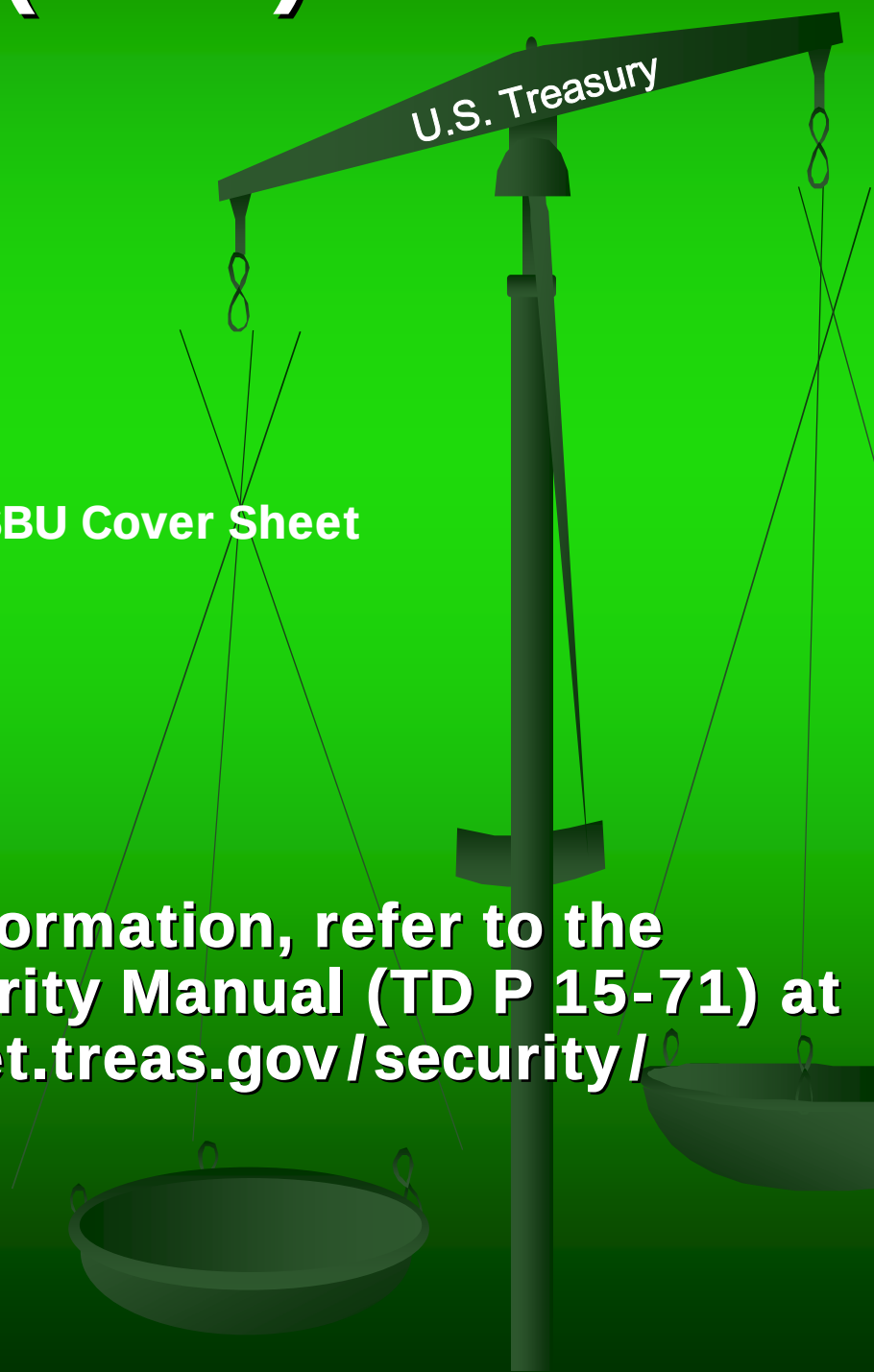
SENSITIVE BUT UNCLASSIFIED (SBU)



SBU Cover Sheet

For further information, refer to the Treasury Security Manual (TD P 15-71) at http://intranet.treas.gov/security/

TD F 15-05.11 (3/07)

This Page Intentionally Left Blank

Audit Report

OIG-19-008

INFORMATION TECHNOLOGY: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2018 Performance Audit for Collateral National Security Systems

October 31, 2018

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 31, 2018

MEMORANDUM FOR **DAVID F. EISNER**
ASSISTANT SECRETARY FOR MANAGEMENT

ERIC OLSON
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 2018 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 2018 Performance Audit for the Collateral National Security Systems*, dated October 31, 2018. 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 its information security program and practices for its collateral national security systems for the 5 Cybersecurity Functions and 8 FISMA program areas. However, the program was not effective as KPMG identified 4 deficiencies within 3 of the 5 Cybersecurity Functions and within 3 of the 8 FISMA program areas. Accordingly, KPMG made 9 recommendations to address these deficiencies.

Appendix III of the attached KPMG report includes *Department of the Treasury's Consolidated Response to DHS's FISMA 2018 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 2018 Performance Audit for the
Collateral National Security Systems

October 31, 2018

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

Department of the Treasury

Federal Information Security Modernization Act Fiscal Year 2018 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 2018 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) Collateral National Security Systems (NSS) 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 2018 Questions for Inspectors General*, dated May 24, 2018. 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. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objective of this performance audit was to assess the effectiveness of the Treasury's information security program and practices for its collateral NSS for the period July 1, 2017 through June 30, 2018. As part of our audit, we responded to the DHS *FISMA 2018 Questions for Inspectors General*, dated May 24, 2018, and assessed the maturity levels on behalf of the Treasury OIG. Additional details regarding the scope of our independent audit are included in Appendix I, *Objective, 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 to DHS's FISMA 2018 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 8 FISMA Metric Domains[2]. However, the program was not effective according to DHS criteria and as reflected in the 4 deficiencies within 3 of the 5 Cybersecurity Functions and within 3 of the 8 FISMA Metric Domains program areas identified as follows:

Cybersecurity Function: Identify:

1. The Security Controls in the Bureau of Engraving and Printing (BEP) and the Departmental Offices (DO) collateral System Security Plans (SSPs) were not defined and implemented in accordance with the Committee on National Security Systems Instruction (CNSSI) 1253, *Security Categorization and Control Selection for National Security Systems*, Bureau Information Security Policies, Treasury Directive Publication (TD P) 85-01, *Department of the Treasury Information Technology Security Policy,* Appendix B, "Initial Security Control Set for Non-Intelligence National Security Systems and Information," and NIST. (Risk Management)
2. Plans of Actions and Milestones (POA&Ms) were not documented appropriately for DO's collateral NSS. (Risk Management).

Cybersecurity Function: Protect

3. DO's collateral NSS access authorization and review controls need enhancement. (Identity and Access Management)

Cybersecurity Function: Respond

4. DO's collateral NSS Incident Response Plan was not reviewed. (Incident Response)

We made 9 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 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 31, 2018

---

1 OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency developed the Fiscal Year (FY) 2018 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. The eight IG FISMA Metric Domains are 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's *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0.1,* the eight FISMA Metric Domains are: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

BACKGROUND

Federal Information Security Modernization Act of 2014

FISMA focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. 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 IGs in complying with requirements of FISMA. The act is supported by OMB, DHS, agency security policy, and risk-based standards and guidelines published by NIST related to information security practices.

FISMA defines a 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 OIG.

FY 2018 IG FISMA Reporting Metrics

For fiscal year (FY) 2018, OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) organized the *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0.1* (FY 2018 IG FISMA Reporting Metrics) 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, the FY 2018 IG FISMA Reporting Metrics use the CIGIE maturity models for the eight metric domains: Risk Management (RM), Configuration Management (CM), Identity and Access Management (IA), Data Protection and Privacy (DP), Security Training (ST), Information Security Continuous Monitoring (ISCM), Incident Response (IR), and Contingency Planning (CP). **Table 1** shows the alignment between the Cybersecurity Framework and the FISMA Metric Domains.

Table 1: *Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FY 2018 IG FISMA Metric Domains*

Cybersecurity Framework Security Functions	FY 2018 IG FISMA Metric Domains
Identify	Risk Management
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

In FY 2018, CIGIE added the Data Protection and Privacy FISMA Metric Domain, which included 5 additional questions. The maturity level for a domain is determined by a simple majority, where the most frequent level across the questions will serve as the domain rating. A security program is considered effective if it is at Level 4, Managed and Measurable.

Table 2: *Inspector General Assessment Maturity Levels*

Maturity Level	Maturity Level Description
Level 1 Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2 Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3 Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4 Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5 Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

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. 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. TD P 85-01, *Department of the Treasury Information Technology Security Policy*, Appendix B*,* "Initial Security Control Set for Non-Intelligence National Security Systems and Information," provides Treasury security policy and standards for all systems that process or communicate classified national security information.

We reviewed both collateral NSSs; one managed by DO and one managed by BEP.

Department of the Treasury Information Security Management Program

Treasury Office of the Chief Information Officer

The Treasury 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 Information Technology (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** – Provides incident reporting with external reporting entities and conducts performance monitoring and analyses of the Computer Security Incident Response Center within Treasury and each bureau's Computer Security Incident Response Center.
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, 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 FISMA requirements, OMB policy, the CNSS policy and guidance, and NIST standards and guidelines, Treasury established and maintained its information system security program and practices for its collateral NSS for the 5 Cybersecurity functions and 8 FISMA metric domains. The FISMA program areas are outlined in the FY 2018 IG FISMA Reporting Metrics and were prepared by DHS Office of Cybersecurity and Communications Federal Network Resilience. The 8 FISMA metric domains, are Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, 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 3 out of the 8 FISMA metric domains (risk management, configuration management, identity and access management, and security training) that needed improvement.

We have made 9 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 FY 2017 FISMA performance audit and noted that management closed 2 of 5 findings. See Appendix II*, Status of Prior-Year Findings*, for additional details.

In a written response to this report, the Deputy Assistant Secretary for Information Systems and CIO agreed with our findings and recommendations and provided planned corrective actions that were responsive to the intent of our recommendations (see Management Response).

FINDINGS

1. The Security Controls in BEP's and DO's Collateral System Security Plans (SSPs) were not defined and implemented in accordance with CNSSI 1253, Bureau Information Security Policies, TD P 85-01, and NIST.

The CNSS Instruction No. 1253, NIST SP 800-53, Rev.4, TD P 85-01 Appendix B, and the bureau specific policies, BEP Minimum Standard Parameters and Departmental Offices Information Technology Security Handbook (DO P-910), require the organization to develop system security plans for information systems that are consistent with the organization's enterprise architecture and 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 FISMA Metric Domain. We noted the following:

- BEP management did not fully implement the required security controls and control enhancements in the BEP Collateral SSP in accordance with CNSSI 1253, NIST SP 800-53, Rev. 4, NIST SP 800-37, NIST SP 800-18, TD P 85-01, the BEP Minimum Standard Parameters and did not create POA&Ms to address the following deficiencies:
  - 3 of 159 controls were not implemented.
  - 26 of 159 controls were partially implemented.
- DO management did not fully implement the required security controls and control enhancements in the DO Collateral System SSP based on the DO Collateral System categorization in accordance with CNSSI 1253, NIST SP 800-53, Rev. 4, NIST SP 800-37, NIST SP 800-18, TD P 85-01 and the DO P-910 and did not create POA&Ms to address the following deficiencies:
  - 18 of 159 controls were not implemented,
  - 15 of 159 controls were partially implemented, and
  - 43 of 159 controls did not have the control enhancements implemented.

For both collateral NSS, due to lack of management oversight and funding, DO management and BEP management stated that they did not commit the resources to implement the required security controls and control enhancements and document them in both the DO Collateral and BEP Collateral SSP, respectively. SSPs provide guidance over controls implemented over the information system. Inaccurate documentation in the SSP could lead to a misunderstanding of the information system control environment, which could lead to improper control implementation, thus causing a vulnerability to threats. *(See recommendations #1 and 2 for BEP and #3 and 4 for DO.)*

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

1. For the BEP collateral NSS, implement an ongoing oversight process and commit resources to ensure that required security controls and control enhancements are implemented and documented in the BEP Collateral SSP as required by BEP Minimum Standard Parameters, TD P 85-01, CNSSI 1253, and NIST SP 800-53, Rev. 4.

   Management Response: BEP management will implement an ongoing oversight process and commit resources to review the security controls and enhancements documented in the System Security Plan (SSP) for the BEP Collateral system. BEP management will ensure all missing or partially implemented controls are properly reported and tested based on the security categorization level, BEP Minimum Standard Parameters, TD P 85-01, CNSSI 1253, and NIST SP 800-53 Rev. 4. Target completion date: May 1, 2019.

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

2. For the BEP collateral NSS, a POA&M should be created for controls and control enhancements not implemented in the DO Collateral SSP.

   Management Response: BEP management will create a POA&M to track the identified findings. Target Completion Date: November 15, 2018.

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

3. For the DO collateral NSS, validate that it has implemented the required security controls and documented the controls implementation statuses and control enhancements in the DO Collateral SSP as required by DO P-910, TD P 85-01, CNSSI 1253, and NIST SP 800-53 Rev. 4.

   Management Response: DO management will update DO P 910 to clarify that it applies to unclassified systems only. The DO Collateral system program will update the SSP to include control enhancements as applicable and will then test all controls added to the SSP. A POA&M will be created for any controls found not to be implemented, or partially implemented. Target completion date: June 30, 2019.

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

4. For the DO collateral NSS, a POA&M should be created for controls and control enhancements not implemented in the DO Collateral SSP.

   Management Response: DO management will update DO P 910 to clarify that it applies to unclassified systems only. The DO Collateral system program will update the SSP to include control enhancements as applicable and will then test all controls

added to the SSP. A POA&M will be created for any controls found not to be implemented, or partially implemented. Target completion date: June 30, 2019.

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

2. POA&Ms were not documented appropriately for the DO collateral NSS.

The TD P 85-01, Appendix B requires the organization to develop POA&Ms for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of security controls and to reduce or eliminate known vulnerabilities in the systems. The organization should update the existing POA&M at least quarterly based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. In addition TD P 85-01, Appendix B, requires the organization to implement a process for ensuring that POA&Ms for the security program and associated organizational information systems are developed and maintained; that they document the remedial information security actions to respond adequately to the risk to the organizational operations and assets, individuals, other organizations, and the Nation; and that POA&Ms are reported in accordance with OMB's FISMA reporting requirements. Furthermore, the organization should update the DO P-910 and define which element should be documented for a POA&M and review the POA&Ms for consistency with the organizational risk management strategy and organization-wide priorities for the risk response. This control falls under the Identify Cybersecurity area, and the Risk Management FISMA Metric Domain. We noted the following:

- DO management did not document the required information in the DO Collateral POA&Ms, which was noted in the following exceptions:
    - Management did not include milestone changes for 2 of 50 open POA&Ms.
    - 5 of 50 open POA&Ms were overdue without a justification for not completing the POA&Ms on time:
        - 4 of 5 were due as of May 1, 2018, and
        - 1 of 5 was due as of May 20, 2018.
    - 20 of 50 open POA&Ms did not have a completion date documented.

In addition, DO management did not create POA&Ms for the weaknesses identified in the Security Assessment Report (SAR) that was completed on August 2, 2017.

Due to limited funding, DO management stated that they did not have the required resources to create POA&Ms for the weaknesses identified in the SAR. Lack of POA&Ms for identified weaknesses could lead to security weaknesses and vulnerabilities not being remediated in a timely manner, thereby increasing risk of unauthorized access, use, and/or modification of the DO Collateral System resources. *(See recommendations #5 and 6.)*

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

5. Update the DO P-910 to establish the elements that should be documented for a POA&M and to ensure that all proper sections of the POA&Ms are completed.

   Management Response: DO management will update DO P 910 to clarify that it applies to unclassified systems only. The DO Collateral system program will update the SSP to identify the appropriate policy for what information is to be documented in the system's POA&M. The DO Collateral system program has completed a new risk assessment as of September 28, 2018. This risk assessment includes all weaknesses from the existing POA&M as well as all weaknesses still open from the SAR that was completed in August 2017. Working with the DO Collateral system Program Office, the system's Cyber Security Operations team will develop a new POA&M based on this risk assessment. The new POA&M will:

   - Include all columns required by applicable policy.
   - Include milestone dates based on availability of funding and resources to ensure timely completion of activities.
   - Include a planned completion data based on the documented milestones.

   Target Completion date: January 31, 2019.

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

6. Create POA&Ms for the weaknesses and vulnerabilities identified in the SAR.

   Management Response: DO management will update DO P 910 to clarify that it applies to unclassified systems only. The DO Collateral system program will update the SSP to identify the appropriate policy for what information is to be documented in the system's POA&M. The DO Collateral system program has completed a new risk assessment as of September 28, 2018. This risk assessment includes all weaknesses from the existing POA&M as well as all weaknesses still open from the SAR that was completed in August 2017. Working with the DO Collateral system Program Office, the system's Cyber Security Operations team will develop a new POA&M based on this risk assessment. The new POA&M will:

   - Include all columns required by applicable policy.
   - Include milestone dates based on availability of funding and resources to ensure timely completion of activities.
   - Include a planned completion data based on the documented milestones.

   Target Completion date: January 31, 2019.

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

3. DO Collateral NSS user access authorization and review controls need enhancement.

Both NIST SP 800-53, Rev. 4 and TD P 85-01, Appendix B, require bureaus and offices to 1) create, enable, modify, disable, and remove information system accounts and to monitor the users of information system accounts; 2) notify account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes; and 3) review accounts for compliance with bureau- and office-defined account management requirements. NIST SP 800-53, Rev. 4 and TD P 85-01 also require bureaus and offices to explicitly define access to organization-defined security functions and security-relevant information. This control falls under the Protect Cybersecurity domain and the Identity and Access Management FISMA Metric Domain. We noted the following:

- For the DO collateral NSS, DO management did not:
  - Perform annual non-privileged and semi-annual privileged user access reviews and recertifications; and
  - Retain access authorization records for 2 of 5 new privileged users.

Due to competing priorities, DO management stated that they did not perform the annual/semi-annual review and recertification of DO collateral NSS non-privileged and privileged user accounts to ensure access was commensurate with assigned responsibilities. Additionally, DO management stated that new privileged user access authorization forms were approved and granted for the two privileged users; however, due to lack of management oversight, management was unable to locate the supporting documentation. Failing to properly retain user access authorization could allow for unauthorized access to the DO collateral NSS. If privileged user authorizations are not tracked and centrally retained, and user access is not periodically reviewed, the risk of unauthorized user gaining access to the system is increased. *(See recommendations #7 and 8.)*

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

7. Implement an ongoing oversight process to ensure that DO collateral NSS non-privileged and privileged user accounts are authorized before granting them access to the system and that privileged and non-privileged accounts are reviewed and recertified on a periodic basis stipulated by TD P 85-01 to ensure user access is commensurate with assigned responsibilities.

   Management Response: The DO Collateral system program will initiate a program to monitor and review privileged accounts. This program will follow documented procedures to include appropriate documentation.

   The DO Collateral system program will identify resource requirements for a program to monitor and review non-privileged users accounts and request additional resources as needed. Upon implementation, this program will follow documented procedures to include appropriate documentation. Target completion date: June 30, 2019.

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

8. Retain supporting documentation evidencing completion of user access authorization and review and recertification of DO Collateral NSS privileged and non-privileged accounts.

   Management Response: The DO Collateral system program will initiate a program to monitor and review privileged accounts. This program will follow documented procedures to include appropriate documentation.

   The DO Collateral system program will identify resource requirements for a program to monitor and review non-privileged users accounts and request additional resources as needed. Upon implementation, this program will follow documented procedures to include appropriate documentation. Target completion date: June 30, 2019.

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

4. DO Collateral NSS Incident Response Plan was not reviewed.

Both TD P 85-01, Appendix B, and DO P-910 require bureaus and offices to develop an incident response plan that is reviewed and approved. The bureaus and offices should review the incident response plans annually. This control falls under the Respond Cybersecurity domain and the Incident Response FISMA Metric Domain. We noted the following:

- DO management last updated and reviewed the DO collateral NSS Incident Response Plan on January 19, 2017.

  Due to a mid-year change in management, DO management stated that the DO Collateral Incident Response Plan was not updated. Without regular management review, update, and approval of the incident response plan, the plan may not sufficiently reflect the most recent information in order to detect, respond, and remediate incidents in the DO collateral NSS operating environment within a timely manner. Further, relevant stakeholders may be unaware of the more current incident response procedures which could lead to unnecessary system downtime *(See recommendation #9.)*

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

9. Review and update the incident response plan for FY 2019 and on an annual basis in accordance with the TD P 85-01, Appendix B, and DO P-910.

   Management Response: An updated DO Collateral system Incident Response plan is in program level review now. DO will perform training on the new Incident Response plan in October and November 2018. DO management will perform testing of the new Incident Response plan in November 2018.Target completion date: December 31, 2018.

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

SELF-IDENTIFIED WEAKNESSES

During the FY 2018 Treasury FISMA performance audit, we noted that the BEP and DO management did not report any self-identified weaknesses for their collateral NSS that relate to NIST SP 800-53, Rev. 4, security control requirements, which are referenced in the FY 2018 IG FISMA Reporting Metrics questionnaire. Therefore, no self-identified weaknesses are reported by Treasury's FY 2018 FISMA Performance Audit for its collateral NSS.

MANAGEMENT RESPONSE TO THE REPORT

The following is the Deputy Assistant Secretary for Information Systems and Chief Information Officer's response, dated October 30, 2018, to the Fiscal Year (FY) 2018 Federal Information Security Modernization Act of 2014 (FISMA) Performance Audit Report.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 30, 2018

MEMORANDUM FOR LARISSA KLIMPEL
DIRECTOR, INFORMATION TECHNOLOGY AUDIT

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

SUBJECT: Management Response to Draft Audit Report – "Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2018 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 2018 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 Bureau of Engraving and Printing and Departmental Offices, management did not report any self-identified weaknesses for their collateral NSS. Therefore, no self-identified weaknesses are reported for the FY18 FISMA Performance Audit for collateral NSS. Finally, we appreciate that this year's Cybersecurity Framework maintained a common scoring model allowing the Department to conduct a year-on-year comparison of FISMA compliance and program advances.

The Department remains committed to the continuous improvement of its information security program through effective continuous monitoring and evaluation of risks to our environment. We have made notable progress over the past year and have accomplished a number of achievements, to include:

- Completed a new Security plan for Treasury Secured Data Network (TSDN). This plan incorporates significant improvements including all NIST 800-53 controls, updated hardware and software inventory.

- Migrated the TSDN link to SIPRnet into the "Fed DMZ", a secure enclave required by DOD for all civilian sector systems with access to SIPRnet.

- Recent DISA PKI audit preliminary results confirmed 100% closure of all prior year findings from audit conducted FY18 Q1.

- Consistently achieved 90% compliance with ACAS scan requirements for credentialed scans throughout the TSDN boundary.

- Significant configuration improvements within the Host Based Security System (HBSS) has led to a successful deployment of McAfee Host Intrusion Prevention System (HIPS) Firewall module to 90% of TSDN's network assets.

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

Attachment

cc: David F. Eisner, Assistant Secretary for Management
Jack Donnelly, Associate Chief Information Officer for Cyber Security and Chief Information Security Officer

In the period from 7/1/2017 through 6/30/2018, OCIO made the following improvements to the OCIO collateral security program:

OCIO closed all findings from the DISA PKI audit conducted in FY18 Q1. This was confirmed in the DISA PKI audit just completed in October of this year. Although a final report has not been issued, the auditor verbally provided a preliminary result of "no findings".

OCIO has appointed new ISSM and ISSO for the TSDN program.

OCIO has achieved 90% compliance with the ACAS scan requirement for credentialed scans.

OCIO has also made significant improvements in the installation of Host Based Security System (HBSS) on TSDN.

Attachment

Management Response to KPMG Recommendations

KPMG Finding 1: The Security Controls in the Bureau of Engraving and Printing's (BEP) and Departmental Office's (DO) Collateral System Security Plans (SSPs) were not defined and implemented in accordance with Committee of National Security Systems Instruction (CNSSI) 1253, Bureau Information Security Policies, Treasury Directive Publication (TD P) 85-01, and National Information Institute of Standards and Technology (NIST).

KPMG Recommendation 1: We recommend BEP management: For the selected system, implement an ongoing oversight process and commit resources to ensure that required security controls and control enhancements are implemented and documented in the BEP Collateral SSP as required by BEP Minimum Standard Parameters, TD P 85-01, CNSSI 1253, and NIST SP 800-53, Rev. 4.

Bureau's planned corrective action: BEP will implement ongoing oversight processes and commit resources to review the security controls and enhancements documented in the System Security Plan (SSP) for the BEP Collateral system. BEP will ensure all missing or partially implemented controls are properly reported and tested based on the security categorization level, BEP Minimum Standard Parameters, TD P 85-01, CNSSI 1253, and NIST SP 800-53 Rev. 4. Target completion date: May 1, 2019.

Responsible Official: BEP, Chief Information Security Officer

KPMG Recommendation 2: We recommend BEP management: For the selected system, a POA&M should be created for controls and control enhancements not implemented in the BEP Collateral SSP.

Bureau's planned corrective action: BEP will create a POA&M to track the identified finding. Target Completion Date: November 15, 2018.

Responsible Official: BEP, Chief Information Security Officer

KPMG Recommendation 3: We recommend DO management: For the selected system, validate that it has implemented the required security controls and documented the controls implementation statuses and control enhancements in the DO Collateral SSP as required by DO P-910, TD P 85-01, CNSSI 1253, and NIST SP 800-53 Rev. 4.

Bureau's planned corrective action: DO will update DO P-910 to clarify that it applies to UNCLASSIFIED systems only. The TSDN program will update the TSDN SSP to include control enhancements, as applicable, and will test all controls added to the SSP. Any controls found not to be implemented, or partially implemented, will be added to the TSDN POA&M. Target completion date: June 30, 2019.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 4: We recommend DO management: For the selected system, a POA&M should be created for controls and control enhancements not implemented in the DO Collateral SSP.

> **Bureau's planned corrective action:** DO will update DO P-910 to clarify that it applies to UNCLASSIFIED systems only. The TSDN program will update the TSDN SSP to include control enhancements, as applicable, and will test all controls added to the SSP. Any controls found not to be implemented, or partially implemented, will be added to the TSDN POA&M. Target completion date: June 30, 2019.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Finding 2: POA&Ms were not documented appropriately for the DO collateral National Security System (NSS).

KPMG Recommendation 5: We recommend DO management: For the selected system, update the DO P-910 to establish the elements that should be documented for a POA&M and to ensure that all proper sections of the POA&Ms are completed.

> **Bureau's planned corrective action:** DO will update DO P-910 to clarify that it applies to unclassified systems only. The TSDN program will update the system security plan to identify the appropriate policy for what information is to be documented in the system POA&M.
>
> TSDN has completed a new Risk Assessment as of 9/28/2018. This risk assessment includes all weaknesses from the existing POA&M as well as all weaknesses still open from the Security Assessment Report (SAR) that was completed in August 2017. Working with the TSDN Program Office, the TSDN Cyber Security Operations team will develop a new POA&M based on this risk assessment. The new POA&M will include:
>
> - All columns required by applicable policy.
> - Milestone dates based on availability of funding and resources to ensure timely completion of activities
> - A planned completion date based on the documented milestones
>
> Target completion date: January 31, 2019.
>
> **Responsible Official:** DO, Chief Information Security Officer

KPMG Recommendation 6: We recommend DO management: For the selected system, create POA&Ms for the weaknesses and vulnerabilities identified in the SAR.

> **Bureau's planned corrective action:** DO will update DO P-910 to clarify that it applies to unclassified systems only. The TSDN program will update the system security plan to identify the appropriate policy for what information is to be documented in the system POA&M.

TSDN has completed a new Risk Assessment as of 9/28/2018. This risk assessment includes all weaknesses from the existing POA&M as well as all weaknesses still open from the SAR that was completed in August 2017. Working with the TSDN Program Office, the TSDN Cyber Security Operations team will develop a new POA&M based on this risk assessment. The new POA&M will include:

- All columns required by applicable policy.
- Milestone dates based on availability of funding and resources to ensure timely completion of activities
- A planned completion date based on the documented milestones

Target completion date: January 31, 2019.

Responsible Official: DO, Chief Information Security Officer

KPMG Finding 3: DO collateral NSS user access authorization and review controls need enhancement.

KPMG Recommendation 7: We recommend DO management: For the selected system, implement an ongoing oversight process to ensure that DO collateral NSS non-privileged and privileged user accounts are authorized before granting them access to the system and that privileged and non-privileged accounts are reviewed and recertified on a periodic basis stipulated by TD P 85-01 to ensure user access is commensurate with assigned responsibilities.

Bureau's planned corrective action: The TSDN program will initiate a program to monitor and review privileged accounts. This program will follow documented procedures to include appropriate documentation.

TSDN will identify resource requirements for a program to monitor and review non-privileged users accounts and request additional resources as needed. Upon implementation, this program will follow documented procedures to include appropriate documentation. Target completion date: June 30, 2019.

Responsible Official: DO, Chief Information Security Officer

KPMG Recommendation 8: We recommend DO management: For the selected system, retain supporting documentation evidencing completion of user access authorization and review and recertification of DO Collateral NSS privileged and non-privileged accounts.

Bureau's planned corrective action: The TSDN program will initiate a program to monitor and review privileged accounts. This program will follow documented procedures to include appropriate documentation.

TSDN will identify resource requirements for a program to monitor and review non-privileged users accounts and request additional resources as needed. Upon implementation,

this program will follow documented procedures to include appropriate documentation. Target completion date: June 30, 2019.

Responsible Official: DO, Chief Information Security Officer

KPMG Finding 4: DO Collateral NSS Incident Response Plan was not reviewed.

KPMG Recommendation 9: We recommend DO management: For the selected system, review and update the incident response plan for FY 2019 and on an annual basis in accordance with the TD P 85-01, Appendix B, and DO P-910.

Bureau's planned corrective action: An updated TSDN Incident Response plan is in program level review now. DO will perform training on the new Incident Response plan in October and November 2018. DO will perform testing of the new Incident Response plan in November 2018. Target completion date: December 31, 2018.

Responsible Official: DO, Chief Information Security Officer

APPENDIX I – OBJECTIVE, SCOPE AND METHODOLOGY

The objective of this *Federal Information Systems Modernization Act of 2014* (FISMA) performance audit was to assess the effectiveness of the Department of the Treasury's (Treasury) information security program and practices for its National Security Systems (NSS) for the period July 1, 2017 through June 30, 2018.[3] 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 the Treasury's Consolidated Response to DHS's FISMA 2018 Questions for Inspectors General*, dated May 24, 2018, and assessed the maturity levels on behalf of the Treasury Office of Inspector General. 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. 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 objective, we evaluated security controls in accordance with applicable legislation; the DHS *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0.1,* (FY 2018 IG FISMA Reporting Metrics*)* dated May 24, 2018; 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 8 FISMA Metric Domains from the FY 2018 IG FISMA Reporting Metrics. In addition the maturity level for a domain is determined by a simple majority, where the most frequent level across the questions will serve as the domain rating. A security program is considered effective if it is at Level 4, Managed and Measurable.

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 8 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 8 FISMA Metric Domains. The test procedures

[3] Contract GS-00F-275CA, Task Order 2031LL18F00006, dated April 9, 2018

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. For maturity level 4 controls that were determined to be effective, we performed level 5 (Optimized) test procedures relevant to the two Collateral NSSs at BEP and DO for the maturity level 5 questions within the 8 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 NSSs. We also evaluated Treasury's and office's and bureau's 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 May 8, 2018, through September 28, 2018. 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 2018 FISMA performance audit:

- Federal Information Security Modernization Act of 2014
- NIST Federal Information Processing Standards (FIPS) and/or Special Publications[4]
    - 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*

[4] 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 800-30 Revision 1, *Guide for Conducting Risk Assessments*
- 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 05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*
  - OMB Memorandum 16-03, *Fiscal Year 2016-2016 Guidance on Federal Information Security and Privacy Management Requirements*
  - OMB Memorandum 16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for Federal Civilian Government*

- OMB Memorandum 17-05, *Fiscal Year 2017-2018 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) 2018, we conducted a Federal Information Security Modernization Act of 2014 (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 – 2017 Performance Audit

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2017 Finding # 1 – OCIO & CNSS – DO 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	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 National Institute of Standards and Technology (NIST) SP 800-53, Revision (Rev.) 4, baseline control enhancements. Specifically, KPMG noted that two control enhancements were omitted. Through inspection of the DO 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	We recommend that OCIO and CNSS – DO management: 1. Update the TD P 85-01, Appendix B, for NSS, to address all Committee on National Security Systems Instruction (CNSSI) Instruction No. 1253 and NIST SP 800-53, Rev. 4, control requirements and control enhancements. 2. Review TD P 85-01, Appendix B, to ensure that all control enhancements are appropriately included. 3. Update the DO Collateral SSP, and supporting documentation, to include an implementation	**Closed** We inspected TD P 85-01, Appendix B, and noted it addressed CNSS Instruction No 1253 and NIST SP 800-53, Rev.4, control requirements and control enhancements. (Recommendations #1 and 2 are closed.) For the DO CNSS SSP, we noted that it defined each of applicable security control to include a statement on how each of the security controls was implemented. (Recommendation #3 is closed.)

Finding #	Prior-Year Condition	Recommendation(s)	Status
updated in accordance with Committee on National Security Systems (CNSS) No. 1253, Security Categorization and Controls Selection for National Security Systems, guidance.	with the TD P 85-01, CNSS Instruction No. 1253, and NIST SP 800-53, Rev.4, guidance.	statement detailing the processes in place to fulfill the requirements for each security control	
Prior Year FY 2017 Finding # 2 – OCIO & CNSS – DO DO Collateral NSS patch management process was not compliant with the Treasury Information Technology Security Policy.	As of June 27, 2017, we noted that there were 107 changes implemented within the DO environment. We identified that sufficient evidence was not available to support the effective management of all randomly selected 15 changes. Specifically, we noted: • Testing documentation was not available for 15 of 15 randomly selected changes; and • Management approval was not available for 1 of 15 randomly selected changes. Further, we noted that there were 1,764 security related system patches implemented on the 5 of 51 randomly selected servers within the DO environment. Both the testing documentation and management approval for implementation of all judgmentally selected 25 patches were unavailable.	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.	**Open** DO management informed us that bureau did not maintain change and patch testing documentation and management approvals.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2017 Finding # 3 – OCIO & CNSS – DO DO collateral NSS account management activities were not compliant with its SSP policies.	DO Collateral NSS SSP and TD P 85-01, Appendix B, require management to disable. 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.	5. Establish a process to review at a defined frequency the DO Collateral NSS user accounts. 6. Disable terminated or inactive DO employees' or contractors' DO Collateral NSS accounts accordingly.	**Open** We noted that 2 of 5 DO privileged users had accounts that were inactive greater than 30 days.
Prior Year FY 2017 Finding # 4 – OCIO & CNSS – DO DO did not perform Business Impact Analyses (BIA) for the DO Collateral NSS.	Since 2012, DO management had not performed and documented a formal BIA that considered the DO Collateral NSS computing environment.	7. Perform and document the Business Impact Analysis for the DO Collateral NSS environment every two years as required by Federal Continuity Directive (FCD)-1.	**Closed** We noted that the BIA for DO was approved on April 6, 2018 and is scheduled to be reviewed/renewed by April 6, 2020.

Prior-Year Findings – 2016 Performance Audit

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2016 Finding # 4 – CNSS – DO DO Collateral Account management activities were not compliant with policies at DO.	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 120 days, and management did not disabled these user accounts. Additionally, one DO employee retained an active account to their system after being terminated.	We recommend that DO management: 10. 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. 11. For the selected system, disable terminated or inactive DO employee or contractor's accounts accordingly. 12. 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.	**Partially Implemented/Open** We inquired of management and noted that they have established an account review process. 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. (Recommendation #10 is closed.) In addition, we compared the listing of terminated employees and contractors to the active DO Collateral System user listing and noted that no terminated users had active access. (Recommendation #11 is closed.) However, the management updated process was not fully effective. During our FY17 and FY18 FISMA testing, we noted there were users who had active user accounts and had not logged in for 30 days. Please refer to the Above Prior-Year FY 2017 Finding # 4 – CNSS. (Recommendation #12 is open.)

FY17 FISMA Self-Identified Weaknesses for Treasury Collateral NSS

Bureau	System	NIST SP 800 53 Control	Applicable FY 2018 IG FISMA Reporting Metric(s)	Weakness	Status
DO	DO Collateral System	IA-2	N/A	POA&M #T-006: Lack of Multi-Factor Authentication.	**No Longer Applicable** This POA&M relates to a control that is not referenced in the FY 2018 IG FISMA Metric questionnaire. Therefore, we did not perform follow-up testing procedures for this prior-year self-identified weakness.
	DO Collateral System	SI4	31, 35	POA&M #242: Management Has Not Implemented a Security Event Information Manager (SIEM)	**Closed** We noted that DO management indicated that this POA&M was originally from FY 2012, and we observed the tools management used to monitor security events for DO Collateral System.

APPENDIX III – DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS's FISMA 2018 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) Federal Information Security Modernization Act of 2002 (FISMA) 2018 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 2018 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 2018 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 designed and executed test procedures to evaluate the effectiveness of management's security control program and practices over the five cybersecurity functions: identify, protect, detect, respond, and recover and the eight FISMA metric domains: risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring (ISCM), incident response, and contingency planning using the available options from CyberScope.[5] If issues were identified related to the metric, we assessed the metric at Ad Hoc (Level 1), Defined (Level 2), or Consistently Implemented (Level 3) and provided explanations in the "Comment" section about the findings or rationale for why Managed and Measurable (Level 4) was not met. We did not include any comments for Managed and Measurable (Level 4), Optimized (Level 5), or Consistently Implemented (Level 3), when it was the highest maturity level determined by management's self- assessment.

Function 1: Identify – Risk Management

1 To what extent 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 SP, Rev. 4: CA-3, PM-5, and CM-8; Office of Management and Budget (OMB)-M-04-25; NIST 800-161; NIST Cybersecurity Framework(CSF): ID.AM-1-4; FT 2018 CIO FISMA Metrics: 1.1, 1.4, and 1.5)?

[5] The scoring methodology is described in the DHS's *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.0.1, May 24, 2018, requires a Managed and Measurable (Level 4) rating for an effective security program and is determined by the entries in CyberScope.

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: To achieve a Managed and Measureable Risk Management (RM) level of practices over the BEP and DO Collateral NSSs, Treasury should ensure that the information systems included in BEP and DO NSSs' inventory are subject to the monitoring processes defined within the BEP and DO Collateral's ISCM strategy.

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; FY 2018 CIO FISMA Metrics:1.2)?

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: The Department Office's Information Technology Security Policy Handbook does not document the requirements for managing and maintaining an up-to-date hardware inventory for NSS in accordance with Treasury Information Technology Security Program.

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: The Department Office's Information Technology Security Policy Handbook does not document the requirements for managing and maintaining an up-to-date software inventory for NSS in accordance with TD P 85-01.

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; FY 2018 CIO FISMA Metrics: 1.1)?

Maturity Level: **Defined (Level 2)** – The organization has categorized and communicated the importance/priority of information systems in enabling its missions and business functions.

Comments: BEP and DO management did not fully define security control baselines based on system categorization for the BEP and DO Collateral system (Refer to Finding #1 above for both BEP and DO).

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 SP 800-39; NIST SP 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); Chief Financial Officer (CFO) Council Enterprise Risk Management (ERM) Playbook; OMB M-17-25; FY 2018 CIO FISMA Metrics: 1.6)?

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 achieve a Managed and Measureable RM level of practices over the BEP and DO Collateral NSSs, BEP and DO management should monitor and analyze their defined qualitative and quantitative performance measures on the effectiveness of their risk management strategy across disciplines and collects, analyzes and reports information on the effectiveness of their risk management program.

6 To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (NIST SP 800-39; FEA Framework; NIST SP 800-53: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; DHS Binding Operational Directive 17-01)?

Maturity Level: **Defined (Level 2)** – The organization has defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture. In addition, the organization has defined a process to conduct a security architecture review for new/acquired hardware/software prior to introducing systems into its development environment.

Comments: BEP and DO management did not fully implement the NIST SP 800-53 , Rev. 4 controls and control enhancements referenced in question 6 in the BEP and DO Collateral System Security Plans (SSP) (Refer to Finding #1 above for both BEP and DO).

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, 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 SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 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 achieve a Managed and Measureable RM level of practices over the BEP and DO Collateral NSSs, BEP and DO management should utilize integrated risk management governance structures for implementing and overseeing enterprise risk management (ERM) capabilities that manage risks from information security, strategic planning and strategic reviews, internal control activities, and applicable mission/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: **Defined (Level 2)** – Policies and procedures for the effective use of POA&Ms have been defined and communicated. These policies and procedures address, at a minimum, the centralized tracking of security weaknesses, prioritization of remediation efforts, maintenance, and independent validation of POA&M activities (Refer to Finding #2 above for DO).

Comments: DO management did not document the required information in the DO Collateral POA&Ms as stipulated by Department Office's Information Technology Security Policy Handbook and Treasury Information Technology Security. Moreover, the DO management did not create POA&Ms for security weaknesses identified in the DO Collateral System Security Assessment Report (SAR) that was completed on August 2, 2017. In addition, see comments in question 19.

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) security controls to mitigate system-level risks (NIST SP 800-37; NIST SP 800-39; NIST SP 800-53: PL-2, RA-1; NIST 800-30; CSF: ID.RA-1 – 6)

Maturity Level: **Defined (Level 2)**.

Comments: The DO management did not create POA&Ms for security weaknesses identified in the DO Collateral System SAR that was completed on August 2, 2017 Refer to Finding #2 above for DO).

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; OMB Circular A-11; Green Book (Principles #9, #14, and #15))?

Maturity Level: **Consistently Implemented (Level 3)** – Policies and procedures for system level risk assessments and security control selections are defined and communicated. In addition, the organization has developed a tailored set of baseline controls and provides guidance regarding acceptable risk assessment approaches.

Comments: From July 1, 2017, through March 1, 2018, DO management did not properly communicate DO Collateral System's information security risks to appropriate internal and external stakeholders in a timely manner.

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; Federal Risk and Authorization Management Program (FedRAMP) standard contract clauses; Cloud Computing Contract Best Practices; FY 2018 CIO FISMA Metrics: 1.5; Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)?

Maturity Level: **Not Applicable.**

Comments: Both the BEP and DO Collateral Systems are not contractor systems. Refer to the FY 2018 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: **Not Applicable.**

Comments: This question is not applicable to both the BEP and DO Collateral Systems since this metric is focused at the Bureau and Department levels. Refer to FY 2018 Treasury Unclassified FISMA Performance Audit Report for our assessed maturity level for the agency.

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

Maturity Level: **Consistently Implemented (Level 3)**

Comments: We determined that Treasury's RM practices for the BEP and DO Collateral Systems did not achieve 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 have no additional information that was not already covered in metric questions 1 to 12 above. According to DHS criteria, we assessed the RM overall maturity levels as Consistently Implemented, which is 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; NIST 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: This is the highest maturity level for this metric.

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 phase within an organization's SDLC;6 configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 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 achieve a Managed and Measureable Configuration Management (CM) level of practices over the BEP and DO Collateral NSSs, Treasury should monitor, analyze, and report to stakeholders qualitative and quantitative performance measures on the effectiveness of its configuration management plans, use this information to take corrective actions when necessary, and 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 SP 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 achieve a Managed and Measureable CM level of practices over the BEP and DO Collateral NSSs, Treasury should monitor, analyze, and report on the qualitative and quantitative performance measures used to gauge 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.

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 2018 CIO FISMA Metrics: 1.1, 1.2; 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.

[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."

Comments: Where feasible, 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 2018 CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on least functionality. Further, the organization consistently utilizes SCAP-validated software assessing (scanning) capabilities against all systems on the network (see inventory from questions #1 - #3) to assess and manage both code-based and configuration-based vulnerabilities.

Comments: Where feasible, Treasury should employ automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network.

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 SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20 Control 4.5; FY 2018 CIO FISMA Metrics: 2.13; 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: Prior-Year FY 2017 Finding #2, "DO Collateral NSS patch management process was not compliant with the Treasury Information Technology Security Policy," was still open. During FY 2018, DO Collateral System did not consistently install critical patches to the DO Collateral System in a timely.

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-08-05)?

Maturity Level: **Not Applicable.**

Comments: This question is not applicable to both the BEP and DO Collateral Systems since this metric is focused at the Bureau and Department levels. Refer to FY 2018 Treasury Unclassified FISMA Performance Audit Report for our assessed maturity level for the agency.

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 SP 800-53: CM-2, CM-3)?

Maturity Level: **Defined (Level 2)** – The organization consistently implements its change control policies, procedures, and processes, including explicit consideration of security impacts prior to change implementation.

Comments: Prior-Year FY 2017 Finding #2, "DO Collateral NSS patch management process was not compliant with the Treasury Information Technology Security Policy," was still open.

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 have no additional information that was not already covered in metric questions 14 to 21 above. According to DHS criteria, we assessed the CM overall maturity level as Consistently Implemented, which is ineffective according to DHS guidance. Please refer to 45.1 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 SP 800-53: AC-1, IA-1, PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Maturity Level: **Consistently Implemented (Level 3)** – Stakeholders have adequate resources (people, processes, and technology) to effectively implement identity, credential, and access management activities.

Comments: This is the highest maturity level for this question.

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

Maturity Level: **Not Applicable.**

Comments: This question is not applicable to both BEP and DO Collateral Systems. BEP Collateral System follows the unclassified BEP policies and practices, and DO Collateral System follows Department of Defense (DOD) identity and access policies and practices.

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 26 through 31) (NIST SP 800-53: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; FY 2018 CIO FISMA Metrics: 2.3)?

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: DO management did not 1) perform periodic user access reviews for non-privileged and privileged DO Collateral System users and 2) retain access authorization records for 2 of 5 new privileged users (Refer to Finding #3 above for DO). Additionally, Prior-Year FY 2017 Finding #4, "DO collateral NSS account management activities compliant with its SSP policies and TD P 85-01, Appendix B," and Prior-Year FY 2016 Finding #4, "DO Collateral Account management activities were not compliant with policies at DO," were still open.

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; FY 2018 CIO FISMA Metrics: 2.16)?

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 achieve a Managed and Measureable Identity and Access Management (IA) level of practices over the BEP and DO Collateral NSSs, Treasury should employ automation to centrally document, track, and share risk designations and screening information with necessary parties.

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: **Defined (Level 2)** – The organization has defined its processes for developing, documenting, and maintaining access agreements for individuals that access its systems.

Comments: See comment for question 25.

28 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 Identity Assurance Level (IAL)3/ Authenticator Assurance Level (AAL) 3/ Federated Assurance Level (FAL) 3 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; FY 2018 CIO FISMA Metrics: 2.4; and Cybersecurity Sprint)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization has consistently implemented strong authentication mechanisms for non- privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets.

Comments: This question is not applicable to the BEP Collateral System based on its configuration. To improve the IA practices for the DO Collateral System, Treasury management should transition to its desired or "to-be" ICAM architecture and integrate its ICAM strategy and activities with its enterprise architecture and the FICAM segment architecture.

29 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-62 r3 IAL 3/ AAL 3/ FAL 3 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; FY 2018 CIO FISMA Metrics: 2.5; and Cybersecurity Sprint)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization has consistently implemented strong authentication mechanisms for privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets.

Comments: This question is not applicable to the BEP Collateral System based on its configuration. To improve the IA practices for the DO Collateral System, Treasury management should use automated mechanisms (e.g., machine-based or user-based enforcement), where appropriate, to manage the effective implementation of its policies and procedures.

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 2018 CIO FISMA Metrics: 2.4 and 2.5; NIST SP 800-53: AC-1, AC-2 (2), AC-17; CSIP)?

Maturity Level: **Defined (Level 2)** – The organization has defined its processes for provisioning, managing, and reviewing privileged accounts. Defined processes cover approval and tracking, inventorying and validating, and logging and reviewing privileged users' accounts.

Comments: See comment for question 25. In addition, DO management has not remediated Prior-Year FY 2017 Finding #3, "DO Collateral NSS account management activity was not compliant with its SSP policies." was still 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 2018 CIO FISMA Metrics: 2.10)?

Maturity Level: **Not Applicable.**

Comments: Based on the nature of the configurations for both BEP and DO Collateral Systems, this question is not applicable at the system level. Refer to FY 2018 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: We have no additional information that was not already covered in metric questions 23 to 32 above. According to DHS criteria, we assessed the IA overall maturity level as Consistently Implemented, which is ineffective according to DHS guidance. Please refer to 45.1.

Function 2C: Protect – Data Protection and Privacy

33 To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 900-122; OMB M-18-02; OMG A-130, Appendix I; NIST SP 800-53: AR-4 and Appendix J)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its privacy program by:

Dedicating appropriate resources to the program maintaining an inventory of the collection and use of PII Conducting and maintaining privacy impact assessments and system of records notices for all applicable systems.
Reviewing and removing unnecessary PII collections on a regular basis (i.e., SSNs)

Comments: For the DO Collateral System, DO management participates in the Department of Defense (DOD) sensitive data monitoring through an interagency agreement with Army Research Laboratories. Because the DO Collateral System does not contain PII, this metric is not applicable.

To improve the Data Protection and Privacy (DP) practices for the BEP Collateral System, Treasury should monitor and analyze quantitative and qualitative performance measures on the effectiveness of its privacy activities and uses that information to make needed adjustments. Treasury should conduct independent reviews of its privacy program and make improvements as necessary.

34 To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (NIST SP 800-53; Appendix J, SC-8, SC-28, MP-3, and MP-6; FY 2018 CIO FISMA Metrics: 2.9 and 2.10)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization's policies and procedures have been consistently implemented for the specified areas, including (i) use of FIPS-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data.

Comments: For the DO Collateral System, DO management participates in the DOD monitoring through an interagency agreement with Army Research Laboratories. Because the DO Collateral System does not contain PII, this metric is not applicable.

To improve the DP practices for the BEP Collateral System, Treasury should ensure that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy.

35 To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53: Appendix J, SE-2; FY 2018 SAOP FISMA Metrics: 3.8-3.12)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware, and blocks against known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic is quarantined or blocked.

Comments: To improve the DP practices for the BEP and DO NSSs, Treasury should analyze qualitative and quantitative

measures on the performance of its data exfiltration and enhanced network defenses. Treasury should also conduct exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses.

36 To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17-25)?

Maturity Level: **Defined (Level 2)** – The organization has defined and communicated its Data Breach Response Plan, including its processes and procedures for data breach notification. Further, a breach response team has been established that includes the appropriate agency officials.

Comments: The DO management did not perform an annual review of DO Collateral Incident Response (IR) Plan. The last update and documented review by DO management was on January 19, 2017(Refer to Finding 4 above for DO).

37 To what degree does the organization ensure that security awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53: AR-5)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization ensures that all individuals receive basic privacy awareness training and individuals having responsibilities for PII or activities involving PII receive role-based privacy training at least annually. Additionally, the organization ensures that individuals certify acceptance of responsibilities for privacy requirements at least annually.

Comments: To improve the DP practices for the BEP and DO NSSs, Treasury should measure the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, Treasury should make updates to its program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing.

38 Provide any addition information on the effectiveness (positive or negative) of the organization's data protection and privacy 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 data protection and privacy program effective?

Comments: We have no additional information that was not already covered in metric questions 33 to 37 above. According to DHS criteria, we assessed the DP overall maturity level as Consistently Implemented, which is ineffective according to DHS guidance. Please refer to 45.1.

Function 2D: Protect – Security Training

39 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 SP 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: This is the highest maturity level for this question.

40 To what extent does the organization utilize of 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 SP 800-53; AT-2 and AT-3; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; 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: To improve Security Training (ST) practices over the BEP and DO Collateral NSSs, Treasury should address its identified knowledge, skills, and abilities gaps through training or hiring of additional staff/contractors.

41 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 SP-800-53: AT-1; NIST SP 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 ST practices over the BEP and DO Collateral NSSs, Treasury should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans.

42 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 of questions 43 and 44 below) (NIST SP 800- 53: AT-1 through AT-4; and NIST SP 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 ST practices over the BEP and DO Collateral NSSs, Treasury should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures.

43 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 SP 800-53: AT-2; FY 2018 CIO FISMA Metrics: 2.15; NIST SP 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: To improve ST practices over the BEP and DO Collateral NSSs, Treasury should measure the effectiveness of its awareness training program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate.

44 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 SP 800-53: AT-3 and AT-4; FY 2018 CIO FISMA Metrics: 2.15)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization ensures that 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.

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

45.1 Please provide the assessed maturity level for the agency's Protect Function.

Maturity Level: **Consistently Implemented (Level 3)**

Comments: We determined that Treasury's CM, IA, DP, and ST practices for BEP and DO Collateral Systems did not achieve the Management 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 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 have no additional information that was not already covered in questions 39 to 44 above. According to DHS criteria, we assessed the Security Training overall maturity level as Consistently Implemented, which is ineffective. Please refer to
45.1 for further explanation.

Function 3: Detect – Information Security Continuous Monitoring

46 To what extent does the organization utilize an 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: **(Defined Level 2)** – The organization has developed and communicated its ISCM strategy that includes: i) considerations at the organization/business process level, ii) considerations at the information system level, and iii) processes to

review and update the ISCM program and strategy. At the organization/business process level, the ISCM strategy defines how ISCM activities support risk management in accordance with organizational risk tolerance. At the information system level, the ISCM strategy addresses monitoring security controls for effectiveness, monitoring for security status, and reporting findings.

Comments: BEP and DO management did not fully implement the required NIST SP 800-53 controls and control enhancements in the BEP and DO Collateral SSP Refer to Finding #1 above for both BEP and DO).

47 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; collection of 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 49)?

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: To improve ISCM practices over the BEP and DO Collateral NSSs, Treasury should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its ISCM policies and procedures and makes updates, as appropriate.

48 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 2018 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 improve ISCM practices over the BEP and DO Collateral NSSs, Treasury should collect, monitor, and analyze qualitative and quantitative performance measures across the organization and reporting data on the effectiveness of the organization's ISCM program.

49 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, and technical) and types (common, hybrid, and system-specific) are assessed and monitored.

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

50 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 is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting.

Comments: DO management did not design a process to capture qualitative and quantitative performance measures for DO Collateral System.

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

Maturity Level: **Consistently Implemented (Level 3)**

Comments: We determined that ISCM 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 3.

51.2 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 have no additional information that was not already covered in questions 46 to 50 above. According to DHS criteria, we assessed the ISCM overall maturity level as Consistently Implemented, which is ineffective. Please refer to 51.1 for further explanation.

Function 4: Respond – Incident Response

52 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; NIST SP 800-184; OMB M-17- 25; FY 2018 CIO FISMA Metrics: 4.1, 4.3, 4.6, and 5.3; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53-58)?

Maturity Level: **Defined (Level 2)** – The organization's incident response policies, procedures, plans, and strategies have been defined and communicated. In addition, the organization has established and communicated an enterprise level incident response plan.

Comments: The DO management did not perform an annual review of DO Collateral IR Plan. The last update and documented review by DO management was on January 19, 2017 Refer to Finding #4 above for DO).

53 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; IR-7; NIST SP 800-83; NIST 800- 61 Rev. 2; OMB M-18-02; OMG M-16-24; FY 2018 CIO FISMA Metrics: Section 4; and US-CERT Federal Incident Notification Guidelines?

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

Comments: For BEP Collateral System, this metric is performed at the BEP unclassified bureau-level and Department Level due to unique nature and size of the BEP Collateral System. Refer to the 2018 Treasury Unclassified FISMA Audit Report for our assessed maturity level for the agency.

To improve the DO Collateral IR program, Treasury management should assign the responsibility for monitoring and tracking the effectiveness of incident response activities. DO management personnel should consistently collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of incident response activities.

54 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; OMB M-18-02; and 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: For BEP Collateral System, this metric is performed at the BEP unclassified bureau-level and Department Level due to unique nature and size of the BEP Collateral System. Refer to the 2018 Treasury Unclassified FISMA Audit Report for our assessed maturity level for the agency.

To improve the DO Collateral IR program, 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.

55 How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2)?

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: For BEP Collateral System, this metric is performed at the BEP unclassified bureau-level and Department Level due to unique nature and size of the BEP Collateral System. Refer to the 2018 Treasury Unclassified FISMA Audit Report for our assessed maturity level for the agency.

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

56 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-18-02; NIST 800-53: IR-6; US-CERT Incident Notification Guidelines; PPD-41; DHS Cyber Incident Reporting Unified Message)?

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: For BEP Collateral System, this metric is performed at the BEP unclassified bureau-level and Department Level due to unique nature and size of the BEP Collateral System. Refer to the 2018 Treasury Unclassified FISMA Audit Report for our assessed maturity level for the agency.

To improve the DO Collateral IR program, Treasury should use IR metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.

57 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, including through contracts/agreements, as appropriate, for incident response support (FY 2018 CIO FISMA Metrics: 4.4; NIST SP 800-86; NIST SP 800-53: IR-4; OMB M-18-02; PPD-41).

Maturity Level: **Not Applicable.**

Comments: For BEP Collateral System, this metric is performed at the BEP unclassified bureau-level and Department Level due to unique nature and size of the BEP Collateral System. For DO Collateral System, this metric is not applicable based on its system environment and mission. Refer to the 2018 Treasury Unclassified FISMA Audit Report for our assessed maturity level for the agency.

58 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 NIST SP 800-44)

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: For BEP Collateral System, this metric is performed at the BEP unclassified bureau-level and Department Level due to unique nature and size of the BEP Collateral System. Refer to the 2018 Treasury Unclassified FISMA Audit Report for our assessed maturity level for the agency.

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

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

Maturity Level: **Consistently Implemented (Level 3)**

Comments: We determined that IR practices for the BEP and DO Collateral Systems did not achieve the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.

59.2 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 about and based on all testing performed, is the incident response program effective?

Comments: We have no additional information that was not already covered in questions 52 to 58 above. According to DHS criteria, we assessed the IR overall maturity level as Consistently Implemented, which is ineffective. Please refer to 59.1 for further explanation.

Function 5: Recover – Contingency Planning

60 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 SP 800-53: CP-1 and CP-2; NIST 800-34; NIST SP 800-84; FCD-1: Annex B)?

Maturity Level: **Consistently Implemented (Level 3) –** 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: This is the highest maturity level for this question.

61 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 62-66) (NIST SP 800-34; NIST SP 800-161; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5).

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 BEP and DO Collateral NSSs, Treasury management should understand and manage its information and communications technology (ICT) supply chain risks related to contingency planning activities. As appropriate, Treasury management should: integrate ICT supply chain concerns into its contingency planning policies and procedures, define and implement a contingency plan for its ICT supply chain infrastructure, apply appropriate ICT supply chain controls to alternate storage and processing sites, and consider alternate telecommunication service providers for its ICT supply chain infrastructure and to support critical information systems.

62 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53: CP-2; NIST SP 800-34, Rev. 1, 3.2, FIPS 199, FCD-1, OMB M-17-09; FY 2018 CIO FISMA Metrics: 5.6)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization incorporates the results of organizational and system level BIAs into strategy and plan development efforts consistently. System level BIAs are integrated with the organizational level BIA and include: characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high-value assets.

Comments: This is the highest maturity level for this question.

63 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; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

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: This question is not applicable for the BEP Collateral System. BEP management has documented and accepted this risk.

To improve the CP practices over DO Collateral NSS, Treasury should 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.

64 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53: CP-3, CP-4; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

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/ continuity of operation plan (COOP) business continuity plan (BCP).

Comments: This question is not applicable for the BEP Collateral System. BEP management has documented and accepted this risk.

To improve the CP practices over the DO Collateral NSS, Treasury should employ automated mechanisms to more thoroughly and effectively test system contingency plans.

65 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 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; FY 2018 CIO FISMA Metrics)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and RAID, as appropriate. Alternate processing and storage sites are chosen based upon risk assessments which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized, and are not subject to the same physical and/or cybersecurity risks as the primary sites. In addition, the organization ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site. Furthermore, backups of information at the user- and system-levels are consistently performed and the confidentiality, integrity, and availability of this information is maintained.

Comments: This question is not applicable for the BEP Collateral System. BEP management has documented and accepted this risk.

For DO Collateral System, this is the highest maturity level for this question.

66 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)?

Maturity Level: **Not Applicable.**

Comments: For BEP and DO Collateral Systems, this control is performed at the bureau level. Refer to the FY 2018 Treasury FISMA Unclassified Performance Audit Report for our assessed maturity level for the agency.

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

Maturity Level: **Consistently Implemented (Level 3)**

Comments: We determined that CP practices for the BEP and DO Collateral Systems did not achieve the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level.

67.2 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 have no additional information that was not already covered in questions 60 to 66 above. According to DHS criteria, we assessed the CP overall maturity level as Consistently Implemented, which is ineffective. Please refer to 67.1 for further explanation.

Function 0: Overall

0.1 Please provide the overall IG self-assessment (Effective/Not Effective)

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 with the grammatical and narrative structure of the Annual Report.

Comments: Consistent with applicable FISMA requirements, OMB and CNSS policy and guidance, 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 eight FISMA Metric Domains. However, the program was not fully effective as reflected by the deficiencies that we identified in the RM IA, and IR, program areas. In addition, we did not assess any of the FISMA Metric Domains as Managed and Measurable (Level 4). The FY 2018 IG FISMA Reporting Metrics define an effective information security program as Managed and Measurable (Level 4).

Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count[7]
Ad-Hoc	0
Defined	4
Consistently Implemented	6
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	0

Function 2A: Protect - Configuration Management

Function	Count[8]
Ad-Hoc	0
Defined	2
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
Function Rating: Ad Hoc (Level 1)	0

[7] As explained in the metric 11 and 12 comments in Appendix III, two RM metrics were not applicable to both BEP and DO Collateral NSSs. As a result, the total metrics assessed for Risk Management totaled to ten.
[8] As explained in the metric 20 comment, one metric was not applicable to both BEP and DO Collateral NSSs. As a result, the total metrics assessed for Risk Management totaled to seven.

Function 2B: Protect - Identity and Access Management

Function	Count[9]
Ad-Hoc	0
Defined	3
Consistently Implemented	4
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Function 2C: Protect – Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	4
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

[9] As explained in the Metric 24 and 31 comments in Appendix III, two IA metrics do not apply to both DO and BEP Collateral Systems. As such, we are only counting seven applicable metrics for IA.

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	4
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

Function 4: Respond - Incident Response

Function	Count[10]
Ad-Hoc	0
Defined	1
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	

[10] As explained in the Metric 57 comment in Appendix III, one IR metric does not apply to both DO and BEP Collateral Systems. As such, we are only counting six applicable metrics for IA.

Function 5: Recover - Contingency Planning

Function	Count[11]
Ad-Hoc	0
Defined	0
Consistently Implemented	0
Managed and Measurable	6
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 RM practices for the BEP and DO Collateral Systems did not achieve the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level, which is ineffective according to DHS guidance.
Function 2A: Protect – Configuration Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	According to DHS criteria, we assessed the CM overall maturity level as Consistently Implemented, which is ineffective according to DHS guidance.
Function 2B: Protect – Identity and Access Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	According to DHS criteria, we assessed the IA overall maturity level as Consistently

[11] As explained in the Metric 66 comment in Appendix III, one CP metric does not apply to both DO and BEP Collateral Systems. In addition, metrics 63, 64, and 65 do not apply to the BEP Collateral System. As such, we are only counting six applicable metrics for IA.

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
			Implemented, which is ineffective according to DHS guidance.
Function 2C: Protect – Data Protection and Privacy	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	According to DHS criteria, we assessed the DP overall maturity level as Consistently Implemented, which is ineffective according to DHS guidance.
Function 2D: Protect – Security Training	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	According to DHS criteria, we assessed the Security Training overall maturity level as Consistently Implemented, which is ineffective according to DHS guidance.
Function 3: Detect – ISCM	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that ISCM practices for the BEP and DO Collateral Systems did not meet the Managed and Measurable maturity level 4. We assess the majority of these metrics at the Consistently Implemented maturity level 3, which is ineffective according to DHS guidance.
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that IR practices for the BEP and DO Collateral Systems did not achieve the Managed and Measurable maturity level 4. We assessed the majority of these metrics at the Consistently Implemented maturity level, which is ineffective according to DHS guidance.
Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	We determined that CP practices for the BEP and DO Collateral Systems did not achieve the

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
			Managed and Measurable maturity level 4; we assessed the majority of these metrics at the Consistently Implemented maturity level 3, which is ineffective according to DHS guidance.
Overall	Not Effective	Not Effective	Consistent with applicable FISMA requirements, OMB and CNSS policy and guidance, 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 eight FISMA Metric Domains. However, the program was not fully effective as reflected by the deficiencies that we identified in the RM IA, and IR, program areas. In addition, we did not assess any of the FISMA Metric Domains as Managed and Measurable (Level 4). The FY 2018 IG FISMA Reporting Metrics define an effective information security program as Managed and Measurable (Level 4). We assessed Treasury's Information Security program for Collateral NSSs as Consistently Implemented (Level 3), which is ineffective according to DHS guidance.

APPENDIX IV – GLOSSARY OF TERMS

Acronym	Definition
AAL	Authenticator Assurance Level
AC	Access Control
ACAS	Assured Compliance Assessment Solution
ACIOCS	Associate Chief Information Officer for Cyber Security
BCP	Business Continuity Planning
BEP	Bureau of Engraving and Printing
BIA	Business Impact Analysis
CCB	Control Change Board
CFO	Chief Financial Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information Security Officers
CM	Configuration Management
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COOP	Continuity of Operation Plan
CP	Contingency Planning
CSS	Cyber Security Sub-Council
CSF	Cyber Security Framework
CSIP	Cybersecurity Strategy and Implementation Plan
Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity
DP	Data Protection and Privacy
DHS	Department of Homeland Security
DO	Departmental Offices
ERM	Enterprise Risk Management
FAL	Federated Assurance Level
FAR	Federal Acquisition Regulation
FCD	Federal Continuity Directive
FEA	Federal Enterprise Architecture
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
HSPD	Homeland Security Presidential Directive
IA	Identity and Access Management

Acronym	Definition
IAL	Identity Assurance Level
ICAM	Identity, Credential, and Access Management
ICT	Information and Communications Technology
IG	Inspector General
IGs	Inspectors General
IR	Incident Reporting
ISCM	Information Security Continuous Monitoring
IT	Information Technology
KPMG	KPMG LLP
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
PPD	Presidential Policy Direction
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
RAID	Redundant Array of Independent Disks
Rev.	Revision
RM	Risk Management
SAR	Security Assessment Report
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