Audit Report

OIG-18-005

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

October 27, 2017

Office of Inspector General

Department of the Treasury

THIS PAGE INTENTIONALLY LEFT BLANK

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 27, 2017

MEMORANDUM FOR KODY KINSLEY
ASSISTANT SECRETARY FOR MANAGEMENT

ERIC OLSON
ACTING DEPUTY ASSISTANT SECRETARY FOR INFORMATION SYSTEMS AND CHIEF INFORMATION OFFICER

FROM: Larissa Klimpel /s/
Director, Cyber/Information Technology Audit

SUBJECT: Audit Report – *Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2017 Performance Audit for the Collateral National Security Systems*

We are pleased to transmit the attached report, *Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2017 Performance Audit for the Collateral National Security Systems*, dated October 26, 2017. The Federal Information Security Modernization Act of 2014 (FISMA) requires that Federal agencies have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices, and to report the results to the Office of Management and Budget (OMB). OMB delegated its responsibility to the Department of Homeland Security (DHS) for the collection of annual FISMA responses. FISMA also requires that the agency Inspector General (IG) or an independent external auditor perform the annual evaluation as determined by the IG.

To meet our FISMA requirements, we contracted with KPMG LLP (KPMG), a certified independent public accounting firm, to perform this year's annual FISMA audit of Treasury's collateral national security systems. In connection with our contract with KPMG, we reviewed its report and related documentation and inquired of its representatives. Our review, as differentiated from an audit performed in accordance with generally accepted auditing standards, was not intended to enable us to conclude on the effectiveness of Treasury's information security program or its compliance with FISMA. KPMG is responsible for its report and the conclusions expressed therein.

In brief, KPMG reported that consistent with applicable FISMA requirements, OMB and the Committee on National Security Systems policy and guidance, and the National Institute of Standards and Technology standards and guidelines, Treasury established and maintained information security programs and practices for its collateral national security systems for the 5 Cybersecurity Functions and 7 FISMA program areas. However, KPMG identified 4 deficiencies within 2 of the 5 Cybersecurity Functions and within 4 of the 7 FISMA program areas. Accordingly, KPMG made 7 recommendations to address these deficiencies.

Appendix III of the attached KPMG report includes *The Department of the Treasury's Consolidated Response to DHS's FISMA 2017 Questions for Inspectors General*.

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

Attachment

Department of the Treasury
Federal Information Security Modernization Act Fiscal Year 2017 Performance Audit for the Collateral National Security Systems

October 26, 2017

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

Department of the Treasury
Federal Information Security Modernization Act Fiscal Year 2017 Performance Audit for the Collateral National Security Systems

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 2017 Performance Audit for Collateral National Security Systems

Dear Mr. Thorson:

This report presents the results of our independent performance audit of the Department of the Treasury's (Treasury or Department) Collateral National Security Systems (NSS) information systems' security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires Federal agencies, including Treasury, to have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices, and to report the results of the evaluations to the Office of Management and Budget (OMB). OMB delegated its responsibility to Department of Homeland Security (DHS) for the collection of annual FISMA responses. DHS prepared the FISMA questionnaire to collect these responses, which is provided in Appendix III, *Department of the Treasury's Consolidated Response to DHS's FISMA 2017 Questions for Inspectors General*, dated April 17, 2017. We also considered applicable OMB policy and guidelines, the Committee on National Security Systems (CNSS) 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, as determined by the IG, perform the annual evaluation. The Treasury Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct an audit of Treasury's information system security program and practices for its collateral NSS.

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

The objective of this performance audit was to assess the effectiveness of the Department of the Treasury's (Treasury) information security program and practices for its collateral NSS for the period July 1, 2016 through June 30, 2017. As part of our audit, we responded to the DHS *FISMA 2017 Questions for Inspectors General*, dated April 17, 2017, and assessed the maturity levels on behalf of the Treasury Office of Inspector General. Additional details regarding the scope of our independent audit are included in Appendix I, *Objectives, Scope and Methodology*. Appendix II, *Status of Prior-Year Findings,* summarizes Treasury's progress in addressing prior-year recommendations. Appendix III includes the *Treasury's Consolidated Response DHS' FISMA 2017 Questions for Inspectors General*, and Appendix IV contains a glossary of terms used in this report.

Consistent with applicable FISMA requirements, OMB and CNSS policy and guidelines, and NIST standards and guidelines, Treasury has established and maintained its information security program and practices for its collateral NSS for the 5 Cybersecurity Functions[1] and 7 FISMA Metric Domains.[2] However, the program was not fully effective as reflected in the 4 deficiencies within 3 of the 5 Cybersecurity Functions and within 4 of the 7 FISMA program areas that we identified as follows:

Cybersecurity Function: Identify:

1. The Treasury Directive Publication (TD P) 85-01, *Department of the Treasury Information Technology Security Policy,* Appendix B, "Classified (National Security Systems)" and Departmental Offices (DO) Collateral NSS System Security Plan (SSP) were not updated in accordance with CNSS No. 1253, *Security Categorization and Control Selection for National Security Systems,* guidance. (Risk Management)

Cybersecurity Function: Protect

2. DO Collateral NSS patch management process was not compliant with the Treasury Information Technology Security policy. (Configuration Management)
3. DO Collateral NSS account management activities were not compliant with its SSP policies. (Identity and Access Management)

Cybersecurity Function: Recover

4. DO did not perform Business Impact Analyses (BIAs) for the DO Collateral NSS. (Contingency Planning)

We made 7 recommendations related to these control deficiencies that, if effectively addressed by management, should strengthen respective bureau's, office's, and Treasury's information security program. In a written response, the Acting Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO) agreed with our findings and recommendations and provided planned corrective actions that were responsive to the intent of our recommendations (see *Management Response)*.

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

Sincerely,

KPMG LLP

October 26, 2017

[1] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the Fiscal Year (FY) 2017 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers (CIO) Council. In FY 2017 the seven IG FISMA Metric Domains were aligned with the five functions of identify, protect, detect, respond, and recover as defined in the *NIST Framework for Improving Critical Infrastructure Cybersecurity*.

[2] As described in the DHS' *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0,* the 7 FISMA Metric Domains are: risk management, configuration management, identity and access management, security training, information security continuous monitoring, incident response, and contingency planning. Contractor systems metrics were consolidated into the risk management FISMA metric domain.

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 Inspectors General (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.

FISMA defines a National Security System (NSS) as any information system used or operated by an agency or by a contractor of an agency where the function, operation, or use of that system (1) involves intelligence activities, (2) involves cryptological activities related to national security, (3) involves command and control of military forces, (4) involves equipment that is an integral part of a weapon or weapon system, or (5) is critical to the direct fulfillment of military or intelligence missions. This report contains the evaluation of the Treasury's information security program and practices for its collateral NSS, which are NSS that do not deal with intelligence. The audit of the Treasury's intelligence NSS will be reported separately by the Treasury Office of Inspector General (OIG).

FY 2017 Inspector General FISMA Reporting Metrics

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

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

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

Federal Standards and Guidelines

Except for systems that meet FISMA's definition of NSS, the Secretary of Commerce is responsible for prescribing standards and guidelines pertaining to federal information systems based on standards and guidelines developed by NIST. The Committee on National Security Systems (CNSS), and Federal agencies that operate systems falling within the definition of NSS, provide security standards and guidance for NSS. CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, states that the controls described in NIST Special Publication (SP) 800-53, Revision (Rev.) 4, April 2013, *Security and Privacy Controls for Federal Information Systems and Organizations*, shall apply to all NSS. In addition, FISMA requires that NIST provide information security controls guidance for systems identified as NSS. Treasury used NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System (August 2003),* to identify its two collateral systems.

Treasury is responsible for implementing policies, procedures, and control techniques for its collateral NSS based on guidance from CNSS. Treasury Directive Publication (TD P) 85-01, *Department of the Treasury Information Technology Security Policy*, Appendix B*,* "Classified (National Security Systems)," provides Treasury security policy and standards for all systems that process or communicate classified national security information.

We reviewed both of the collateral NSS; one managed by the Departmental Offices (DO) and one managed by the Bureau of Engraving and Printing (BEP).

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

Department of the Treasury Information Security Management Program

Treasury Office of the Chief Information Officer

The Treasury Chief Information Officer (CIO) is responsible for providing Treasury-wide leadership and direction for all areas of information and technology management, as well as the oversight of a number of IT programs. Among these programs is Cyber Security, which has responsibility for the implementation and management of Treasury-wide IT security programs and practices. Through its mission, the 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, Appendix B, 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 OCIO's Cyber Security Program are also responsible for promoting and coordinating a Treasury IT security program, as well as monitoring and evaluating the status of Treasury's IT security posture and compliance with statutes, regulations, policies, and guidance. Lastly, the ACIOCS has the responsibility of managing Treasury's IT Critical Infrastructure Protection (CIP) program for Treasury IT assets.

Bureau CIOs

Organizationally, Treasury has established a Treasury CIO and bureau-level CIOs. The bureau-level CIOs are responsible for managing the IT security program for their respective bureau, as well as advising the bureau head on significant issues related to the bureau IT security program. The CIOs also have the responsibility for overseeing the development of procedures that comply with the Treasury OCIO's policy and guidance and federal statutes, regulations, policy, and guidance. The bureau Chief Information Security Officers (CISO) are tasked by their respective CIOs to serve as the central point of contact for the bureau's IT security program, as well as to develop and oversee the bureau's IT security program. This includes the development of policies, procedures, and guidance required to implement and monitor the bureau IT security program.

Department of the Treasury – Bureau OCIO Collaboration

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

OVERALL PERFORMANCE AUDIT RESULTS

Consistent with applicable Federal Information Security Modernization Act of 2014 (FISMA) requirements, Office of Management and Budget (OMB) policy, the Committee on National Security Systems (CNSS) policy and guidance, and National Institute of Standards and Technology (NIST) standards and guidelines, Treasury established and maintained its information system security program and practices for its collateral national security systems (NSSs) for the 5 Cybersecurity functions and 7 FISMA metric domains. The FISMA program areas are outlined in the *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0* and were prepared by DHS Office of Cybersecurity and Communications Federal Network Resilience. The 7 program areas are Risk Management, Configuration Management, Identity and Access Management, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning. However, while the security program has been implemented across Treasury for both its collateral NSS, it was not fully effective as we identified 4 deficiencies in 3 of the 5 Cybersecurity Functions (identify, protect, detect, respond, and recover) and 4 out of the 7 FISMA program areas (risk management, configuration management, identity and access management, and security training) that needed improvement.

We have made 7 recommendations that if effectively addressed by management, should strengthen respective bureau's, office's, and Treasury's information system security programs. The *Findings* section of this report presents the detailed findings and associated recommendations. Additionally, we evaluated prior-year findings from the fiscal year (FY) 2016 FISMA performance audit and noted that management closed 5 of 6 findings. See Appendix II*,* *Status of Prior-Year Findings*, for additional details.

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

FINDINGS

1. The Treasury Directive Publication (TD P) 85-01, *Department of the Treasury Information Technology Security Policy,* Appendix B, "Classified (National Security Systems),"and Departmental Offices (DO) Collateral National Security System (NSS) System Security Plan (SSP) were not updated in accordance with Committee on National Security Systems (CNSS) No. 1253, *Security Categorization and Controls Selection for National Security Systems,* guidance.

The CNSS Instruction No. 1253, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, and the TD P 85-01, Appendix B, requires the organization to develop a security plan for the information system that is consistent with the organization's enterprise architecture, provide an overview of the security requirements for the system, identify any relevant overlays, if applicable, and describe the security controls in place, or planned, for meeting those requirements including a rationale for tailoring and supplementation decisions. This control falls under the Identify Cybersecurity area and the Risk Management Federal Information Security Modernization Act of 2014 (FISMA) Metric Domain. We noted the following:

- Office of the Chief Information Officer (OCIO) management did not ensure that the TD P 85-01: Appendix B: was updated to address all of the applicable CNSS Instruction No. 1253, and NIST SP 800-53, Rev. 4, baseline control enhancements. Specifically, KPMG noted that two control enhancements were omitted. Due to lack of oversight, OCIO management did not include all required control enhancements within the minimum-security baseline for NSS. The lack of documented security control requirements and control enhancements increases the risk that the controls are implemented in a manner that does not align to the organizational risk tolerance. Thus, the organization is susceptible to risk they are not willing to accept. (See recommendations #1 & 2.)

- Through inspection of the DO Collateral NSS System Security Plan (SSP), we found that the SSP lacked sufficient descriptions regarding the implementation of each TD P 85-01 security control. Specifically, we determined the security controls implementation was not defined for any security control in accordance with the TD P 85-01, CNSS Instruction No. 1253, and NIST 800-53, Rev.4, guidance. Due to competing priorities and change in personnel, DO management did not place emphasis on updating the DO Collateral NSS SSP to address how the security controls are implemented within the DO Collateral NSS environment. SSPs document the security controls implemented within the DO Collateral NSS environment. Incomplete documentation in the SSP regarding how each security control is implemented, or planned to be implemented, increases the risk of misunderstanding how system controls are implemented, potentially leading to a false sense of security. *(See recommendation #3.)*

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

1. Update the TD P 85-01, Appendix B, for NSS, to address all CNSSI Instruction No. 1253 and NIST SP 800-53, Rev. 4, control requirements, and control enhancements.

   Management Response: Treasury management will ensure the TD P85-01 Appendix B: Minimum Security Controls for NSS is updated in accordance with CNSS No. 1253, Security Categorization and Controls Selection for NSS, guidance. Target completion date: November 30, 2017.

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

2. Review TD P 85-01, Appendix B, to ensure that all control enhancements are appropriately included.

   Management Response: Treasury management will incorporate a periodic review process of Appendix B to ensure that all CNSS 1253 control enhancements are appropriately included in Treasury's NSS. Target completion date: October 30, 2017.

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

3. Update the DO Collateral SSP, and supporting documentation, to include an implementation statement detailing the processes in place to fulfill the requirements for each security control.

   Management Response: The DO Collateral system program will identify resources to update the SSP or related documentation to reflect all security controls required under TD P 85-01. Target completion date: May 30, 2018.

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

2. DO Collateral NSS patch management process was not compliant with the Treasury Information Technology Security Policy.

The TD P 85-01, Appendix B, requires the organization to review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses and to document configuration change decisions associated with the information system. TD P 85-01, Appendix B, also requires the organization to analyze changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. Moreover, TD P 85-01, Appendix B, requires the organization to identify, report, and correct information system flaws; test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; and ensure security patches are tested and installed on a timeline in accordance with the criticality of the patches. This control falls under the Protect Cybersecurity area, and the Identity and Access Management FISMA Metric Domain.

DO collateral NSS management stated that, due to the lack of a segmented test environment, management is unable to perform test case analysis on changes and patches prior to implementation into the production environment. Further, lack of management oversight has contributed to management not approving and maintaining documentation supporting the testing and implementation of the changes and patches. Inconsistent change management and patch management processes increases the risk to the current security posture of the information system and the risk of unauthorized changes being implemented into the production environment. This increases the potential for adverse effects to the system and to the integrity of system data. The inability to test changes and patches appropriately prior to implementation further increases the risk of adverse effects on the system. *(See recommendation #4.)*

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

4. Evaluate current test environment to determine if management needs to enhance the environment to allow for adequate testing of changes and patches, and, if necessary, implement a cost-effective solution.

   Management Response: DO OCIO will evaluate the current test environment and develop, as required, a plan of action for improvements and enhancements to the environment. Target completion date: April 30, 2018.

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

3. DO collateral NSS account management activities were not compliant with its SSP policies.

The TD P 85-01, Appendix B, and the DO Collateral NSS' SSP require management to disable user accounts that are inactive for more than 30 days. This control falls under the Protect Cybersecurity area, and the Identity and Access Management FISMA Metric Domain. We noted the following:

- DO Collateral NSS SSP and TD P 85-01, Appendix B, require management to disable DO Collateral NSS user's accounts that are inactive for more than 30 days. DO Collateral NSS management failed to disable 90 users that were inactive for more than 30 days. In addition, 40 new DO Collateral NSS users had not logged into their account for over 30 days and were not disabled, and 5 terminated users were not disabled or removed. Due to competing priorities, accounts of the terminated users were not monitored or disabled in a timely manner. To the extent that valid inactive accounts are present in DO Collateral NSS, user accounts have an increased risk of being compromised by unauthorized individuals. Further, unauthorized user account access may result in the loss of data, data corruption, and/or other privileged access. *(See recommendations #5 & 6.)*

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

5. Establish a process to review at a defined frequency the DO Collateral NSS user accounts.

   Management Response: DO plans to have outlined processes and procedures in place to review collateral user accounts. Target completion date: October 30, 2017.

   Auditor Comment: Management's response meets the intent of our recommendation so long as the indicated action addresses defining the frequency of DO Collateral NSS user accounts.

6. Disable terminated or inactive DO employees' or contractors' DO Collateral NSS accounts accordingly.

   Management Response: DO plans to have outlined processes and procedures in place to disable terminated or inactive DO employees' or contractors' DO Collateral NSS accounts accordingly. Target completion date: October 30, 2017.

   Auditor Comment: Management's response meets the intent of our recommendation so long as the indicated action addresses disabling inactive DO Collateral NSS user accounts per a defined frequency.

4. DO did not perform Business Impact Analyses (BIAs) for the DO Collateral NSS.

TD P 85-01, Appendix B, provides directions to bureaus and offices to complete Business Impact Analyses (BIAs) to determine and plan for the resumption of essential mission and business functions. The bureaus and offices should provide the capability to restore information system components within the time period contained within the BIAs from configuration-controlled and integrity-protected information representing a known, operational state for the components. The Department of Homeland Security (DHS) Federal Continuity Directive 1 (FCD-1) requires bureaus and offices to perform and document the BIA every two years. This control falls under the recover Cybersecurity domain and the contingency planning FISMA program area. We noted the following:

- Since 2012, DO management had not performed and documented a formal BIA that considered the DO Collateral NSS computing environment. DO management has included an initiative to update the DO Collateral NSS BIA within its strategic plan; however, due to competing priorities and change in personnel, DO management has not prioritized conducting a BIA. An outdated BIA that is not reflective of the current operating environment increases the risk that recovery strategies and priorities, including maximum tolerable downtime, recovery point objective, and recovery time objective, do not align with management expectations. *(See recommendation #7.)*

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

7. Perform and document the Business Impact Analysis for the DO Collateral NSS environment every two years as required by FCD-1.

   Management Response: DO OCIO will execute a Business Impact Analysis for the selected DO Collateral System. Target completion date: May 30, 2018.

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

SELF-IDENTIFIED WEAKNESSES

During the Fiscal Year (FY) 2017 Department of the Treasury (Treasury or Department) Federal Information Security Modernization Act of 2014 (FISMA) performance audit, we noted Departmental Offices' (DO) had a self-identified weakness. This self-identified weakness was associated with 2 open Plans of Action and Milestones (POA&Ms). We reviewed the self-identified weakness and noted that the weakness had a corrective action plan documented within the POA&M, and therefore, did not provide any additional recommendations.

FY17 FISMA Self-Identified Weaknesses – Department of the Treasury

Bureau	System(s)	NIST SP 800-53 Control	Weakness
DO	DO CNSS System	IA-2	POA&M #T-006: Lack of Multi-Factor Authentication
DO	DO CNSS System	SI-4	POA&M #242: Management Has Not Implemented a Security Event Information Manager (SIEM)

MANAGEMENT RESPONSE TO THE REPORT

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

DEPARTMENT OF THE
TREASURY
WASHINGTON, D.C.
20220

October 17, 2017

MEMORANDUM FOR LARISSA KLIMPEL
DIRECTOR, INFORMATION TECHNOLOGY AUDIT

FROM: Eric Olson /s/
Acting Deputy Assistant Secretary for Information
Systems and Chief Information Officer

SUBJECT: Management Response to Draft Audit Report – "Department of the Treasury Federal Information Security Modernization Act Fiscal Year
2017 Performance Audit for Collateral National Security Systems."

Thank you for the opportunity to comment on the draft report entitled, *Department of the Treasury Federal Information Security Modernization Act [FISMA] Fiscal Year 2017 Performance Audit for Collateral National Security Systems* (NSS). We are pleased the report states our security program is consistent with applicable FISMA requirements, the Office of Management and Budget (OMB) and Committee on National Security Systems policy and guidelines, 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 and agree with all findings and recommendations. Please refer to the attachment for further details on our planned corrective actions. We appreciate your noting that for the Departmental Offices' one self-identified weaknesses, a Plan of Action and Milestones (POA&M) had adequate corrective action plans established, and therefore, your auditors did not provide any additional recommendations. Finally, we acknowledge recent changes to the five-level maturity model deviates from previous guidance in how performance audits are scored and evaluated. Incorporating these changes, we still noted a moderate improvement in the overall results of this year's performance audit.

While the Department remains committed to improving its security program, the Treasury Secured Data Network (TSDN) has undergone significant cyber improvements during the past year to include receiving a favorable score on the Defense Information

Systems Agency (DISA) mandated Cyber Command Readiness Inspection (CCRI) assessment of our enclave. TSDN's other notable accomplishments include:

- Migrated Windows Servers from 2008 R2 to 2012 resulting in the enhancement of additional security features to the TSDN environment.

- Significantly reduced network vulnerabilities through improved patch management and reporting, enhanced configuration assessment, and upgraded hardware and software infrastructure.

- Updated Incident Response Plan to formalize reporting structure resulting in better incident handling and visibility.

- Deployment of Host Based protection to endpoints throughout the TSDN boundary.

- Significantly improved Privileged Vulnerability Scans resulting in a better understanding of cyber posture within the network.

- Upgraded the operational environment to benefit from the latest version of Microsoft Exchange server architecture.

- Developed and enhanced Windows group policies to ensure computer baseline configurations comply with DOD Security Technical Information Guidelines (STIG) specifications.

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

Attachment

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

Attachment

Management Response to KPMG Recommendations

KPMG Finding 1: The Treasury Directive Publication (TD P) 85-01, Department of the Treasury Information Technology Security Policy, Appendix B, "Classified (National Security Systems),"and Departmental Offices (DO) Collateral National Security System (NSS) System Security Plan (SSP) were not updated in accordance with Committee on National Security Systems (CNSS) No. 1253, Security Categorization and Controls Selection for National Security Systems, guidance.

KPMG Recommendation 1: We recommend Treasury management: For the selected system, update the TD P 85-01, Appendix B, for NSS, to address all CNSSI Instruction No. 1253 and NIST SP 800-53, Rev. 4, control requirements, and control enhancements.

> **Bureau's planned corrective action:** Treasury management will ensure the TD P85-01 Appendix B: Minimum Security Controls for NSS is updated in accordance with CNSS No. 1253, Security Categorization and Controls Selection for NSS, guidance. Target completion date: November 30, 2017.
>
> **Responsible Official:** Treasury, Chief Information Security Officer

KPMG Recommendation 2: We recommend Treasury management: For the selected system, review TD P 85-01, Appendix B, to ensure that all control enhancements are appropriately included.

> **Bureau's planned corrective action:** Treasury management will incorporate a periodic review process of Appendix B to ensure that all CNSS 1253 control enhancements are appropriately included in Treasury's NSS. Target completion date: October 30, 2017.
>
> **Responsible Official:** Treasury**,** Chief Information Security Officer

KPMG Recommendation 3: We recommend DO management: For the selected system, update the DO Collateral SSP, and supporting documentation, to include an implementation statement detailing the processes in place to fulfill the requirements for each security control.

> **Bureau's planned corrective action:** The TSDN program will identify resources to update the SSP or related documentation to reflect all security controls required under TD P 85-01. Target completion date: May 30, 2018.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Finding 2: DO Collateral NSS patch management process was not compliant with the Treasury Information Technology Security Policy.

KPMG Recommendation 4: We recommend DO management: For the selected system, evaluate and current test environment to determine if management needs to enhance the environment to allow for adequate testing of changes and patches, and, if necessary, implement a cost-effective solution.

> **Bureau's planned corrective action:** DO OCIO will evaluate the current test environment and develop, as required, a plan of action for improvements and enhancements to the environment. Target completion date: April 30, 2018.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Finding 3: DO collateral NSS account management activities were not compliant with its SSP policies.

KPMG Recommendation 5: We recommend DO management: For the selected system, establish a process to review at a defined frequency the DO Collateral NSS user accounts.

> **Bureau's planned corrective action:** DO plans to have outlined processes and procedures in place to review collateral user accounts. Target completion date: October 30, 2017.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Recommendation 6: We recommend DO management: For the selected system, disable terminated or inactive DO employees' or contractors' DO Collateral NSS accounts accordingly.

> **Bureau's planned corrective action:** DO plans to have outlined processes and procedures in place to disable terminated or inactive DO employees' or contractors' DO Collateral NSS accounts accordingly. Target completion date: October 30, 2017.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Finding 4: DO did not perform Business Impact Analyses (BIAs) for the DO Collateral NSS.

KPMG Recommendation 7: We recommend DO management: For the selected system, perform and document the Business Impact Analysis for the DO Collateral NSS environment every two years as required by FCD-1.

> **Bureau's planned corrective action:** DO OCIO will execute a Business Impact Analysis for the TSDN. Target completion date: May 30, 2018.
>
> **Responsible Official:** DO, Chief Information Security Officer

APPENDIX I – OBJECTIVE, SCOPE AND METHODOLOGY

The objective for this performance audit was to assess the effectiveness of the Department of the Treasury's (Treasury or Department) information security program and practices for its National Security Systems (NSS) for the period July 1, 2016 through June 30, 2017.[4] Specifically, we assessed the effectiveness of the Treasury information security program and practices for its two Collateral NSSs maintained at Bureau of Engraving and Printing (BEP) and Departmental Offices (DO). As part of our audit, we responded to the Department of Homeland Security (DHS) *Federal Information Security Modernization Act of 2014 (FISMA) 2017 Questions for Inspectors General*, dated April 17, 2017, and assessed the maturity levels on behalf of the Treasury OIG. Finally, we followed up on the status of prior-year FISMA findings.

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

To accomplish our audit objectives, we evaluated security controls in accordance with applicable legislation; the DHS *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0,* dated April 17, 2017; Committee on National Security Systems (CNSS guidelines); 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 complied with the implementation of these policies and procedures for collateral NSS.

The following is our approach for accomplishing the FISMA audit and being able to determine the maturity levels for each of the 7 FISMA Metric Domains from the FY 2017 FISMA Reporting Metrics for Inspector Generals (IGs):

1. We requested that BEP and DO management communicate their self-assessed maturity levels, where applicable, for the two Collateral NSSs to confirm our understanding of the FISMA-related policies and procedures, guidance, structures, and processes established by the two Bureaus. This helped us to understand specific artifacts to evaluate as part the FISMA audit.
2. We performed test procedures relevant to the two Collateral NSSs for maturity level 3 (Consistently Implemented) at BEP and DO for the maturity level 3 questions within the seven FISMA Metric Domains. The test procedures evaluated the design and operating effectiveness of the controls. If we determined that relevant maturity level 3 controls are ineffective, we assessed, based on test results and evidence obtained, the maturity at level 1 (Ad Hoc) or 2 (Defined) for the questions that failed testing.
3. For maturity level 3 controls that were determined to be effective, we performed level 4 (Managed and Measurable) test procedures relevant to the Collateral NSSs at BEP and DO for the maturity level 4 questions within the seven FISMA Metric Domains. The test procedures evaluated the design and operating effectiveness of the controls. If we determined that maturity level 4 controls are ineffective, we assessed, based on test results and evidence obtained, the maturity at level 3 for the questions that failed testing.

[4] Contract GS-23F-8127H, Task Order TPDOIG13K0012, Modification #0029, dated March 1, 2017

4. For maturity level 4 controls that were determined to be effective, we performed level 5 (Optimal) test procedures relevant to the two Collateral NSSs at BEP and DO for the maturity level 5 questions within the seven FISMA Metric Domains. The test procedures evaluated the design of the controls. If we determine that maturity level 5 controls are ineffective, we will assess, based on test results and evidence obtained, the maturity at level 4 for the questions that failed testing.

Other Considerations

In performing our control evaluations, we interviewed key Treasury DO and BEP personnel who had significant information security responsibilities, and personnel responsible for the two Treasury collateral NSS. 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 packages, configuration assessment results, and training records.

We performed our fieldwork at Treasury's headquarters offices in Washington, DC, and bureau locations in Washington, DC, during the period of April 4, 2017 through August 10, 2017. During our audit, we met with Treasury management to discuss our preliminary conclusions.

Criteria

We focused our FISMA evaluation approach on federal information security guidance developed by CNSS, NIST, and Office of Management and Budget (OMB). NIST Special Publications (SPs) provide guidelines that are considered essential to the development and implementation of agencies' security programs. The following is a listing of the criteria used in the performance of the Fiscal Year 2017 FISMA performance audit:

- Federal Information Security Modernization Act of 2014
- NIST Federal Information Processing Standards (FIPS) and/or Special Publications[5]
  - FIPS Publication 199*, Standards for Security Categorization of Federal Information and Information Systems*
  - FIPS Publication 200*, Minimum Security Requirements for Federal Information and Information Systems*
  - NIST Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*
  - NIST Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*

[5] Per OMB FISMA reporting instructions, while agencies are required to follow NIST standards and guidance in accordance with OMB policy, there is flexibility within NIST's guidance documents (specifically in the 800 series) in how agencies apply the guidance. However, NIST FIPS are mandatory. Unless specified by additional implementing policy by OMB, guidance documents published by NIST generally allow agencies latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable and compliant with the guidance.

- NIST Special Publication 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST Special Publication 800-39, *Managing Information Security*
- NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST Special Publication 800-61 Revision 2, *Computer Security Incident Handling Guide*
- NIST Special Publication 800-70 Revision 3, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*
- NIST Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response
- NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*

▪ CNSS Policy and Instructions

- CNSSP No. 22, *Policy on Information Assurance Risk Management for National Security Systems*
- CNSSI No. 1253, *Security Categorization and Control Selection for National Security Systems*

▪ OMB Policy Directives

- OMB Circular A-130, *Management of Federal Information Resources*
- OMB Memorandum 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*
- OMB Memorandum 05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*
- OMB Memorandum 16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for Federal Civilian Government*
- OMB Memorandum 16-03, *Fiscal Year 2016-2016 Guidance on Federal Information Security and Privacy Management Requirements*

  - OMB Memorandum 17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Requirements

- U.S. Department of Homeland Security
  - Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics
  - Federal Continuity Directive 1 (FCD-1), *Federal Executive Branch National Continuity Program and Requirements*

- Treasury Policy Directives
  - Treasury Directive Publication 15-71, *Department of Treasury Security Manual*
  - Treasury Directive Publication 85-01, *Treasury Information Technology (IT) Security Policy Appendix B Classified (National Security) Systems*

APPENDIX II – STATUS OF PRIOR-YEAR FINDINGS

In Fiscal Year (FY) 2016, we conducted a FISMA Performance Audit in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. As part of this year's FISMA 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.

Prior Year Findings – 2016 Performance Audit

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 1 – Committee of National Security Systems (CNSS) – Bureau of Engraving and Printing (BEP) Collateral NSS System Security Plan (SSP) was not in accordance with Committee on National Security Systems Instruction (CNSSI) No.1253 guidance.	For a selected BEP system, the SSP did not follow CNSSI No. 1253 or NIST SP 800-18 guidance as follows: • minimum security controls were not fully defined under CNSSI No. 1253 and NIST SP 800-53, Rev. 4, Control CP-3. Specifically, we noted the control selection for the SSP mirrored the control selection for an unclassified system and did not include the additional controls required for a collateral NSS. • controls were inappropriately inherited from the BEP network General Support System (GSS). In particular, we noted that, for CNSSI No. 1253 control RA-5, BEP incorrectly referred to a vulnerability scanning tool for the BEP network GSS; it did not refer to the manual quarterly	We recommend that BEP management: 1. For the selected system, review the controls that BEP collateral system is inheriting in the certification and accreditation tool to ensure they apply. 2. For the selected system, document the CNSSI No. 1253 controls in the SSP maintained in certification and accreditation tool. 3. For the selected system, create formal risk acceptances for any security constraints the system is	**Closed** We obtained and inspected the SSP and determined that updates had been made to fully define the security control implementations for the Collateral system in accordance with CNSSI No. 1253. In addition, we obtained and inspected risk assessments for controls deviating from TD P 85-01 requirements. We noted that BEP management had approved these deviations.

	vulnerability scan tool used for the BEP collateral NSS. • sections required by NIST SP 800-18 guidance were missing, specifically document approval date and related laws, regulations, and policies date.	unable to meet since it runs on an isolated network. 4. For the selected system, ensure sure all appropriate sections are added to the SSP.	
Prior Year FY 2016 Finding # 1 – CNSS – Department Offices (DO) Collateral NSS SSP was not in accordance with CNSSI No.1253 guidance.	For a selected DO system, the SSP was not updated to address changes to the system's environment. Specifically, the SSP referenced out-of-date technology and did not discuss the implementation of new tools for continuous monitoring and compliance and audit logging. Additionally, DO management did not document in the SSP an updated system inventory of software or reference the current baseline configuration	We recommend that DO management: 1. For the selected system, ensure that the SSP is updated to address changes to the information system and environment. 2. For the selected system, ensure that the SSP documents an updated system inventory of software and references the current baseline configuration documents.	**Closed** We inspected the Collateral System SSP and noted that management updated the document to reflect the current environment. In addition, we noted the Collateral System software inventory and baseline documentation were current.
Prior Year FY 2016 Finding # 2 – CNSS – DO POA&Ms were not tracked in accordance with the CNSS No. 1253 guidance and Treasury requirements.	DO management did not regularly update and monitor progress towards remediating existing POA&Ms and did not close POA&Ms by the established milestones documented. DO management had a total of 77 POA&M items that were past due and were not updated nor provided justification of why they have not been closed during the FISMA reporting period of July 1, 2015 through June 30, 2016. In addition, the POA&M report did not adequately outline the	We recommend that CNSS DO management: 1. For the selected system, develop a process or mechanism to ensure that POA&Ms are being monitored and updated, as necessary, according to T DP 85-01guidance. 2. For the selected system, ensure POA&Ms are remediated accordingly with established milestones. If POA&Ms are not remediated, then POA&Ms should	**Closed** We inspected the Collateral System POA&M Report and noted management has a process in place to track, prioritize and remediate POA&Ms. In addition, we noted management adheres to milestone remediation dates and provides adequate justification for missed remediation dates.

	remedial actions with the updated dates and address the effectiveness of the remediation plan.	be updated with an adequate justification.	
Prior Year FY 2016 Finding # 3 – CNSS – BEP Vulnerability scans were not compliant with policies.	Vulnerability scans were not being conducted quarterly for the BEP collateral system, as outlined in the quarterly procedures. Specifically, for the system's hard drive inspected, we noted that BEP management only performed one vulnerability scan during the FISMA performance period of July 1, 2015 – June 30, 2016. The BEP collateral system is a moderate confidentiality, moderate integrity, and low availability system. Due to errors in the transition of the SSP to NIST SP 800-53, Rev. 4, the acceptance of quarterly scans in lieu of the TD P 85-01 prescribed scan frequency was not documented.	We recommend that BEP management: 1. For selected system, establish a process to ensure that vulnerability scans are conducted in accordance with the TD P 85-01 prescribed scan frequency or perform a risk assessment and obtain a formal risk acceptance to scan the system on a less-frequent basis.	**Closed** We obtained and inspected the Corrective Action Plan and noted that BEP decided to draft a formal risk acceptance for scanning the system on a less-frequent basis than defined in TD P 85-01. In addition, we obtained and inspected a formal risk acceptance and that the altered scanning timeline was approved by BEP management. Further, we inspected a hard drive for compliance with the new timeline and determined that scans were performed in accordance with the risk assessment.
Prior Year FY 2016 Finding # 4 – CNSS – DO Account management activities were not compliant with policies.	The TD P 85-01 and the system's SSP, require management to disable user's accounts that are inactive for more than 120 days. This control falls under the protect Cybersecurity domain, and the identity and access management FISMA program area. DO management failed to disable 91 users that were inactive for more than 120 days. In addition, 46 users had not logged into their account within	We recommend that DO management: 1. For the selected system, establish a process to review user accounts at a defined frequency but no less than every 120 days in accordance with TD P 85-01, and the system's SSP. 2. For the selected system, disable terminated or inactive DO	**Partially Implemented/Open** We inquired of management and noted that they have established an account review process; however, it was not effective. We noted that management manually reviews accounts every month to assess if they have not been logged into for 30 days. In the event they have not, they are disabled.

	120 days, and management did not disabled these user accounts. Additionally, one DO employee retained an active account to their system after being terminated.	employee or contractor's accounts accordingly. 3. For the selected system, configure or acquire additional system capability to disable user accounts automatically that have been inactive for more than 120 days of inactivity.	During our FY17 FISMA testing, we noted there were some terminated users who had active user accounts. Please refer to Finding #3 in the "Findings" section of this report.
Prior Year FY 2016 Finding #5 – CNSS – DO DO did not ensure proper completion of annual security awareness training for users of the collateral NSS.	DO Management did not ensure proper completion of annual security awareness training for 10 of the 25 users selected.	We recommend that DO management: 1. For the selected system, ensure that all users complete the annual security awareness training.	**Closed** During FY17 FISMA, we selected a sample of users and noted that all users sampled completed their annual security awareness training.

APPENDIX III – DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS' FISMA 2017 QUESTIONS FOR INSPECTORS GENERAL

The information included in Appendix III represents Department of the Treasury's (Treasury) Collateral National Security System (NSS) responses to Department of Homeland Security's (DHS) FISMA 2017 questions for Inspectors General. We prepared responses to DHS questions based on an assessment of two Collateral NSSs maintained by the Bureau of Engraving and Printing (BEP) and the Departmental Offices (DO). The scope of the FY 2017 Treasury Collateral NSS Performance Audit was limited to the two systems only, as the Collateral systems make up a subset of the overall Treasury information security program. Therefore, the assessed maturity levels reflect the effectiveness of Treasury's Collateral information system security program and security practices at the system levels, not the overall Department or bureaus' effectiveness. The assessed maturity levels for the Department are detailed in the FY 2017 Treasury FISMA Performance Audit Report for Unclassified Systems. 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 Collateral NSS security program and practices over Risk Management, Configuration Management, Identity and Access Management, Security Training, and Contingency Planning were at that self-assessed maturity level. We provided the assessed maturity level for each metric using the available options from CyberScope. In most cases if we determined that one or more Collateral NSSs had a finding related to the metric, we assessed the maturity level at 1 ("Ad Hoc") or 2 ("Defined"). For metrics that were assessed as maturity level 1, 2, or 3 ("Consistently Implemented"), we provided explanations in the "Comment" areas to explain why a maturity level 4 ("Management and Measurable") was not obtained.

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

Function 0 is the overall summary for the FISMA Performance Audit for Treasury. Functions 1–5 follow the 5 Cybersecurity Functions.

Function 0: Overall

0.1 Please provide an overall IG self-assessment rating:

Not Effective

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform to the grammatical and narrative structure of the Annual Report.

Comments: Consistent with applicable FISMA requirements, OMB and CNSS policy and guidelines, and NIST standards and guidelines, Treasury has established and maintained its information security program and practices for its collateral NSS for the five Cybersecurity Functions and seven FISMA program areas. However, the program was not fully effective as reflected by the deficiencies that we identified in the risk management, configuration management, identity and access management, and contingency planning metric domains. In addition, we did not assess any of the FISMA Metric Domains as Managed and Measurable (Level 4). The FY 2017 IG FISMA Reporting Metrics defines an effective information security program as Managed and Measurable (Level 4).

Function 1: Identify – Risk Management

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

Maturity Level: **Consistently Implemented (Level 3)** - The organization maintains a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third party systems), and system interconnections.

Comments: This is the highest level for this metric.

2 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network and uses this taxonomy to inform which assets can/cannot be introduced into the network.

Comments: To achieve Managed and Measureable Risk Management practices over the BEP and DO NSSs, Treasury should ensure that the hardware assets connected to the network are subject to the monitoring processes defined within the its ISCM strategy.

3 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment and uses this taxonomy to inform which assets can/cannot be introduced into the network.

Comments: To improve the Risk Management practices over the BEP and DO NSSs, Treasury should ensure that the software assets on the network (and their associated licenses) are subject to the monitoring processes defined within its ISCM strategy.

4 To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; and FIPS 199)?

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

Comments: This is the highest level for this metric.

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that include the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST 800-39; NIST 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; CFO Council ERM Playbook)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently implements its risk management policies, procedures, and strategy at the enterprise, business process, and information system levels. The organization uses its risk profile to facilitate a determination on the aggregate level and types of risk that management is willing to assume. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of risk management processes and activities to update the program.

Comments: To improve the Risk Management practices over the BEP and DO NSSs, Treasury should monitor and analyze its defined qualitative and quantitative performance measures on the effectiveness of its risk management strategy across disciplines. Treasury should collect, analyze and report information on the effectiveness of its risk management program.

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

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

Comments: This is the highest level for this metric.

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST 800-39: Section 2.3.1 and 2.3.2; NIST 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2, OMB A-123, CFO Council ERM Playbook)?

Maturity Level: **Consistently Implemented (Level 3)** - Roles and responsibilities of stakeholders involved in risk management have been defined and communicated across the organization. Stakeholders have adequate resources (people, processes, and technology) to effectively implement risk management activities.

Comments: To improve the Risk Management practices over the BEP and DO NSSs, Treasury should utilize an integrated risk management governance structure for implementing and overseeing an enterprise risk management (ERM) capability that manages risks from information security, strategic planning and strategic reviews, internal control activities, and applicable business areas.

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

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

Comments: To improve the Risk Management practices over BEP and DO NSSs, Treasury should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its POA&M activities and use that information to make appropriate adjustments, as needed to ensure that its risk posture is maintained.

9 To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing

(i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework
(ii) internal and external asset vulnerabilities, including through vulnerability scanning,
(iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and
(iv) selecting and implementing security controls to mitigate system-level risks (NIST 800-37; NIST 800-39; NIST 800-53: PL-2, RA-1; NIST 800-30; CSF:ID.RA-1 – 6)

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

Comments: To improve the Risk Management practices over the BEP and DO NSSs, Treasury should consistently monitor the effectiveness of risk responses to ensure that enterprise-wide risk tolerance is maintain at an appropriate level.

10 To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123)?

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

Comments: To improve the Risk Management practices over the BEP and DO NSSs, Treasury should employ robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization. The dashboard presents qualitative and quantitative metrics that provide indicators of risk.

11 To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (FAR Case 2007-004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, 52.239-1; President's Management Council; NIST 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2017 CIO FISMA Metrics: 1.7, 1.8).

Maturity Level: **Not Applicable**.

Comments: Both the BEP and DO Collateral Systems are not contractor systems. Refer to FY 2017 Treasury Unclassified FISMA Performance Audit Report for our assessed maturity level for the agency.

12 To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?

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

Comments: This metric is not applicable to the DO Collateral NSS due to its operational mission, and BEP self-assessed a maturity level of Defined (Level 2) for BEP Collateral NSS for this metric. Based on managements' combined self-assessment levels and the results of test work, we have assessed Treasury at Defined (Level 2) for its Collateral Systems.

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

Consistently Implemented (Level 3)

Comments: We determined that Treasury's Risk Management practices for the BEP and DO Collateral Systems did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.

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

Comments: We had no additional information that was not already covered in metric questions 1 to 12 above. According to DHS criteria, we assessed the Risk Management overall maturity level as ineffective. Please refer to 13.1 for explanation.

Function 2A: Protect – Configuration Management

14 To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800- 53: CM-1; SP 800-128: Section 2.4)?

Maturity Level: **Consistently Implemented (Level 3)** - Stakeholders have adequate resources (people, processes, and technology) to consistently implement information system configuration management activities.

Comments: To improve the Configuration Management (CM) practices over the BEP and DO NSSs, Treasury should assign personnel with responsibilities for developing and maintaining metrics on the effectiveness of information system configuration management activities. Treasury should collect, monitor, analyze, and update qualitative and quantitative performance measures across the agency and should report data on the effectiveness of the organization's information system configuration management program to the Chief Information Security Officer.

15 To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate location within an organization's SDLC;[6] configuration monitoring; and applying configuration management requirements to contracted systems (NIST 800-128: Section 2.3.2; NIST 800-53: CM-9)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization has consistently implemented an organization wide configuration management plan and has integrated its plan with its risk management and continuous monitoring programs. Further, the organization utilizes lessons learned in implementation to make improvements to its plan.

Comments: To improve CM practices over the BEP and DO NSSs, Treasury should monitor, analyze, and report to stakeholders the qualitative and quantitative performance measures on the effectiveness of its configuration management plan, should use this information to take corrective actions when necessary, and should ensure that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

16 To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53: CM-1; NIST 800-128: 2.2.1)

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently implements its policies and procedures for managing the configurations of its information systems. Further, the organization utilizes lessons learned in implementation to make improvements to its policies and procedures.

Comments: To improve the CM practices over the BEP and DO NSSs, Treasury should monitor, analyze, and report on the qualitative and quantitative performance measures on the effectiveness of its configuration management policies and procedures and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

[6] The Federal Information Systems Audit Manual (FISCAM) defines System Development Life Cycle (SDLC) methodology as the "policies and procedures that govern software development and modification as a software product goes through each phase of its life cycle."

17 To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53: CM-2, CM-8; FY 2017 CIO FISMA Metrics: 1.4, 1.5, and 2.1; CSF: ID.DE.CM-7)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently records, implements, and maintains under configuration control, baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures.

Comments: To improve CM practices of the BEP and DO NSSs, Treasury should employ automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit any security impact.

18 To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53: CM-6, CM-7, and SI-2; FY 2017 CIO FISMA Metrics: 2.2; SANS/CIS Top 20 Security Controls 3.7)?

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

Comments: DO did not maintain testing documentation and management approval of configuration changes and patches for implementation on the DO Collateral System.

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53: CM-3, SI-2; NIST 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20 Control 4.5; and DHS Binding Operational Directive 15-01)?

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

Comments: DO did not maintain testing documentation and management approval of configuration changes and patches for implementation on the DO Collateral System.

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

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

Comments: This is the highest level for this metric.

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

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

Comments: DO did not maintain testing documentation and management approval of configuration changes and patches for implementation on the DO Collateral System

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

Comments: We had no additional information that was not already covered in metric questions 14 to 21 above. According to DHS criteria, we assessed the Configuration Management overall maturity level as ineffective. Please refer to 39.1 for explanation.

Function 2B: Protect – Identity and Access Management

23 To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST 800-53: AC-1, IA-1, PS-1; and the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Maturity Level: **Defined (Level 2)** - Roles and responsibilities at the organizational and information system levels for stakeholders involved in ICAM have been fully defined and communicated across the organization. This includes, as appropriate, developing an ICAM governance structure to align and consolidate the agency's ICAM investments, monitoring programs, and ensuring awareness and understanding.

Comments: To improve the Identity and Access Management (IA) practices over the BEP and DO NSSs, Treasury should assign personnel with responsibilities for developing, managing, and monitoring metrics on the effectiveness of Identity, Credentialing, and Access, Management (ICAM) activities. The assigned personnel should consistently collect, monitor, and analyze qualitative and quantitative performance measures across the organization and should report data on the effectiveness of the organization's identity, credential, and access management program.

24 To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?

Maturity Level: **Defined (Level 2)** - The organization has defined its ICAM strategy and developed milestones for how it plans to align with Federal initiatives, including strong authentication, the FICAM segment architecture, and phase 2 of DHS's Continuous Diagnostics Mitigation (CDM) program, as appropriate.

Comments: This metric was not applicable to the BEP Collateral system as management indicated that it follows the unclassified BEP policies, procedures, and practices. DO management self-assessed a maturity level of Ad Hoc (Level 1) for the DO Collateral NSS this metric. Based on the results of test work, we have assessed Treasury at Ad Hoc (Level 1) for the DO Collateral System.

25 To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 27 through 31) (NIST 800-53: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); and SANS/CIS Top 20: 14.1)?

Maturity Level: **Defined (Level 2)** - The organization has developed, documented, and disseminated its policies and procedures for ICAM. Policies and procedures have been tailored to the organization's environment and include specific requirements.

Comments: The DO Collateral System did not disable current users after 30 days of inactivity, and the system did not disable new users that had not logged into the Collateral System within 30 days, as by the system security plan. In addition, DO did not remove or disable the accounts of terminated DO Collateral users.

26 To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53: PS-2, PS- 3; and National Insider Threat Policy)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically.

Comments: To improve IA practices over the BEP and DO NSSs, Treasury should employ automation to document and track centrally and share risk designations and screening information with necessary parties, as appropriate.

27 To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non- privileged users) that access its systems are completed and maintained (NIST SP 800-53: AC-8, PL-4, and PS-6)?

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

Comments: This is the highest level for this metric.

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

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

Comments: This metric was not applicable to the BEP Collateral system based on its configuration. DO management self-assessed a maturity level of Defined (Level 2) for the DO Collateral NSS this metric. Based on the results of test work, we have assessed Treasury at Defined (Level 2) for the DO Collateral System.

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

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

Comments: This metric was not applicable to the BEP Collateral system based on its configuration. DO management self-assessed a maturity level of Defined (Level 2) for the DO Collateral NSS this metric. Based on the results of test work, we have assessed Treasury at Defined (Level 2) for the DO Collateral System.

30 To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2017 CIO FISMA metrics: Section 2; NIST SP 800-53: AC-1, AC-2 (2), AC-17; CSIP)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization ensures that its processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. The organization limits the functions that can be performed when using privileged accounts; limits the duration that privileged accounts can be logged in; limits the privileged functions that can be performed using remote access; and ensures that privileged user activities are logged and periodically reviewed.

Comments: The FY 2016 DO Finding #4 regarding DO Collateral system's user accounts were inactive for more than 120 days remained open.

31 To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53: AC-17, SI-4; and FY 2017 CIO FISMA Metrics: Section 2)?

Maturity Level: **Not Applicable**

Comments: Based on the nature and configuration of both DO and BEP Collateral Systems, this metric is not applicable at the system-level. Refer to FY 2017 Treasury Unclassified FISMA Performance Audit Report for our assessed maturity level for the agency.

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

Comments: DO self-identified deficiencies in the following POA&Ms: (a) #T-006 related to lack of multifactor authentication for the DO Collateral system, and (b) #242 management has not implemented a Security Event Information Manager (SIEM). According to DHS criteria, we assessed the Identity and Access Management overall maturity level as ineffective. Please refer to 39.1 for explanation.

Function 2C: Protect – Security Training

33 To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST 800-53: AT-1; and NIST SP 800-50)?

Maturity Level: **Consistently Implemented (Level 3)** - Roles and responsibilities for stakeholders involved in the organization's security awareness and training program have been defined and communicated across the organization. In addition, stakeholders have adequate resources (people, processes, and technology) to consistently implement security awareness and training responsibilities.

Comments: To improve the Security Training (ST) practices over the BEP and DO NSSs, Treasury should assign responsibility for monitoring and tracking the effectiveness of security awareness and training activities. The assigned personnel should consistently collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of security awareness and training activities.

34 To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST 800-53: AT-2 and AT-3; NIST 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181 (Draft); and CIS/SANS Top 20: 17.1)?

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

Comments: The FY 2016 DO Finding #4 regarding DO Management not ensuring proper completion of annual security awareness training remained open.

35 To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST 800-53: AT-1; NIST 800-50: Section 3))

Maturity Level: **Consistently Implemented (Level 3)** - The organization has consistently implemented its organization-wide security awareness and training strategy and plan.

Comments: To improve the ST practices over the BEP and DO NSSs, Treasury should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. Treasury should ensure that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

36 To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity questions 37 and 38 below) (NIST 800-53: AT-1 through AT-4; and NIST 800-50)

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

Comments: To improve the ST practices over the BEP and DO NSSs, Treasury should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures. Treasury should ensure that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

37 To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: Awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST 800-53: AT-2; FY 17 CIO FISMA Metrics: 2.23; NIST 800-50: 6.2; SANS Top 20: 17.4)

Maturity Level: **Consistently Implemented (Level 3)** - The organization ensures that all systems users complete the organization's security awareness training (or a comparable awareness training for contractors) prior to system access and periodically thereafter and maintains completion records. The organization obtains feedback on its security awareness and training program and uses that information to make improvements.

Comments: The FY 2016 DO Finding #4 regarding DO Management not ensuring proper completion of annual security awareness training remained open.

38 To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST 800-53: AT-3 and AT-4; FY 17 CIO FISMA Metrics: 2.23)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization ensures individuals with significant security responsibilities are provided specialized security training prior to information system access or performing assigned duties and periodically thereafter and maintains appropriate records. Furthermore, the organization maintains specialized security training completion records.

Comments: To improve the ST practices over the BEP and DO NSSs, Treasury should obtain feedback on its security training content and make updates to its program, as appropriate. In addition, Treasury should measure the effectiveness of its specialized security training program and following up with additional awareness or training, and/or disciplinary action, as appropriate.

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

Consistently Implemented (Level 3)

Comments: We determined that Treasury's Configuration Management, Identity and Access Management, and Security Training practices for the BEP and DO Collateral Systems did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.

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

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

Function 3: Detect – ISCM

40 To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM (NIST SP 800-137: Sections 3.1 and 3.6)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization's ISCM strategy is consistently implemented at the organization/business process and information system levels. In addition, the strategy supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captures lessons learned to make improvements to the ISCM strategy.

Comments: To improve the ISCM practices over the BEP and DO NSSs, Treasury should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its ISCM strategy and makes updates, as appropriate. Treasury should ensure that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

41 To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53: CA-7). (Note: The overall maturity level should take into consideration the maturity of question 43)

Maturity Level: **Consistently Implemented (Level 3)** - The organization's ISCM policies and procedures have been consistently implemented for the specified areas. The organization also consistently captures lessons learned to make improvements to the ISCM policies and procedures.

Comments: BEP management self-assessed a maturity level of Defined (Level 2) for the BEP Collateral NSS this metric, and DO management self-assessed a maturity level of Consistently Implemented (Level 3) for the DO Collateral NSS. Based on the results of test work, we have assessed Treasury at Defined (Level 2) for its Collateral Systems.

42 To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53: CA-1; NIST SP 800-137; and FY 2017 CIO FISMA Metrics)?

Maturity Level: **Consistently Implemented (Level 3)** - Defined roles and responsibilities are consistently implemented and teams have adequate resources (people, processes, and technology) to effectively implement ISCM activities.

Comments: To enhance its ISCM practices for the BEP and DO Collateral NSSs, Treasury should consistently collect, monitor, and analyze qualitative and quantitative performance measures across the agency and report data on the effectiveness of the Treasury's ISCM program.

43 How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800-137: Section 2.2; NIST SP 800-53: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization has consistently implemented its processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls to provide a view of the organizational security posture as well as each system's contribution to said security posture. All security control classes (management, operational, technical) and types (common, hybrid, and system-specific) are assessed and monitored.

Comments: To improve the ISCM practices over the BEP and DO NSSs, Treasury should utilize the results of security control assessments and monitoring to maintain ongoing authorizations of information systems.

44 How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?

Maturity Level: **Consistently Implemented (Level 3) –** The organization has consistently implemented its process for performing ongoing security control assessments, granting system access authorizations, and monitoring security to provide a view of the organization security posture as well as each system's contribution to said security posture. All security control classes (management, operational, technical) and types (common, hybrid, and system-specific) are assessed and monitored.

Comments: To improve its ISCM practices for the BEP and DO Collateral NSSs, Treasury should utilize the results of security control assessments and monitoring to maintain ongoing authorizations of information systems.

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

Consistently Implemented (Level 3)

Comments: We determined that Treasury's Information Security Continuous Monitoring practices for the BEP and DO Collateral Systems did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.

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

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

Function 4: Respond – Incident Response

46 To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53: IR-1; NIST 800-61 Rev. 2; FY 2017 CIO FISMA Metrics: 4.1, 4.3, and 4.6)? (Note: The overall maturity level should take into consideration the maturity of questions 48 - -52)

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently implements its incident response policies, procedures, plans, and strategies. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident response policies, procedures, strategy, and processes to update the program.

Comments: To improve the Incident Response (IR) practices over the BEP and DO NSSs, Treasury should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies, as appropriate.

47 To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-16-03; OMB M-16-04; FY 2017 CIO FISMA Metrics: 1.6 and 4.5; and US-CERT Federal Incident Notification Guidelines)?

Maturity Level: **Defined (Level 2)** – The organization has defined and communicated the structures of its incident response teams, roles, and responsibilities of incident response stakeholders, and associated levels of authority and dependencies. In addition, the organization has designated a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities.

Comments: DO management self-identified a deficiency in POA&M #242 relating to management not implementing a Security Event Information Manager (SIEM) for the DO Collateral NSS environment.

48 How mature are the organization's processes for incident detection and analysis (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; US- CERT Incident Response Guidelines)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently utilizes its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements, and analyzes precursors and indicators generated by, for example, the following technologies: intrusion detection/prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity checking software.

Comments: To improve the IR practices over the BEP and DO NSSs, Treasury should utilize profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. Through profiling techniques, Treasury should maintain a comprehensive baseline of network operations and expected data flows for users and systems.

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

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently implements its containment strategies, incident eradication processes, processes to remediate vulnerabilities that may have been exploited on the target system(s), and recovers system operations.

Comments: To improve the IR practices over the BEP and DO NSSs, Treasury should manage and measure the impact of successful incidents and should be able to mitigate related vulnerabilities quickly on other systems so that they are not subject to exploitation of the same vulnerability.

50 To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-16-03; NIST 800-53: IR-6; US-CERT Incident Notification Guidelines)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently shares information on incident activities with internal stakeholders. The organization ensures that security incidents are reported to US-CERT, law enforcement, the Office of Inspector General, and the Congress (for major incidents) in a timely manner.

Comments: To improve the IR practices over the BEP and DO NSSs, Treasury should use incident response metrics to measure and manage the timely reporting of incident information to its officials and external stakeholders.

51 To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents and enter into contracts, as appropriate, for incident response support (FY 2017 CIO FISMA Metrics: 4.4; NIST SP 800-86)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently utilizes on-site, technical assistance/surge capabilities offered by DHS or ensures that such capabilities are in place and can be leveraged when needed. In addition, the organization has entered into contractual relationships in support of incident response processes (e.g., for forensic support), as needed. The organization is utilizing DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its network.

Comments: This metric is not applicable to the DO Collateral system based on its environment and mission. For BEP Collateral, this is the high level for this metric.

52 To what degree does the organization utilize the following technology to support its incident response program?

- Web application protections, such as web application firewalls
- Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools
- Aggregation and analysis, such as security information and event management (SIEM) products
- Malware detection, such as antivirus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2)

Maturity Level: **Consistently Implemented (Level 3)** - The organization has consistently implemented its defined incident response technologies in the specified areas. In addition, the technologies utilized are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans.

Comments: To improve the IR practices over the BEP and DO NSSs, Treasury should use technologies for monitoring and analyzing qualitative and quantitative performance across the agency and should collect, analyze, and report data on the effectiveness of its technologies for performing incident response activities.

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

Consistently Implemented (Level 3)

Comments: We determined that Treasury's Incident Response practices for the BEP and DO Collateral Systems did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.

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

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

Function 5: Recover – Contingency Planning

54 To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST 800-53: CP-1 and CP-2; NIST 800-34; NIST 800-84; FCD-1: Annex B)?

Maturity Level: **Consistently Implemented (Level 3)** - Roles and responsibilities of stakeholders involved in information system contingency planning have been fully defined and communicated across the organization. In addition, the organization has established appropriate teams that are ready to implement its information system contingency planning strategies. Stakeholders and teams have adequate resources (people, processes, and technology) to effectively implement system contingency planning activities.

Comments: To improve the Contingency Planning (CP) practices over the BEP and DO NSSs, Treasury should assign responsibility for monitoring and tracking the effectiveness of information systems contingency planning activities. Treasury should collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of information system contingency planning program activities, including validating the operability of an IT system or system component to support essential functions during a continuity event.

55 To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate? (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 56-60) (NIST SP 800-34; NIST SP 800-161).

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently implements its defined information system contingency planning policies, procedures, and strategies. In addition, the organization consistently implements technical contingency planning considerations for specific types of systems, including but not limited to methods such as server clustering and disk mirroring. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of information system contingency planning policies, procedures, strategy, and processes to update the program.

Comments: To improve the CP practices over the BEP and DO NSSs, Treasury should understand and manage its information and communications technology (ICT) supply chain risks related to contingency planning activities. As appropriate, Treasury should integrate ICT supply chain concerns into its contingency planning policies and procedures, define and implements a contingency plan for ICT supply chain infrastructure, applies appropriate ICT supply chain controls to alternate storage and processing sites, and consider alternate telecommunication services providers for its ICT supply chain infrastructure to support critical information systems.

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

Maturity Level: **Defined (Level 2)** - Processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts have been defined.

Comments: For Metric 56, both BEP and DO management self-assessed maturity levels of Defined (Level 2) for the BEP and DO Collateral systems. In addition, the DO Collateral System BIA was not current and did not reflect the current operating environment. Based on managements' combined self-assessment levels and the results of test work, we have assessed Treasury at Ad Hoc (Level 1) for its Collateral Systems.

57 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST 800-53: CP-2; NIST 800-34)?

Maturity Level: **Consistently Implemented (Level 3)** - Information system contingency plans are consistently developed and implemented for systems, as appropriate, and include organizational and system level considerations for the following phases: activation and notification, recovery, and reconstitution. In addition, system level contingency planning development/maintenance activities are integrated with other continuity areas including organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan (as appropriate), and occupant emergency plans.

Comments: To improve the CP practices over the BEP and DO NSSs, Treasury should be able to integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency, as appropriate to deliver persistent situational awareness across the organization.

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

Maturity Level: **Consistently Implemented (Level 3)** - Processes for information system contingency plan testing and exercises are consistently implemented. ISCP testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP[7]/BCP.[8]

Comments: To improve the CP practices over the BEP and DO NSSs, Treasury should employ automated mechanisms to test system contingency plans more thoroughly and effectively.

59 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST 800-53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD1; NIST CSF: PR.IP- 4; and NARA guidance on information systems security records)?

Maturity Level: **Defined (Level 2)** - Processes, strategies, and technologies for information system backup and storage, including use of alternate storage and processing sites and RAID,[9] as appropriate, have been defined. The organization has considered alternative approaches when developing its backup and storage strategies, including cost, maximum downtimes, recovery priorities, and integration with other contingency plans.

Comments: The DO Collateral System BIA was not current and did not reflect the current operating environment.

60 To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST 800-53: CP-2, IR-4)?

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

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

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

Maturity Level: **Consistently Implemented (Level 3)** - Information on the planning and performance of recovery activities is consistently communicated to relevant stakeholders and executive management teams, who utilize the information to make risk based decisions.

Comments: To improve the CP practices over the BEP and DO NSSs, Treasury should communicate metrics on the effectiveness of recovery activities to relevant stakeholders, and Treasury should ensure that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.

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

Consistently Implemented (Level 3)

Comments: We determined that Treasury's Contingency Planning practices for the BEP and DO Collateral Systems did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.

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

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

Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count[10]
Ad-Hoc	0
Defined	1
Consistently Implemented	10
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	6
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

[10] As explained in the Metric 31 comment in Appendix III , one RM metric was not applicable to both BEP and DO Collateral NSSs as they systems are managed at Treasury, not a third party. As a result, the total metrics assessed for Risk Management totaled to ten.

Function 2B: Protect - Identity and Access Management

Function	Count[11]
Ad-Hoc	0
Defined	5
Consistently Implemented	3
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Function 2C: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	6
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

[11] As explained in the Metric 31 comment in Appendix III, one IA metric did not apply to both DO and BEP Collateral Systems. As such, we are only counting eight applicable metrics for IA.

Function 3: Detect - ISCM

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

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	6
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's Risk Management practices for the BEP and DO Collateral Systems did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 2: Protect - Configuration Management/Identity Management/Security Training	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's Configuration Management, Identity and Access Management, and Security Training practices for the BEP and DO Collateral Systems did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 3: Detect - ISCM	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's Information Security Continuous Monitoring practices for the BEP and DO Collateral Systems did not meet

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
			the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's Incident Reponses practices for the BEP and DO Collateral Systems did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that Treasury's Configuration Management practices for the BEP and DO Collateral Systems did not meet the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.
Overall	Not Effective	Not Effective	Consistent with applicable FISMA requirements, OMB and CNSS policy and guidelines, and NIST standards and guidelines, Treasury has established and maintained its information security program and practices for its collateral NSS for the five Cybersecurity Functions and seven FISMA program areas. However, the program was not fully effective as reflected deficiencies that we identified in risk management, configuration management, identity and access management, and contingency planning. In addition, we did not assess any of the FISMA Metric Domains as Managed and Measurable (Level 4).

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
			The FY 2017 IG FISMA Reporting Metrics defines an effective information security programs as Managed and Measurable (Level 4).

APPENDIX IV – GLOSSARY OF TERMS

Acronym	Definition
AC	Access Control
ACAS	Assured Compliance Assessment Solution
AICPA	American Institute of Certified Public Accounts
AT	Awareness and Training
BCP	Business Continuity Planning
BEP	Bureau of Engraving and Printing
BIA	Business Impact Analysis
CA	Security Assessment and Authorization
CCB	Control Change Board
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CM	Configuration Management
CNSS	Committee on National Security Systems
COOP	Continuity of Operation Plan
CP	Contingency Planning
CS	Contractor Systems
CSF	Cyber Security Framework
CSIP	Cybersecurity Strategy and Implementation Plan
Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity
DHS	Department of Homeland Security
DO	Departmental Offices
FAR	Federal Acquisition Regulation
FCD	Federal Continuity Directive
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
HSPD	Homeland Security Presidential Directive
HBSS	Host Base Security System
IA	Identity and Access Management
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IGs	Inspector General's
IR	Incident Reporting
ISCM	Information Security Continuous Monitoring
IT	Information Technology
KPMG	KPMG LLP

Acronym	Definition
MD	Maximum Tolerable Downtime
NIST	National Institute of Standards and Technology
NSS	National Security System
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
RAID	Redundant Array of Independent Disks
Rev.	Revision
RM	Risk Management
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SA	System and Services Acquisition
SA&A	Security Assessment and Security
SI	System and Information Integrity
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SSP	System Security Plan
SP	Special Publication
ST	Security Training
TD P	Treasury Directive Publication
TIC	Trusted Internet Connection
Treasury	Department of the Treasury
US-CERT	United States Computer Emergency Readiness Team

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