization's risk management program.
Met	Level 3: Consistently Implemented	**Processes** **3.3.1.5 (Processes)** ISCM processes are consistently performed across the organization in the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security-related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program.

3.0 Detect **Status of Information Security Continuous Monitoring Program**	**Maturity Model Indicator**	***Information Security Continuous Monitoring***
Met	Level 3: Consistently Implemented	**3.3.1.6 (Processes)** The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization.
Not Met	Level 3: Consistently Implemented	**3.3.1.7 (Processes)** The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting. ISCM measures provide information on the effectiveness of ISCM processes and activities. **TIGTA Comments:** The IRS has identified and defined the performance measures and requirements within the ISCM Program Plan. The measures are consistently collected, analyzed, and used appropriately across the IRS. However, the metrics providing comprehensive information on the effectiveness of ISCM processes and activities are not collected and analyzed.
Not Met	Level 3: Consistently Implemented	**3.3.1.8 (Processes)** The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes. **TIGTA Comments:** The ISCM Program Plan is thoroughly reviewed by all affected stakeholders, and a comprehensive update is preformed to ensure that different processes and activities making up ISCM are updated appropriately. However, consistently sharing lessons learned to make timely improvements to the ISCM program has not occurred.
Not Met	Level 3: Consistently Implemented	**Technology** **3.3.1.9 (Technology)** The organization has consistently implemented its defined technologies in all of the following ISCM automation areas. ISCM tools are interoperable to the extent practicable. • Patch management • License management • Information management • Software assurance • Vulnerability management • Event management • Malware detection • Asset management • Configuration management • Network management

3.0 Detect **Status of Information Security Continuous Monitoring Program**	**Maturity Model Indicator**	***Information Security Continuous Monitoring***
		• Incident management **TIGTA Comments:** The IRS has not met this metric.
Not Met	Level 3: Consistently Implemented	**3.3.1.10 (Technology)** The organization can produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **TIGTA Comments:** The IRS stated that it has defined the continuous diagnostics and mitigation tool requirements for inventory automation that will produce an accurate point-in-time inventory, but it has not implemented the tool yet.
	Level 4: Managed and Measurable	**Definition** **3.4.1 (Definition)** In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.
Not Met	Level 4: Managed and Measurable	**People** **3.4.1.1 (People)** The organization's staff is consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of the organization's ISCM program. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 4: Managed and Measurable	**3.4.1.2 (People)** Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the ISCM program. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 4: Managed and Measurable	**3.4.1.3 (People)** Staff are assigned responsibilities for developing and monitoring ISCM metrics as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the ISCM program. **TIGTA Comments:** The IRS did not meet this metric.

3.0 Detect **Status of Information Security Continuous Monitoring Program**	**Maturity Model Indicator**	***Information Security Continuous Monitoring***
Not Met	Level 4: Managed and Measurable	**Processes** **3.4.1.4 (Processes)** The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing ISCM. **TIGTA Comments:** The IRS has not yet implemented the continuous diagnostics and mitigation tool suite needed to generate the data that will assist the IRS in analyzing quantitative and qualitative performance measures across the organization.
Not Met	Level 4: Managed and Measurable	**3.4.1.5 (Processes)** Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 4: Managed and Measurable	**3.4.1.6 (Processes)** The organization is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 4: Managed and Measurable	**3.4.1.7 (Processes)** The organization uses its ISCM metrics for determining risk response actions including risk acceptance, avoidance/rejection, or transfer. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 4: Managed and Measurable	**3.4.1.8 (Processes)** ISCM metrics are reported to the organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 4: Managed and Measurable	**3.4.1.9 (Processes)** ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (*i.e.*, System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis. **TIGTA Comments:** The IRS did not meet this metric.

3.0 Detect **Status of Information Security Continuous Monitoring Program**	**Maturity Model Indicator**	***Information Security Continuous Monitoring***
Not Met	Level 4: Managed and Measurable	**Technology** **3.4.1.10 (Technology)** The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing ISCM. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 4: Managed and Measurable	**3.4.1.11 (Technology)** The organization's ISCM performance measures include data on the implementation of its ISCM program for all sections of the network from the implementation of technologies that provide standard calculations, comparisons, and presentations. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 4: Managed and Measurable	**3.4.1.12 (Technology)** The organization utilizes a security information and event management tool to collect, maintain, monitor, and analyze information technology security information, achieve situational awareness, and manage risk. **TIGTA Comments:** The IRS did not meet this metric.
	Level 5: Optimized	**Definition** **3.5.1 (Definition)** In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.
Not Met	Level 5: Optimized	**People** **3.5.1.1 (People)** The organization's assigned personnel collectively possess a high skill level to perform and update ISCM activities on a near real-time basis to make any changes needed to address ISCM results based on organization risk tolerance, the threat environment, and business/mission requirements. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 5: Optimized	**Processes** **3.5.1.2 (Processes)** The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity and practices. **TIGTA Comments:** The IRS did not meet this metric.

3.0 Detect **Status of Information Security Continuous Monitoring Program**	**Maturity Model Indicator**	***Information Security Continuous Monitoring***
Not Met	Level 5: Optimized	**3.5.1.3 (Processes)** On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 5: Optimized	**3.5.1.4 (Processes)** The ISCM program is fully integrated with strategic planning, enterprise architecture and capital planning and investment control processes, and other mission/business areas, as appropriate. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 5: Optimized	**3.5.1.5 (Processes)** The ISCM program achieves cost-effective information technology security objectives and goals and influences decisionmaking that is based on cost, risk, and mission impact. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 5: Optimized	**Technology** **3.5.1.6 (Technology)** The organization has institutionalized the implementation of advanced cybersecurity technologies in near real time. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 5: Optimized	**3.5.1.7 (Technology)** The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its ISCM program. **TIGTA Comments:** The IRS did not meet this metric.

4.0 Respond **Status of Incident Response Program**	**Maturity Model Indicator**	***Incident Response Program***
	Level 1: Ad-Hoc	**Definition** **4.1.1 (Definition)** The incident response program is not formalized and incident response activities are performed in a reactive manner, resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with the FISMA (including guidance from NIST SP 800-83, NIST SP 800-61, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and United States-Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines).[25]
Met	Level 1: Ad-Hoc	**People** **4.1.1.1 (People)** Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have not been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, the DHS, and the OMB for all incident response activities.
Met	Level 1: Ad-Hoc	**4.1.1.2 (People)** The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. Key personnel do not possess the knowledge, skills, and abilities to successfully implement an effective incident response program.
Met	Level 1: Ad-Hoc	**4.1.1.3 (People)** The organization has not defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders and used to make timely, risk-based decisions.
Met	Level 1: Ad-Hoc	**4.1.1.4 (People)** The organization has not defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas as appropriate.

[25] NIST, NIST SP 800-83 Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* (July 2013). NIST, NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide* (Aug. 2012). OMB, OMB M-16-03, *Fiscal Year 2015–2016 Guidance on Federal Information Security and Privacy Management Requirements* (Oct. 2015).

4.0 Respond **Status of Incident Response Program**	**Maturity Model Indicator**	***Incident Response Program***
Met	Level 1: Ad-Hoc	**Processes** **4.1.1.5 (Processes)** Incident response processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: incident response planning; incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting to internal and external stakeholders using standard data elements and impact classifications within time frames established by the US-CERT.
Met	Level 1: Ad-Hoc	**4.1.1.6 (Processes)** The organization has not fully defined how it will collaborate with the DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents.
Met	Level 1: Ad-Hoc	**4.1.1.7 (Processes)** The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk.
Met	Level 1: Ad-Hoc	**4.1.1.8 (Processes)** The organization has not defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes.
Met	Level 1: Ad-Hoc	**Technology** **4.1.1.9 (Technology)** The organization has not identified and defined the incident response technologies needed in one or more of the following areas and relies on manual/procedural methods in instances where automation would be more effective. Use of incident response technologies in the following areas is ad-hoc. • Web application protections, such as web application firewalls. • Event and incident management, such as intrusion detection and prevention tools and incident tracking and reporting tools. • Aggregation and analysis, such as security information and event management products. • Malware detection, such as antivirus and antispam software technologies. • Information management, such as data loss prevention. • File integrity and endpoint and server security tools.
Met	Level 1: Ad-Hoc	**4.1.1.10 (Technology)** The organization has not defined how it will meet the defined Trusted Internet Connection (TIC) security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points as appropriate.

4.0 Respond **Status of Incident Response Program**	**Maturity Model Indicator**	***Incident Response Program***
Met	Level 1: Ad-Hoc	**4.1.1.11 (Technology)** The organization has not defined how it plans to utilize the DHS's Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks.
Met	Level 1: Ad-Hoc	**4.1.1.12 (Technology)** The organization has not defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems.
	Level 2: Defined	**Definition** **4.2.1 (Definition)** The organization has formalized its incident response program through the development of comprehensive incident response policies, plans, and procedures consistent with the FISMA (including guidance from NIST SP 800-83, NIST SP 800-61, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and the US-CERT Federal Incident Notification Guidelines). However, incident response policies, plans, and procedures are not consistently implemented organizationwide.
Met	Level 2: Defined	**People** **4.2.1.1 (People)** Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, the DHS, and the OMB for all incident response activities. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement incident response activities. Further, the organization has not verified roles and responsibilities as part of incident response testing.
Met	Level 2: Defined	**4.2.1.2 (People)** The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective incident response program.
Met	Level 2: Defined	**4.2.1.3 (People)** The organization has defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders and used to make timely, risk-based decisions. However, the organization does not consistently utilize its threat vector taxonomy, and incident response information is not always shared with individuals with significant security responsibilities and other stakeholders in a timely manner.

4.0 Respond **Status of Incident Response Program**	**Maturity Model Indicator**	***Incident Response Program***
Met	Level 2: Defined	**4.2.1.4 (People)** The organization has defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas as appropriate. However, incident response activities are not consistently integrated with these areas.
Met	Level 2: Defined	**Processes** **4.2.1.5 (Processes)** Incident response processes have been fully defined for the following areas: incident response planning; incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within time frames established by the US-CERT. However, these processes are inconsistently implemented across the organization.
Met	Level 2: Defined	**4.2.1.6 (Processes)** The organization has fully defined, but not consistently implemented, its processes to collaborate with the DHS and other parties, as appropriate, to provide on-site technical assistance/surge resources/special capabilities for quickly responding to incidents.
Met	Level 2: Defined	**4.2.1.7 (Processes)** The organization has identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization.
Met	Level 2: Defined	**4.2.1.8 (Processes)** The organization has defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. However, lessons learned are not consistently captured and shared across the organization and used to make timely improvements to security controls and the incident response program.
Met	Level 2: Defined	**Technology** **4.2.1.9 (Technology)** The organization has identified and fully defined the incident response technologies it plans to utilize in the following areas. • Web application protections, such as web application firewalls. • Event and incident management, such as intrusion detection and prevention tools and incident tracking and reporting tools. • Aggregation and analysis, such as security information and event management products. However, the organization has not ensured that security and event data are aggregated and correlated from all relevant sources and sensors.

4.0 Respond **Status of Incident Response Program**	**Maturity Model Indicator**	***Incident Response Program***
		• Malware detection such as antivirus and antispam software technologies. • Information management, such as data loss prevention. • File integrity and endpoint and server security tools. However, the organization has not fully implemented technologies in these areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policies, plans, and procedures.
Met	Level 2: Defined	**4.2.1.10 (Technology)** The organization has defined how it will meet the defined TIC security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points as appropriate. However, the organization has not ensured that the TIC 2.0 provider- and agency-managed capabilities are consistently implemented.
Met	Level 2: Defined	**4.2.1.11 (Technology)** The organization has defined how it plans to utilize the DHS's Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its networks.
Met	Level 2: Defined	**4.2.1.12 (Technology)** The organization has defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. However, the organization has not established, and does not consistently maintain, a comprehensive baseline of network operations and expected data flows for users and systems.
	Level 3: Consistently Implemented	**Definition** **4.3.1 (Definition)** In addition to the formalization and definition of its incident response program (Level 2), the organization consistently implements its incident response program across the agency in accordance with the FISMA (including guidance from NIST SP 800-83, NIST SP 800-61, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and the US-CERT Federal Incident Notification Guidelines). However, data supporting metrics on the effectiveness of the incident response program across the organization are not verified, analyzed, and correlated.

4.0 Respond **Status of Incident Response Program**	**Maturity Model Indicator**	***Incident Response Program***
Met	Level 3: Consistently Implemented	**People** **4.3.1.1 (People)** Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined, communicated, and consistently implemented across the organization (Level 2). Further, the organization has verified roles and responsibilities of incident response stakeholders as part of incident response testing.
Met	Level 3: Consistently Implemented	**4.3.1.2 (People)** The organization has fully implemented its plans to close any gaps in the skills, knowledge, and resources needed to effectively implement its incident response program. Incident response teams are periodically trained to ensure that knowledge, skills, and abilities are maintained. **TIGTA Comments:** The skills gap assessment conducted by the IRS indicated a skills proficiency gap when comparing the IRS CSIRC personnel to the industry standard level of technical proficiency. In addition, the staffing assessment showed 2.6 percent of the requisite staffing was considered unmet. The IRS indicated that these staffing and skills gaps have been addressed by augmenting Federal employees with contractors. TIGTA is currently engaged in an audit of the CSIRC organization and intends to further assess this assertion to ensure that the combined skill set and staffing level is sufficient to protect the IRS network from increasingly sophisticated adversaries.
Met	Level 3: Consistently Implemented	**4.3.1.3 (People)** The organization consistently utilizes its defined threat vector taxonomy and shares information with individuals with significant security responsibilities and other stakeholders in a timely fashion to support risk-based decisionmaking.
Met	Level 3: Consistently Implemented	**4.3.1.4 (People)** Incident response activities are integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas as appropriate.
Met	Level 3: Consistently Implemented	**Processes** **4.3.1.5 (Processes)** Incident response processes are consistently implemented across the organization for the following areas: incident response planning; incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within time frames established by the US-CERT.
Met	Level 3: Consistently Implemented	**4.3.1.6 (Processes)** The organization has ensured that processes to collaborate with the DHS and other parties, as appropriate, to provide on-site technical assistance/surge resources/special capabilities for quickly responding to incidents are implemented consistently across the organization.

4.0 Respond **Status of Incident Response Program**	**Maturity Model Indicator**	***Incident Response Program***
Met	Level 3: Consistently Implemented	**4.3.1.7 (Processes)** The organization is consistently capturing qualitative and quantitative performance metrics on the performance of its incident response program. However, the organization has not ensured that the data supporting the metrics was obtained accurately and in a reproducible format or that the data are analyzed and correlated in ways that are effective for risk management.
Met	Level 3: Consistently Implemented	**4.3.1.8 (Processes)** The organization is consistently collecting and capturing lessons learned and incident data on the effectiveness of its incident response program and activities. However, lessons learned may not be shared across the organization in a timely manner and used to make timely improvements to the incident response program and security measures.
Met	Level 3: Consistently Implemented	**4.3.1.9 (Processes)** The rigor, intensity, scope, and results of incident response activities (*i.e.*, preparation, detection, analysis, containment, eradication, and recovery, reporting, and post incident) are comparable and predictable across the organization.
Met	Level 3: Consistently Implemented	**Technology** **4.3.1.10 (Technology)** The organization has consistently implemented its defined incident response technologies in the following areas. • Web application protections, such as web application firewalls. • Event and incident management, such as intrusion detection and prevention tools and incident tracking and reporting tools. • Aggregation and analysis, such as security information and event management products. The organization ensures that security and event data are aggregated and correlated from all relevant sources and sensors. • Malware detection such as antivirus and antispam software technologies. • Information management, such as data loss prevention. • File integrity and endpoint and server security tools. In addition, the tools are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans.
Met	Level 3: Consistently Implemented	**4.3.1.11 (Technology)** The organization has consistently implemented defined TIC security controls and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points as appropriate.

4.0 Respond **Status of Incident Response Program**	**Maturity Model Indicator**	***Incident Response Program***
Met	Level 3: Consistently Implemented	**4.3.1.12 (Technology)** The organization is utilizing the DHS's Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving their networks.
Met	Level 3: Consistently Implemented	**4.3.1.13 (Technology)** The organization has fully implemented technologies to develop and maintain a baseline of network operations and expected data flows for users and systems.
	Level 4: Managed and Measurable	**Definition** **4.4.1 (Definition)** In addition to being consistently implemented (Level 3), incident response activities are repeatable and metrics are used to measure and manage the implementation of the incident response program, achieve situational awareness, and control ongoing risk. In addition, the incident response program adapts to new requirements and governmentwide priorities.
Met	Level 4: Managed and Measurable	**People** **4.4.1.1 (People)** Incident response stakeholders are consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and are collecting, analyzing, and reporting data on the effectiveness of the organization's incident response program.
Met	Level 4: Managed and Measurable	**4.4.1.2 (People)** Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the incident response program.
Met	Level 4: Managed and Measurable	**4.4.1.3 (People)** Incident response stakeholders are assigned responsibilities for developing and monitoring incident response metrics as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the incident response program.
Met	Level 4: Managed and Measurable	**Processes** **4.4.1.4 (Processes)** The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing incident response.
Met	Level 4: Managed and Measurable	**4.4.1.5 (Processes)** Data supporting incident response measures and metrics are obtained accurately, consistently, and in a reproducible format.

4.0 Respond **Status of Incident Response Program**	**Maturity Model Indicator**	***Incident Response Program***
Met	Level 4: Managed and Measurable	**4.4.1.6 (Processes)** Incident response data, measures, and metrics are analyzed, collected, and presented using standard calculations, comparisons, and presentations.
Met	Level 4: Managed and Measurable	**4.4.1.7 (Processes)** Incident response metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities.
Met	Level 4: Managed and Measurable	**Technology** **4.4.1.8 (Technology)** The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities.
Met	Level 4: Managed and Measurable	**4.4.1.9 (Technology)** The organization's incident response performance measures include data on the implementation of its incident response program for all sections of the network.
	Level 5: Optimized	**Definition** **4.5.1 (Definition)** In addition to being managed and measurable (Level 4), the organization's incident response program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.
Not Met	Level 5: Optimized	**People** **4.5.1.1 (People)** The organization's assigned personnel collectively possess a high skill level to perform and update incident response activities on a near real-time basis to make any changes needed to address incident response results based on organization risk tolerance, the threat environment, and business/mission requirements. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 5: Optimized	**Processes** **4.5.1.2 (Processes)** The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity practices. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 5: Optimized	**4.5.1.3 (Processes)** On a near real-time basis, the organization actively adapts its incident response program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a near real-time manner. **TIGTA Comments:** The IRS did not meet this metric.

4.0 Respond **Status of Incident Response Program**	**Maturity Model Indicator**	***Incident Response Program***
Not Met	Level 5: Optimized	**4.5.1.4 (Processes)** The incident response program is fully integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas as appropriate. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 5: Optimized	**4.5.1.5 (Processes)** The incident response program achieves cost-effective information technology security objectives and goals and influences decisionmaking that is based on cost, risk, and mission impact. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 5: Optimized	**Technology** **4.5.1.6 (Technology)** The organization has institutionalized the implementation of advanced incident response technologies in near real-time. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 5: Optimized	**4.5.1.7 (Technology)** The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its incident response program. **TIGTA Comments:** The IRS did not meet this metric.
Not Met	Level 5: Optimized	**4.5.1.8 (Technology)** The organization uses simulation based technologies to continuously determine the impact of potential security incidents to its information technology assets and adjusts incident response processes and security measures accordingly. **TIGTA Comments:** The IRS did not meet this metric.

5.0 Recover **Status of Contingency Planning Program**	**Maturity Model Indicator**	***Contingency Planning (Recover)***
Yes	Level 2: Defined	**5.1** Has the organization established an enterprisewide business continuity/disaster recovery program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

5.0 Recover **Status of Contingency Planning Program**	**Maturity Model Indicator**	***Contingency Planning* (*Recover*)**
Yes	Level 3: Consistently Implemented	**5.1.1** Develops and facilitates recovery testing, training, and exercise programs. (Federal Continuity Directive 1 (FCD1), NIST SP 800-34, NIST SP 800-53)[26]
Yes	Level 3: Consistently Implemented	**5.1.2** Incorporates the system's Business Impact Analysis and Business Process Analysis into analysis and strategy toward development of the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan. (NIST SP 800-34)
Yes	Level 3: Consistently Implemented	**5.1.3** Develops and maintains documented recovery strategies, plans, and procedures at the division, component, and information technology infrastructure levels. (NIST SP 800-34)
Yes	Level 3: Consistently Implemented	**5.1.4** A Business Continuity Plan and Disaster Recovery Plan are in place and ready to be executed upon if necessary. (FCD1, NIST SP 800-34, FY 2016 CIO FISMA Metrics 5.3, PMC)
Yes	Level 4: Managed and Measurable	**5.1.5** Tests Business Continuity Plan and Disaster Recovery Plan for effectiveness and updates plans as necessary. (FY 2016 CIO FISMA Metrics 5.4)
Yes	Level 3: Consistently Implemented	**5.1.6** Tests system-specific contingency plans, in accordance with organizationally defined time frames, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4)
Yes	Level 4: Managed and Measurable	**5.1.7** Develops after-action reports that address issues identified during contingency/disaster recovery exercises in order to improve contingency/disaster recovery processes. (FCD1, NIST SP 800-34)
Yes	Level 3: Consistently Implemented	**5.1.8** Determines alternate processing and storage sites based upon risk assessments which ensure that the potential disruption of the organization's ability to initiate and sustain operations is minimized and are not subject to the same physical and/or cybersecurity risks as the primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-6 and CP-7)

[26] DHS, *Federal Continuity Directive 1 (FCD 1): Federal Executive Branch National Continuity Program and Requirements* (Oct. 2012). NIST, NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010, updated Nov. 2010).

5.0 Recover **Status of Contingency Planning Program**	**Maturity Model Indicator**	***Contingency Planning* (*Recover*)**
Yes	Level 4: Managed and Measurable	**5.1.9** Conducts backups of information at the user and system levels and protects the confidentiality, integrity, and availability of backup information at storage sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-9, NIST CF PR.IP-4, National Archives and Records Administration guidance on information systems security records)
Yes	Level 2: Defined	**5.1.10** Contingency planning that considers supply chain threats.
Effective		**5.1.11** Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Based on all testing performed, is the contingency planning program effective?

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the effectiveness of the IRS's information security program, procedures, and practices and its compliance with FISMA requirements for the period July 1, 2015, to June 30, 2016. To accomplish our objective, we responded to the questions provided in the DHS *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*,[1] issued on June 20, 2016. The questions related to five cybersecurity functions that included eight security program areas:

1. **Identify**
   - *Risk Management*
   - *Contractor Systems*
   - *Configuration Management*
2. **Protect**
   - *Identity and Access Management*
   - *Security and Privacy Training*
3. **Detect**
   - *Information Security Continuous Monitoring*
4. **Respond**
   - *Incident Response*
5. **Recover**
   - *Contingency Planning*

We based our evaluation work, in part, on a representative subset of 10 major IRS information systems. We used the system inventory contained within the Treasury FISMA Information Management System of major applications and general support systems with a security classification of "Moderate" or "High" as the population for this subset. We also considered the results of TIGTA audits completed during the FY 2016 FISMA evaluation period, as listed in Appendix IV, as well as an audit report from the GAO that contained results applicable to the FISMA questions.

Based on our evaluative work, we will indicate with a yes or a no whether the IRS has achieved a satisfactory level of performance for each security program area as well as each specific attribute. The Treasury Office of the Inspector General will combine our results for the IRS with its results for the non-IRS bureaus and input the combined yes or no responses into Cyberscope.[2]

[1] DHS, *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (Version 1.1.1, Aug. 2016).
[2] An online data collection tool administrated by the DHS to collect performance data for FISMA compliance reporting.

Appendix II

Major Contributors to This Report

Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Midori Ohno, Lead Auditor
Cindy Harris, Senior Auditor
Bret Hunter, Senior Auditor
Mary Jankowski, Senior Auditor
Louis Lee, Senior Auditor
Esther Wilson, Senior Auditor
Linda Cieslak, Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Chief Information Officer
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, User and Network Services
Director, Office of Audit Coordination

Appendix IV

Information Technology Security-Related Reports Issued During the Fiscal Year 2016 Evaluation Period

1. TIGTA, Ref. No. 2015-20-060, *The Return Review Program Enhances the Identification of Fraud; However, System Security Needs Improvement* (July 2015).
2. TIGTA, Ref. No. 2015-23-062, *Affordable Care Act Information Sharing and Reporting Project* (Aug. 2015).
3. TIGTA, Ref. No. 2015-20-079, *Stronger Access Controls and Further System Enhancements Are Needed to Effectively Support the Privacy Impact Assessment Program* (Sept. 2015).
4. TIGTA, Ref. No. 2015-20-087, *Improvements Are Needed to Ensure That External Interconnections Are Identified, Authorized, and Secured* (Sept. 2015).
5. TIGTA, Ref. No. 2015-20-088, *Improvements Are Needed to Ensure That New Information Systems Deploy With Compliant Audit Trails and That Identified Deficiencies Are Timely Corrected* (Sept. 2015).
6. TIGTA, Ref. No. 2015-20-092, *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2015* (Sept. 2015).
7. TIGTA, Ref. No. 2015-23-081, *Affordable Care Act Verification Service: Security and Testing Risks* (Sept. 2015).
8. TIGTA, Ref. No. 2015-20-073, *Inadequate Early Oversight Led to Windows Upgrade Project Delays* (Sept. 2015).
9. TIGTA, Ref. No. 2015-20-093, *Review of the Electronic Fraud Detection System* (Sept. 2015).
10. TIGTA, Ref. No. 2015-20-094, *Annual Assessment of the Internal Revenue Service Information Technology Program* (Sept. 2015).
11. TIGTA, Ref. No. 2016-20-002, *Measurable Agreements on Security Controls Are Needed to Support the Enterprise Storage Services Solution* (Oct. 2015).
12. TIGTA, Ref. No. 2016-40-007, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed* (Nov. 2015).
13. TIGTA, Ref. No. 2016-20-019, *Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement* (Feb. 2016).
14. TIGTA, Ref. No. 2016-23-040, *Affordable Care Act Compliance Validation System: Security and Testing Risks* (May 2016).

15. TIGTA, Ref. No. 2016-2R-044, *The Internal Revenue Service's Cybersecurity Incidents, Policies, and Procedures* (June 2016).

16. TIGTA, Ref. No. 2016-10-038, *Access to Government Facilities and Computers Is Not Always Removed When Employees Separate* (June 2016).

17. GAO, Ref. No. GAO-16-398, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data* (Mar. 2016).

Treasury OIG Website

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

Report Waste, Fraud, and Abuse

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