Evaluation Report

OIG-CA-16-007

INFORMATION TECHNOLOGY: Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2015 Independent Evaluation for Collateral National Security Systems

November 12, 2015

Office of Inspector General

Department of the Treasury

THIS PAGE INTENTIONALLY LEFT BLANK

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

November 12, 2015

MEMORANDUM FOR BRODI FONTENOT
ASSISTANT SECRETARY FOR MANAGEMENT

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

FROM: Tram J. Dang /s/
Director, Information Technology Audit

SUBJECT: Evaluation Report – *Department of the Treasury Federal Information Security Modernization Act Fiscal Year 2015 Independent Evaluation 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 2015 Independent Evaluation for the Collateral National Security Systems,* dated November 11, 2015. The Federal Information Security Modernization Act of 2014 (FISMA) requires that Federal agencies have an annual independent evaluation performed of their information security program and practices to determine 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 the annual FISMA responses. FISMA also requires that the agency Inspector General (IG) or an independent external auditor perform the annual evaluation as determined by the IG.

To meet our FISMA requirements, we contracted with KPMG LLP (KPMG), an independent certified public accounting firm, to perform this year's annual FISMA evaluation. Appendix III of the attached KPMG report includes *The Department of the Treasury's Consolidated Response to DHS's FISMA 2015 Questions for Inspectors General*. KPMG conducted its evaluation in accordance with the *Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation*. In connection with our contract with KPMG, we reviewed its report and related documentation and inquired of its representatives.

In brief, KPMG did not identify any substantial control deficiencies that impacted the design and operating effectiveness of Treasury's collateral national security systems at the Departmental Offices and Bureau of Engraving and Printing, and therefore, did not include any recommendations.

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

Attachment

cc: Terry Bartlett
Acting Associate Chief Information Officer,
Cyber Security

Department of the Treasury
Federal Information Security Modernization Act
Fiscal Year 2015 Independent Evaluation for the Collateral National Security Systems

November 11, 2015

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

Department of the Treasury
Federal Information Security Modernization Act Fiscal Year 2015 Evaluation for Collateral National Security Systems

Table of Contents

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 2015 Independent Evaluation for Collateral National Security Systems

Dear Mr. Thorson:

This report presents the results of our independent evaluation of the Department of the Treasury's (Treasury) collateral National Security Systems (NSS) information 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 2015 questionnaire to collect these responses. Appendix III, *Department of the Treasury's Consolidated Response to DHS's FISMA 2015 Questions for Inspectors General,* provides Treasury's response to the questionnaire. FISMA requires that the agency Inspector General (IG) or an independent external auditor perform the annual evaluation as determined by the IG. The Treasury Office of Inspector General (OIG) engaged KPMG LLP (KPMG) to conduct this independent evaluation in accordance with the Council of the *Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation.*

The objectives for this independent evaluation were to assess the effectiveness of Treasury's information security program and practices for the period of July 1, 2014 to June 30, 2015 for collateral NSS and to evaluate Treasury's compliance for the two collateral NSS with FISMA and related information security policies, procedures, standards, and guidelines. Additional details regarding the scope of our independent evaluation are included in Appendix I, *Objectives, Scope and Methodology*. Appendix II, *Status of Prior-Year Findings,* summarizes Treasury's progress in addressing prior year recommendations. Appendix IV contains a glossary of terms used in this report.

For fiscal year (FY) 2015, KPMG did not identify any substantial control deficiencies that impacted the design and operating effectiveness of Treasury's collateral NSS at the Departmental Offices (DO) and Bureau of Engraving and Printing (BEP) information security programs, and therefore, did not include any recommendations. Consistent with applicable FISMA requirements, OMB policy and guidelines, Committee on National Security Systems (CNSS) policy and guidelines, and National Institute of Standards and Technology (NIST) standards and guidelines, the Treasury's information security program and practices for its collateral NSS were established and have been maintained for the

10 FISMA program areas.[1] In a written response, the Treasury Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO) agreed with our conclusion (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

November 11, 2015

[1] As described in the DHS' *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics Version 1.2*, the 10 FISMA program areas are: continuous monitoring management, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, and contractor systems.

BACKGROUND

Federal Information Security Modernization Act of 2014 (FISMA)

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

FISMA defines a National Security System (NSS) as any information system used or operated by an agency or by a contractor of an agency where the function, operation, or use of those systems (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 collateral NSS, which are NSS that do not deal with intelligence. The audit of the Treasury's intelligence NSS will be reported separately by the Treasury Office of Inspector General (OIG).

Federal Standards and Guidelines

Except for systems that meet FISMA's definition of NSS, the Secretary of Commerce is responsible for prescribing standards and guidelines pertaining to federal information systems based on standards and guidelines developed by NIST. The Committee on National Security Systems (CNSS), and federal agencies that operate systems falling within the definition of NSS, provide security standards and guidance for NSS. CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, states that the controls described in NIST Special Publication (SP) 800-53, Revision (Rev.) 3, August 2009, *Recommended Security Controls for Federal Information Systems and Organizations*, shall apply to all NSS. In March 2014, CNSS updated the CNSS Instruction No. 1253 to include the updated NIST SP 800-53, Rev. 4, April 2013, *Security and Privacy Controls for Federal Information Systems and Organizations*, security controls. In addition, FISMA requires that NIST provide information security controls guidance for systems identified as NSS. Treasury used NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System (August 2003)*, to identify its two collateral systems.

Treasury is responsible for implementing policies, procedures, and control techniques for its collateral NSS based on guidance from CNSS. Treasury Directive Publication (TD P) 85-01 Volume II, provides Treasury security policy and standards for all systems that process or communicate classified national security information.

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

Treasury Information Security Management Program

The Treasury Chief Information Officer (CIO) is responsible for providing Treasury-wide leadership and direction for all areas of information and technology management, as well as the oversight of a number of 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 Treasury Office of the CIO (OCIO) Cyber Security Program develops and implements IT security policies and provides policy compliance oversight for both unclassified and collateral NSS managed by each of Treasury's bureaus. Two of the OCIO Cyber Security Program's missions are the management and coordination of the Treasury-wide program to address the cyber security requirements of NSS and the development of policy and program, or technical security performance reviews.

OVERALL EVALUATION RESULTS

Consistent with applicable FISMA requirements, OMB policy, CNSS policy and guidance and NIST standards and guidelines, the Treasury's information security program and practices for its collateral NSS were established and have been maintained for the 10 FISMA program areas. The FISMA program areas are outlined in the *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics Version 1.2* and were prepared by U.S. Department of Homeland Security (DHS) Office of Cybersecurity and Communications Federal Network Resilience. The 10 program areas are continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, and contractor systems. For FY 2015, we did not identify any substantial control deficiencies that impacted the design and operating effectiveness of Treasury's collateral NSS for the DO and BEP information security programs and, therefore, did not include any findings or recommendations in this report. In a written response to this report, the Treasury Deputy Assistant Secretary for Information Systems and CIO agreed with our conclusion (see *Management Response*).

Additionally, we evaluated the prior-year finding from the fiscal year (FY) 2014 FISMA Evaluation and determined that it was closed. See Appendix II, *Status of Prior-Year Findings*, for additional details.

MANAGEMENT RESPONSE TO THE REPORT

The following is the Treasury CIO's response, dated November 6, 2015, to the FY 2015 FISMA Evaluation for Collateral National Security Systems Report.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

November 6, 2015

MEMORANDUM FOR TRAM J. DANG
DIRECTOR FOR INFORMATION TECHNOLOY AUDIT

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

SUBJECT: Management Response to Draft Evaluation Report – Fiscal Year 2015 Evaluation of Treasury's Compliance with the Federal Information Security Management Act for Collateral National Security Systems

Thank you for the opportunity to review the Office of the Inspector General (OIG) draft report on the 2015 audit of the Department's implementation of the Federal Information Security Management Act (FISMA) for its collateral National Security Systems (NSS). We appreciate the OIG's recognition of our NSS cybersecurity program's general compliance with FISMA requirements for FY 2015, including the concurrence that the corrective actions taken in response to last year's audit were completed satisfactorily. This memorandum provides the management response to the draft report.

The report found that Treasury established an information security program and practices for its collateral NSS consistent with applicable FISMA requirements, OMB policy, CNSS policy and guidance and NIST standards and guidelines. We acknowledge that the draft report did not identify any substantial control deficiencies, and therefore, did not include any recommendations.

The Department remains committed to improving its security program. We have made notable progress over the past year to include:

- Improving vulnerability reporting and leadership engagement, allowing for greater awareness of the current security posture of the NSS.

- Initiating the deployment of Public Key Infrastructure and IPSec Virtual Private Network to enhance the security of information transferred across the network.

- Procuring additional personnel solely dedicated to the support and oversight of the NSS security program's goals.

Going forward, we will continue to improve our security posture by implementing a Continuous Monitoring plan that will ensure security controls remain aligned with organizational risk tolerance and provide the information needed to respond to any risks in a timely manner. If you have any questions, feel free to contact Terry Bartlett, Acting Associate Chief Information Officer for Cyber Security, at 202-622-2786.

APPENDIX I – OBJECTIVES, SCOPE AND METHODOLOGY

The objectives for this independent evaluation were to assess effectiveness of the Department of the Treasury's (Treasury) information security program and practices for the period July 1, 2014 to June 30, 2015 for the Treasury's collateral National Security Systems (NSS). Specifically, the objectives of this evaluation were to:

- Perform the annual independent Federal Information Security Modernization Act of 2014 (FISMA) evaluation of Treasury's information security programs and practices, as they relate to its collateral NSS.
- Respond to Department of Homeland Security (DHS) FISMA Questions on behalf of the Treasury Office of Inspector General (OIG).
- Follow up on the status of prior-year FISMA findings.

We conducted our independent evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation and the contract requirement, which called for an evaluation of a limited subset of NIST Special Publication (SP) 800-53 Revision (Rev.) 4 controls.

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; Presidential directives; the DHS *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics Version 1.2*, dated June 19, 2015; 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.

We took a phased approach to satisfy the evaluation's objective as listed below:

PHASE A: **Assessment of Department-Level Compliance**

To gain an enterprise-level understanding, we assessed management, policies, and guidance for the overall Treasury-wide information security program for collateral NSS per requirements defined in FISMA and DHS *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics Version 1.2*, NIST SP 800-53, Rev. 4, as well as Treasury guidelines developed in response to FISMA. This included program controls applicable to certification and accreditation, security configuration management, incident response and reporting, security training, plan of action and milestones (POA&M), remote access, account and identity management, continuous monitoring management, contingency planning, and contractor systems.

PHASE B: Assessment of System-Level Compliance

To gain a system-level understanding, we assessed the implementation of the guidance for the two limited-connectivity Treasury collateral NSS according to requirements defined in FISMA and DHS *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics Version 1.2*, as well as Treasury guidelines developed in response to FISMA. This included program controls applicable to certification and accreditation, security configuration management, incident response and reporting, security training, POA&M, remote access, account and identity management, continuous monitoring management, contingency planning, and contractor systems.

Other Considerations

In performing our control evaluations, we interviewed key Treasury Office of the Chief Information Officer (OCIO) and BEP personnel who had significant information security responsibilities, and personnel responsible for the two Treasury collateral NSS. We also evaluated Treasury's and bureaus' policies, procedures, and guidelines. Lastly, we evaluated selected security-related documents and records, including certification and accreditation 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 22, 2015 through August 31, 2015. During our evaluation, we met with Treasury management to discuss our preliminary conclusions.

Criteria

We focused our FISMA evaluation approach on federal information security guidance developed by CNSS, NIST, and Office of Management and Budget (OMB). NIST 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 (FY) 2015 FISMA evaluation:

CNSS Policy and Instructions

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

NIST Federal Information Processing Standards (FIPS) and/or Special Publications

- 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 SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-based Model*
- NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST SP 800-46 Revision 1, *Guide to Enterprise Telework and Remote Access Security*
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*

- NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*
- NIST SP 800-60 Revision 1, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*
- NIST SP 800-70, Revision 2, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*

OMB Policy Directives

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

United States Department of Homeland Security

- DHS' *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics Version 1.2*

Treasury Policy Directives

- Treasury Directive Publication (TD P) 15-71, *Department of the Treasury Security Manual*
- TD P 85-01, *Treasury Information Security Policy Volume II Classified (National Security) Systems*
- Other Treasury Information and Information Technology Security Policies and Procedures

APPENDIX II – STATUS OF PRIOR-YEAR FINDINGS

As part of this year's FISMA Evaluation, we followed up on the status of the prior year findings. For the following prior year finding, we evaluated the collateral National Security Systems (NSS) to determine whether the recommendations have been implemented. We inquired of the 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 determined the finding to be closed.

Prior Year Findings – 2014 Evaluation

Finding #	Prior-Year Condition	Recommendation(s)	Status
Prior Year FY 2014 Finding #1 – Departmental Office (DO) Logical account management activities were not consistently performed for the DO collateral NSS	We identified two TSDN user accounts who never logged in and were not disabled after 90 days of inactivity.	We recommend that CNSS DO management: 1. Ensure the security team is appropriately re-enabling the correct accounts. 2. Ensure that the all user's accounts are disabled after 90 days of inactivity.	**Implemented/Closed** KPMG obtained and inspected the user listing for the DO collateral NSS and noted that no user account were inappropriately re-enabled. KPMG further inspected the user listing and noted that all inactive users had been appropriately disabled after 90 days of inactivity.

APPENDIX III – DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS's FISMA 2015 QUESTIONS FOR INSPECTORS GENERAL

The information included in Appendix III represents the Department of the Treasury's (Treasury) consolidated responses to Department of Homeland Security's (DHS) FISMA 2015 questions for Inspectors General. KPMG prepared responses to DHS questions based on an assessment of the two collateral NSS and across two Treasury components. KPMG determined the overall status of each DHS question based on the magnitude of the aggregated findings under each category with OIG acceptance.

1: Continuous Monitoring Management		
Status of Continuous Monitoring Management Program [check one: Yes or No]		**1.1** Utilizing the ISCM maturity model definitions, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.
	Ad Hoc (Level 1)*	**1.1.1.** Please provide the D/A ISCM maturity level for the People domain.
	Ad Hoc (Level 1)*	**1.1.2.** Please provide the D/A ISCM maturity level for the Processes domain.
	Ad Hoc (Level 1)*	**1.1.3.** Please provide the D/A ISCM maturity level for the Technology domain.
	Ad Hoc (Level 1)*	**1.1.4.** Please provide the D/A ISCM maturity level for the ISCM Program Overall.
	N/A†	**1.2.** Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model above.

Note *: In FY 2015, CyberScope included the Inspector General (IG) Information Security Continuous Monitoring (ISCM) maturity model to summarize the status on a 5-level scale from lowest to highest: Ad Hoc (Level 1), Defined (Level 2), Consistently Implemented (Level 3), Managed and Measurable (Level 4), and Optimized (Level 5).

2: Configuration Management		
Status of Configuration Management Program [check one: Yes or No]	Yes	**2.1** Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**2.1.1.** Documented policies and procedures for configuration management.
	Yes	**2.1.2.** Defined standard baseline configurations.
	Yes	**2.1.3.** Assessments of compliance with baseline configurations

† No additional information on the effectiveness.

2: Configuration Management		
	Yes	**2.1.4.** Process for timely (as specified in organization policy or standards) remediation of scan result findings.
	Yes	**2.1.5.** For Windows-based components, USGCB secure configuration settings are fully implemented (when available), and any deviations from USGCB baseline settings are fully documented.
	Yes	**2.1.6.** Documented proposed or actual changes to the hardware and software configurations.
	Yes	**2.1.7.** Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI-2).
	Yes	**2.1.8.** Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2).
	Yes	**2.1.9.** Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches (NIST SP 800-53: CM-3, SI-2).
	N/A[†]	**2.2.** Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above.
	Yes	**2.3.** Does the organization have an enterprise deviation handling process and is it integrated with the automated scanning capability.
	Yes	**2.3.1.** Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented.

3: Identity and Access Management		
Status of Identity and Access Management Program [check one: Yes or No]	Yes	**3.1** Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?
	Yes	**3.1.1.** Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1).
	Yes	**3.1.2.** Identifies all users, including Federal employees, contractors, and others who access organization systems (HSPD 12, NIST SP 800-53, AC-2).
	Yes	**3.1.3.** Organization has planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). **Comments - Treasury OIG for collateral NSS:** DO did not fully implement multifactor authentication as required by NIST and Treasury guidance. However, DO has a plan for implementation

[†] No additional information on the effectiveness.

3: Identity and Access Management		
		of PIV for logical access. In the interim, DO has accepted this risk and a risk-based acceptance letter has been signed that remains in effect until August 31, 2015.
	Yes	**3.1.4.** Organization has planned for implementation of PIV for physical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).
	Yes	**3.1.5.** Ensures that the users are granted access based on needs and separation-of-duties principles.
	Yes	**3.1.6.** Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. IP phones, faxes, printers).
	Yes	**3.1.7.** Ensures that accounts are terminated or deactivated once access is no longer required.
	Yes	**3.1.8.** Identifies and controls use of shared accounts.
	N/A[†]	**3.2.** Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was not noted in the questions above.

4: Incident Response and Reporting		
Status of Identity and Access Management Program [check one: Yes or No]	Yes	**4.1** Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**4.1.1.** Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1).
	Yes	**4.1.2.** Comprehensive analysis, validation, and documentation of incidents.
	Yes	**4.1.3.** When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19).
	Yes	**4.1.4.** When applicable, reports to law enforcement and the agency Inspector General within established time frames.
	Yes	**4.1.5.** Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19).
	Yes	**4.1.6.** Is capable of correlating incidents.
	Yes	**4.1.7.** Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; and OMB M-07-16, M-06-19).
	N/A[†]	**4.2.** Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.

[†] No additional information on the effectiveness.

5: Risk Management		
Status of Risk Management Program [check one: Yes or No]	Yes	**5.1** Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	Yes	**5.1.1.** Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1.
	Yes	**5.1.2.** Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1.
	Yes	**5.1.3.** Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1.
	Yes	**5.1.4.** Has an up-to-date system inventory.
	Yes	**5.1.5.** Categorizes information systems in accordance with government policies.
	Yes	**5.1.6.** Selects an appropriately tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.
	Yes	**5.1.7.** Implements the approved set of tailored set of baseline security controls specified in metric 5.1.6.
	Yes	**5.1.8.** Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
	Yes	**5.1.9.** Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
	Yes	**5.1.10.** Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.
	Yes	**5.1.11.** Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).
	Yes	**5.1.12.** Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks.
	Yes	**5.1.13.** Security authorization package contains system security plan, security assessment report, POA&M, and accreditation boundary in accordance with government policies (NIST SP 800-18, SP 800-37).
	Yes	**5.1.14.** The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.
	Yes	**5.1.15** For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems

5: Risk Management		
	N/A†	**5.2.** Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above.

6: Security Training		
Status of Security Training Program [check one: Yes or No]	Yes	**6.1** Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**6.1.1.** Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1).
	Yes	**6.1.2.** Documented policies and procedures for specialized training for users with significant information security responsibilities.
	Yes	**6.1.3.** Security training content based on the organization and roles, as specified in organization policy or standards.
	Yes	**6.1.4.** Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training.
	Yes	**6.1.5.** Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.
	Yes	**6.1.6.** Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53).
	N/A†	**6.2.** Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.

7: POA&M		
Status of POA&M Program [check one: Yes or No]	Yes	**7.1** Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**7.1.1.** Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.
	Yes	**7.1.2.** Tracks, prioritizes, and remediates weaknesses.
	Yes	**7.1.3.** Ensures remediation plans are effective for correcting weaknesses.
	Yes	**7.1.4.** Establishes and adheres to milestone remediation dates and provides adequate justification for missed remediation dates.

† No additional information on the effectiveness.

7: POA&M		
	Yes	**7.1.5.** Ensures resources and ownership are provided for correcting weaknesses.
	Yes	**7.1.6.** POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25).
	Yes	**7.1.7.** Costs associated with remediating weaknesses are identified in terms of dollars (NIST SP 800-53: PM-3; OMB M-04-25).
	Yes	**7.1.8.** Programs officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53: CA-5; and OMB M-04-25).
	N/A[†]	**7.2.** Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above.

8: Remote Access Management		
Status of Remote Access Management Program [check one: Yes or No]	Yes	**8.1** Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**8.1.1.** Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17).
	Yes	**8.1.2.** Protects against unauthorized connections or subversion of authorized connections.
	Yes	**8.1.3.** Users are uniquely identified and authenticated for all access (NIST 800-46, Section 4.2, Section 5.1).
	Yes	**8.1.4.** Telecommuting policy is fully developed (NIST 800-46, Section 5.1).
	Yes	**8.1.5.** Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.
	Yes	**8.1.6.** Defines and implements encryption requirements for information transmitted across public networks.
	Yes	**8.1.7.** Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.
	Yes	**8.1.8.** Lost or stolen devices are disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).
	Yes	**8.1.9.** Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4).
	Yes	**8.1.10.** Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1, NIST SP 800-53, PS-6).

[†] No additional information on the effectiveness.

8: Remote Access Management		
	N/A	**8.2.** Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above. **Comments - Treasury OIG for collateral NSS:** While OCIO has a policy in place that addresses Remote Access Management, neither DO nor BEP's collateral NSS allow remote access.
	Yes	**8.3.** Does the organization have a policy to detect and remove unauthorized (rogue) connections?

9: Contingency Planning		
Status of Contingency Planning Program [check one: Yes or No]	Yes	**9.1** Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**9.1.1.** Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1).
	Yes	**9.1.2.** The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the appropriate analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan (NIST SP 800-34).
	Yes	**9.1.3.** Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures (NIST SP 800-34).
	Yes	**9.1.4.** Testing of system-specific contingency plans.
	Yes	**9.1.5.** The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).
	Yes	**9.1.6.** Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53).
	Yes	**9.1.7.** Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans.
	Yes	**9.1.8.** After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).
	Yes	**9.1.9.** Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for system that require them (FCD1, NIST SP 800-34, NIST SP 800-53).
	Yes	**9.1.10.** Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).
	Yes	**9.1.11.** Contingency planning that considers supply chain threats.

9: Contingency Planning		
	N/A†	**9.2.** Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.

10: Contractor Systems		
Status of Contractor Systems [check one: Yes or No]	Yes	**10.1** Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including for organization systems and services residing in the cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes?
	Yes	**10.1.1.** Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities (including other government agencies), including organization systems and services residing in a public, hybrid, or private cloud.
	Yes	**10.1.2.** The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with FISMA requirements, OMB policy, and applicable NIST guidelines (NIST SP 800-53: CA-2).
	Yes	**10.1.3.** A complete inventory of systems operated on the organization's behalf by contractors or other entities, (including other government agencies), including organization systems and services residing in a public, hybrid, or private cloud.
	Yes	**10.1.4.** The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5).
	Yes	**10.1.5.** The Organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.
	Yes	**10.1.6.** The inventory of contractor systems is updated at least annually.
	N/A†	**10.2.** Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.

† No additional information on the effectiveness.

APPENDIX IV – GLOSSARY OF TERMS

Acronym	Definition
AC	Access Control
AT	Awareness and Training
BCP	Business Continuity Planning
BEP	U.S. Bureau of Engraving and Printing
BIA	Business Impact Analysis
CA	Security Assessment and Authorization
CIO	Chief Information Officer
CM	Configuration Management
CNSS	Committee on National Security Systems
DHS	Department of Homeland Security
DO	Departmental Offices
DRP	Disaster Recovery Plan
FCD	Federal Continuity Directive
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
HSPD	Homeland Security Presidential Directive
IG	Inspector General
ISCM	Information Security Continuous Monitoring
IT	Information Technology
KPMG	KPMG LLP
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NSS	National Security System
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestone
PL	Planning
PM	Program Management
PS	Personnel Security
RA	Risk Assessment
Rev.	Revision
SA	System and Services Acquisition
SI	System and Information Integrity
SP	Special Publication
TD P	Treasury Directive Publication

Acronym	Definition
Treasury	Department of the Treasury
TT&E	Test, Training & Exercise
USGCB	United States Government Configuration Baseline

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