



Audit Report



(U) OIG-14-047

(U) Fiscal Year 2014 Audit of Treasury's Compliance with the Federal Information Security Management Act for Its Intelligence Systems

(U) September 15, 2014

Derived By: Tram J. Dang
Director, Information Technology Audit
Derived From: Treasury Classification Guide
March 2, 2012
Declassify On: 20390916

Controlled by 4822
Date 7/21/15

Office of
Inspector General
Department of the Treasury

Contents

(U) Audit Report

(U) Results in Brief 2

(U) Background..... 3

(U) Results of Audit..... 4

 (U//~~FOUO~~) Finding 1 Not All TFIN Devices Were Compliant with
 Baseline Configurations 4

 (U) Recommendation 5

Appendix 1 (U) Objectives, Scope, and Methodology 7

Appendix 2 (U) Management Response 8

Appendix 3 (U) Responses to Intelligence Community Inspector General
 Questions 9

Appendix 4 (U) Major Contributors to this Report..... 26

Appendix 5 (U) Report Distribution..... 27

(U) Abbreviations and Acronyms

(U) CIO	Chief Information Officer
(U) CNSSI	Committee on National Security Systems Instruction
(U) DO	Departmental Offices
(U) FISMA	Federal Information Security Management Act
(U) IC	Intelligence Community
(U) IC IG	Office of the Inspector General of the Intelligence Community
(U) IT	Information Technology
(U) NIST SP	National Institute of Standards and Technology Special Publication
(U) TD P	Treasury Directive Publication
(U) TFIN	Treasury Foreign Intelligence Network
(U) Treasury	Department of the Treasury

This Page Intentionally Left Blank



Audit Report

*The Department of the Treasury
Office of Inspector General*

September 15, 2014

Leslie Ireland
Assistant Secretary for Intelligence and Analysis

Raghav Vajjhala
Acting Deputy Assistant Secretary for Information Systems
and Chief Information Officer

(U//~~FOUO~~) This report presents the results of our audit of the Department of the Treasury's (Treasury) compliance with the Federal Information Security Management Act of 2002 (FISMA)¹ related to its intelligence systems. FISMA requires that we perform an annual evaluation of Treasury's security programs and practices for its national security systems. The objective of this audit was to assess the status of Treasury's compliance with FISMA requirements related to its intelligence systems for fiscal year (FY) 2014. As part of our audit, we also assessed Treasury's progress in resolving the previously reported FISMA-related weakness cited in our prior year report². Furthermore, the Office of the Inspector General of the Intelligence Community (hereinafter referred to as the IC IG) issued a memorandum dated April 8, 2014³ that directed the Offices of Inspector General within the Intelligence Community (IC) to base their evaluations or audits on the Department of Homeland Security's FY 2014 FISMA guidance⁴. Appendix 1 provides

¹ (U) Pub. L. 107-347 (Dec. 17, 2002)

² (U) *Information Technology: Fiscal Year 2013 Audit of Treasury's FISMA Implementation for Its Intelligence Systems*, OIG-13-048 (Aug. 29, 2013).

³ (U) IC IG memorandum, *FY 2014 Federal Information Security Management Act of 2002 Guidance for Offices of the Inspector General of the Intelligence Community* (Apr. 8, 2014).

⁴ (U) *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics* (Dec. 2, 2013)

more detail of our objective, scope, and methodology. Appendix 3 provides our responses to the IC IG's FY 2014 FISMA metrics.

(U) Results in Brief

(U//FOUO) In brief, we determined that Treasury's information security program and practices, as they relate to its intelligence systems, generally complied with FISMA requirements in FY 2014. However, we found that some Treasury Foreign Intelligence Network (TFIN) devices were not fully compliant with baseline configurations, and therefore, recommend that Treasury's Chief Information Officer (CIO) ensure that Departmental Offices (DO) complete its planned corrective actions to ensure all TFIN's baseline configurations are established and implemented. We also determined that Treasury appropriately closed the previously reported finding and recommendation related to security incident response and reporting identified in our prior year audit.

(U//FOUO) It should also be noted that we did not report on Treasury's compliance with the recently updated *Committee on National Security Systems Instruction (CNSSI) 1253*, revised March 27, 2014. The revised instruction requires updates to system security plans for all national security systems and additional controls from the National Institute of Standards and Technology Special Publication (NIST SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Rev. 4, which was issued in April 2013. We plan to assess Treasury's compliance with the new requirements as part of our FY 2015 FISMA engagement.

(U) A copy of this report will be provided to the IC IG and will be included in the IC IG's report to the Director of National Intelligence.

(U//FOUO) In a written response to a draft copy of this report, the Assistant Secretary for Intelligence and Analysis and the Deputy Assistant Secretary for Information Systems and CIO agreed with our finding and associated recommendation and stated that the CIO had previously identified this concern and

already established a plan of corrective action with a target completion date of April 2015 (see appendix 2). The planned corrective action is responsive to the intent of our recommendation.

(U) Background

(U) FISMA was enacted as part of the E-Government Act of 2002⁵, intended to enhance the management and promotion of electronic government services and processes. FISMA provides a framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets and for the maintenance of minimum controls required to protect federal information and information systems.

(U) FISMA defines a national security system as any information system used or operated by an agency or an agency contractor where the function, operation, or use of those systems involves: (1) intelligence activities, (2) cryptologic activities related to national security, (3) command and control of military forces, (4) equipment that is an integral part of a weapon or weapons system, or (5) a system that is critical to the direct fulfillment of military or intelligence missions. FISMA requires agencies to annually review their national security systems' information security program and practices.

(U//~~FOUO~~) Treasury Directive Publication (TD P) 15-03⁶ established the Assistant Secretary for Intelligence and Analysis (OIA) as Treasury's "IC element head"⁷ who is responsible for Treasury's intelligence information technology (IT) systems, networks, and applications. In December 2011, the Assistant Secretary for Intelligence and Analysis designated Treasury's

⁵ (U) Pub. L. 107-347 (Dec. 17, 2002)

⁶ (U) TD P 15-03, *Intelligence Information Systems Security Manual*, version 2.1. (June 2013)

⁷ (U) TD P 15-03, "The Treasury IC element head is a government employee who possesses the ultimate IT systems security responsibility for his or her Treasury programs, including responsibility for any decisions made on his or her behalf. This responsibility includes IT systems security program oversight and IT system security protections commensurate with the risk and impact to the program."

CIO as the Authorizing Official for Treasury's intelligence information systems. The Authorizing Official has specific accreditation authority and responsibility for TFIN under DO [REDACTED] 7E [REDACTED]. In a memo dated April 28, 2014, the Assistant Secretary for Intelligence and Analysis and the Assistant Secretary for Management agreed to transition the responsibilities and resources for the management and operation of Treasury Intelligence Information Systems back to the Office of Intelligence and Analysis.

(U) TD P 15-03 also set forth the security policy for classified intelligence IT systems to ensure Treasury's compliance with all laws and standards applicable to the IC. Authoritative standards include CNSSI 1253 which is the standard for categorizing information and information systems, and for selecting security and programmatic controls for national security systems. It serves as a companion to NIST SP 800-53, Rev. 3⁸, with CNSSI 1253 being the authoritative standard should conflict arise. NIST SP 800-53A, Rev. 1⁹, provides guidelines for building effective security assessment plans and a comprehensive set of procedures for assessing the effectiveness of security controls. As noted above, recent changes to CNSSI 1253 and NIST SP 800-53 were not applicable to Treasury's FY 2014 FISMA compliance.

(U) Results of Audit

(U//FOUO) Finding 1 Not All TFIN Devices Were Compliant with Baseline Configurations

(U//FOUO) We found that some TFIN devices did not comply with baseline configuration requirements based on our review of Treasury's *Department's Monthly National Security Program Status of Key Performance Metrics Report[s]*. Specifically, CIO reported that scans of devices attached to TFIN's network (e.g.

⁸ (U) NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (Aug. 2009)

⁹ (U) NIST Special Publication 800-53A Revision 1, *Guide for Assessing Security Controls in Federal Information Systems and Organizations* (June 2010)

computer workstations, servers, printers) showed baseline configuration compliance at 71 percent in March 2014 and 74 percent for April and May 2014.

(U//FOUO) NIST SP 800-53 requires that organizations develop, document, and maintain under configuration control, a current baseline configuration of the information system. Additionally, organizations must document and approve any deviations from the established baseline configuration. Non-compliance with secure configuration baselines may interfere with patch management and version control. As a result, TFIN devices may not be protected with the most secure recommended configurations, increasing the risk of being compromised or misused.

(U//FOUO) According to DO management, TFIN does not have documented configuration baselines for some devices. In addition, changes in configuration baseline requirements for national security systems, as included in the National Security Agency's *2013 Minimum Baseline Requirements for National Security Systems – Action Memorandum*, are still being implemented on some devices. As noted in the Office of the Chief Information Officer's *Department of the Treasury Departmental Offices National Security Program Review Report (Intelligence) Fiscal Year 2014*, secure configuration baselines are still being established for some devices. DO management concurred with the observations and recommendations made in this report and noted that it plans to remediate the issue by April 30, 2015. Furthermore, we verified that DO is tracking the issue in its Plan of Action and Milestones. We plan to assess the status of DO's remediation as part of our FY 2015 FISMA engagement.

(U) Recommendation

(U//FOUO) We recommend that Treasury's CIO ensures that DO carries out its planned corrective actions to resolve TFIN baseline configuration deviations.

(U) Management Response

(U//FOUO) Management agreed with our recommendation and stated the CIO had previously identified this concern and already established a plan of corrective action with a target completion date of April 2015.

(U) Office of Inspector General Comment

(U) Management's reported corrective action is responsive to our recommendation.

* * * * *

(U) I would like to extend my appreciation to the Treasury Office of Intelligence and Analysis and the Office of the Chief Information Officer for the cooperation and courtesies extended to my staff during the audit. If you have any questions, please contact me at (202) 927-5171 or Larissa Klimpel, Audit Manager, IT Audit, at (202) 927-0361. Major contributors to this report are listed in appendix 4.

/s/

Tram J. Dang
Director, IT Audit

Appendix 1
(U) Objectives, Scope, and Methodology

(U) In March 2014, we initiated an audit of the Department of the Treasury's (Treasury) compliance with the *Federal Information Security Act of 2002* (FISMA). FISMA requires that we perform an annual evaluation of Treasury's security programs and practices for its national security systems. The objective of our audit was to assess the status of Treasury's compliance with FISMA requirements related to its intelligence systems in fiscal year 2014. As part of our audit, we also assessed Treasury's progress in resolving the previously reported FISMA related weakness cited in our prior year's report¹⁰. This audit was included in the *Office of Inspector General's Annual Plan Fiscal Year 2014*.

(U) To meet our audit objectives, we reviewed applicable laws, regulations, and standards related to national security systems; conducted data calls of Treasury's bureaus and offices; analyzed supporting documentation and other classified information; interviewed key Treasury officials and personnel; and followed up on the status of the prior year finding. We performed our audit fieldwork between March 2014 and July 2014.

(U) 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.

¹⁰ (U) *Information Technology: Fiscal Year 2013 Audit of Treasury's Federal Information Security Management Act Implementation for Its Intelligence Systems*, OIG-13-048 (Aug. 29, 2013).

Appendix 2
(U) Management Response



(UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)
DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

SEP 4 2014

**MEMORANDUM FOR MARLA FREEDMAN
ASSISTANT INSPECTOR GENERAL FOR AUDIT**

FROM: S. Leslie Ireland [REDACTED] 6
Assistant Secretary for Intelligence and Analysis

Raghav Vajjhala [REDACTED] 6
Acting Deputy Assistant Secretary for Information Systems
and Chief Information Officer

SUBJECT: (U) Management Response to Draft Report – Fiscal Year 2014
Audit of Treasury’s Federal Information Security Management Act
Implementation for its Intelligence Systems

(U) Thank you for the opportunity to review the Office of the Inspector General’s (OIG) draft report on the 2014 audit of the Department’s implementation of the Federal Information Security Management Act for its Intelligence Systems. We appreciate the OIG’s recognition of our Intelligence Community cybersecurity program’s general compliance with FISMA requirements for FY2014, including the concurrence that all corrective actions planned following last year’s audit were completed satisfactorily.

(U//~~FOUO~~) The draft report makes one recommendation with regard to configuration management. We accept this recommendation and its associated finding. As noted in the draft report, the Treasury CIO had previously identified this concern, and had established a plan of corrective action with a target completion date of April 2015.

(U) Going forward, we will continue to strive to improve and sustain a strong security program and provide appropriate protection to critical information throughout Treasury. If you have any questions, feel free to contact Edward Roback, Associate Chief Information Officer for Cyber Security, on 202-622-2593.

cc: Tram Dang, Director, Information Technology Audit

(UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~)

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

(U) FY 2014 IG FISMA Metrics

1: (U) CONTINUOUS MONITORING MANAGEMENT		Answer
(U) <i>Please select Yes or No from the pull down menu.</i>		
1.1 (U) Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		Yes
1.1.1	(U) Documented policies and procedures for continuous monitoring (NIST SP 800-53: CA-7)(AP)	Yes
1.1.2	(U) Documented strategy for information security continuous monitoring (ISCM) (AP)	Yes
1.1.3	(U) Implemented ISCM for information technology assets (AP)	Yes
1.1.4	(U) Evaluate risk assessments used to develop their ISCM strategy (AP)	Yes
1.1.5	(U) Conduct and report on ISCM results in accordance with their ISCM strategy (AP)	Yes
1.1.6	(U) Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53, NIST SP 800-53A) (AP)	Yes
1.1.7	(U) Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, NIST SP 800-53A) (AP)	Yes
This chart is UNCLASSIFIED		

(U) Fiscal Year 2014 Audit of Treasury's Compliance with the Federal Information Page 9 Security Management Act for Its Intelligence Systems (OIG-14-047)

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

1: (U) CONTINUOUS MONITORING MANAGEMENT	Answer
<u>(U) Please select Yes or No from the pull down menu.</u>	
(U) Explanation: N/A	
1.2 (U) Please provide any additional information on the effectiveness of the organization's Continuous Monitoring Management Program that was <u>not noted</u> in the questions above.	
1.2 (U) Response: N/A	
This chart is UNCLASSIFIED	

2: (U) CONFIGURATION MANAGEMENT	Answer	
<u>(U) Please select Yes or No from the pull down menu.</u>		
2.1 (U) 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?		
2.1.1	(U) Documented policies and procedures for configuration management (Base)	Yes
2.1.2	(U) Defined standard baseline configurations (Base)	Yes
2.1.3	(U) Assessments of compliance with baseline configurations (Base)	Yes
2.1.4	(U) Process for timely (as specified in organization policy or standards) remediation of scan result deviations (Base)	Yes
2.1.5	(U// FOUO) For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented (Base)	No
2.1.6	(U) Documented proposed or actual changes to hardware and software configurations (Base)	Yes
This chart is UNCLASSIFIED// FOR OFFICIAL USE ONLY		

(U) Fiscal Year 2014 Audit of Treasury's Compliance with the Federal Information Page 10 Security Management Act for Its Intelligence Systems (OIG-14-047)

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

2: (U) CONFIGURATION MANAGEMENT		Answer
<u>(U) Please select Yes or No from the pull down menu.</u>		
2.1.7	(U) Process for timely and secure installation of software patches (Base)	Yes
2.1.8	(U) Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53: RA-5, SI-2) (Base)	Yes
2.1.9	(U) 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) (Base)	Yes
2.1.10	(U) Patch management process is fully developed, as specified in organization policy or standards (NIST SP 800-53: CM-3, SI-2) (Base)	Yes
Explanation: (U// FOUO) 2.1.5. TFIN devices are not compliant with baseline configurations. Note: When USGCB was not applicable, we evaluated based on NSA-defined baseline requirements , as prescribed in the 2013 Minimum Baseline Requirements for National Security Systems Memo, issued by NSA on January 25, 2013		
2.2 (U) Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was <u>not noted</u> in the questions above.		
2.2 (U) Response: N/A		
2.3 (U) Does the organization have an enterprise deviation handling process and is it integrated with the automated capability (Base)		Yes
2.3.1	(U) Is there a process for mitigating the risk introduced by those deviations (Base)	Yes
This chart is UNCLASSIFIED// FOR OFFICIAL USE ONLY		

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

3: (U) Identity and Access Management		Answer
<i>(U) Please select Yes or No from the pull down menu.</i>		
		Yes
3.1.1	(U) Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1) (Base)	Yes
3.1.2	(U) Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2) (Base)	Yes
3.1.3	(U) Identifies when special access requirements (e.g., multi-factor authentication) are necessary (Base)	Yes
3.1.4	(U) If multi-factor authentication is in use, it is linked to the organization's PIV program where appropriate (NIST SP 800-53, IA-2) (KFM)	Yes
3.1.5	(U) 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) (AP)	Yes
3.1.6	(U) Organization has adequately planned for implementation of PIV for physical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11)	Yes
3.1.7	(U) Ensures that the users are granted access based on needs and separation-of-duties principles (Base)	Yes
This chart is UNCLASSIFIED		

(U) Fiscal Year 2014 Audit of Treasury's Compliance with the Federal Information Page 12 Security Management Act for Its Intelligence Systems (OIG-14-047)

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

3: (U) Identity and Access Management		Answer
<i>(U) Please select Yes or No from the pull down menu.</i>		
3.1.8	(U) Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts) (Base)	Yes
3.1.9	(U) Identifies all user and non-user accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users) (Base)	Yes
3.1.10	(U) Ensures that accounts are terminated or deactivated once access is no longer required (Base)	Yes
3.1.11	(U) Identifies and controls use of shared accounts (Base)	Yes
(U) Explanation: N/A		
3.2 (U) Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was <u>not noted</u> in the questions above.		
3.2 (U) Response: N/A		
This chart is UNCLASSIFIED		

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

4: (U) Incident Response and Reporting		Answer
(U) <i>Please select Yes or No from the pull down menu.</i>		
4.1 (U) 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	(U) Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1) (Base)	Yes
4.1.2	(U) Comprehensive analysis, validation, and documentation of incidents (KFM)	Yes
4.1.3	(U) When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, NIST SP 800-61; OMB M-07-16, OMB M-06-19) (KFM)	Yes
4.1.4	(U) When applicable, reports to law enforcement within established timeframes (SP 800-61) (KFM)	Yes
4.1.5	(U) Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, NIST SP 800-61; OMB M-07-16, OMB M-06-19) (KFM)	Yes
4.1.6	(U) Is capable of tracking and managing risks in a virtual/cloud environment, if applicable (Base)	Yes
4.1.7	(U) Is capable of correlating incidents (Base)	Yes
4.1.8	(U) Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, NIST SP 800-61; OMB M-07-16, OMB M-06-19) (Base)	Yes
(U) Explanation: N/A		
4.2 (U) Please provide any additional information on the effectiveness of the organization's Incident Management Program that was <u>not noted</u> in the questions above.		
This chart is UNCLASSIFIED		

(U) Fiscal Year 2014 Audit of Treasury's Compliance with the Federal Information Page 14 Security Management Act for Its Intelligence Systems (OIG-14-047)

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

4: (U) Incident Response and Reporting	Answer
(U) <i>Please select Yes or No from the pull down menu.</i>	
4.2 (U) Response: N/A	
This chart is UNCLASSIFIED	

5: (U) Risk Management		Answer
(U) <i>Please select Yes or No from the pull down menu.</i>		
5.1 (U) 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	(U) Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process (Base)	Yes
5.1.2	(U) Addresses risk from an <u>organization perspective</u> with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1 (Base)	Yes
5.1.3	(U) Addresses risk from a <u>mission and business process perspective</u> and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1 (Base)	Yes
5.1.4	(U) Addresses risk from an <u>information system perspective</u> 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 (Base)	Yes
5.1.5	(U) Has an up-to-date system inventory (Base)	Yes
This chart is UNCLASSIFIED		

(U) Fiscal Year 2014 Audit of Treasury's Compliance with the Federal Information Page 15 Security Management Act for Its Intelligence Systems (OIG-14-047)

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

5: (U) Risk Management		Answer
(U) <i>Please select Yes or No from the pull down menu.</i>		
5.1.6	(U) Categorizes information systems in accordance with government policies (Base)	Yes
5.1.7	(U) Selects an appropriately tailored set of baseline security controls (Base)	Yes
5.1.8	(U) Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation (Base)	Yes
5.1.9	(U) 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 (Base)	Yes
5.1.10	(U) 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 (Base)	Yes
5.1.11	(U) Ensures information security controls are monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials (Base)	Yes
5.1.12	(U) Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization (Base)	Yes
5.1.13	(U) Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO) (Base)	Yes
This chart is UNCLASSIFIED		

(U) Fiscal Year 2014 Audit of Treasury's Compliance with the Federal Information Page 16 Security Management Act for Its Intelligence Systems (OIG-14-047)

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

5: (U) Risk Management		Answer
<i>(U) Please select Yes or No from the pull down menu.</i>		
5.1.14	(U) 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 (Base)	Yes
5.1.15	(U) Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies (NIST SP 800-18, NIST SP 800-37) (Base)	Yes
5.1.16	(U) Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems (Base)	Yes
(U) Explanation: N/A		
5.2 (U) Please provide any additional information on the effectiveness of the organization's Risk Management Program that was <u>not noted</u> in the questions above.		
5.2 (U) Response: N/A		
This chart is UNCLASSIFIED		

6: (U) Security Training		Answer
<i>(U) Please select Yes or No from the pull down menu.</i>		
6.1	(U) 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
This chart is UNCLASSIFIED		

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

6: (U) Security Training		Answer
(U) <i>Please select Yes or No from the pull down menu.</i>		
6.1.1	(U) Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1)(Base)	Yes
6.1.2	(U) Documented policies and procedures for specialized training for users with significant information security responsibilities (Base)	Yes
6.1.3	(U) Security training content based on the organization and roles, as specified in organization policy or standards (Base)	Yes
6.1.4	(U) 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 (KFM)	Yes
6.1.5	(U) 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 (KFM)	Yes
6.1.6	(U) Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, NIST SP 800-53) (Base)	Yes
(U) Explanation: N/A		
6.2 (U) Please provide any additional information on the effectiveness of the organization's Security Training Program that was <u>not noted</u> in the questions above.		
6.2 (U) Response N/A		
This chart is UNCLASSIFIED		

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

7: (U) PLAN OF ACTION & MILESTONES (POA&M)		Answer
(U) <i>Please select Yes or No from the pull down menu.</i>		
7.1 (U) 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	(U) Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation (Base)	Yes
7.1.2	(U) Tracks, prioritizes, and remediates weaknesses (Base)	Yes
7.1.3	(U) Ensures remediation plans are effective for correcting weaknesses (Base)	Yes
7.1.4	(U) Establishes and adheres to milestone remediation dates (Base)	Yes
7.1.5	(U) Ensures resources and ownership are provided for correcting weaknesses (Base)	Yes
7.1.6	(U) 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) (Base)	Yes
7.1.7	(U) Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3; OMB M-04-25) (Base)	Yes
7.1.8	(U) Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5; OMB M-04-25) (Base)	Yes
(U) Explanation: N/A		
This chart is UNCLASSIFIED		

(U) Fiscal Year 2014 Audit of Treasury's Compliance with the Federal Information Page 19 Security Management Act for Its Intelligence Systems (OIG-14-047)

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

7: (U) PLAN OF ACTION & MILESTONES (POA&M)	Answer
(U) <i>Please select Yes or No from the pull down menu.</i>	
7.2 (U) Please provide any additional information on the effectiveness of the organization's POA&M Program that was <u>not noted</u> in the questions above.	
7.2 (U) Response: N/A	
This chart is UNCLASSIFIED	

8: (U) Remote Access Management		Answer
(U) <i>Please select Yes or No from the pull down menu.</i>		
8.1 (U) 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	(U) Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17) (Base)	Yes
8.1.2	(U) Protects against unauthorized connections or subversion of authorized connections (Base)	Yes
8.1.3	(U) Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1) (Base)	Yes
8.1.4	(U) Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1) (Base)	Yes
8.1.5	(U) If applicable, multi-factor authentication is required for remote access (NIST SP 800-46, Section 2.2, Section 3.3) (KFM)	Yes
This chart is UNCLASSIFIED		

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

8: (U) Remote Access Management		Answer
(U) <i>Please select Yes or No from the pull down menu.</i>		
8.1.6	(U) Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms (Base)	Yes
8.1.7	(U) Defines and implements encryption requirements for information transmitted across public networks (KFM)	Yes
8.1.8	(U) Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required (Base)	Yes
8.1.9	(U) Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines) (Base)	Yes
8.1.10	(U) Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4) (Base)	Yes
8.1.11	(U) Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1; NIST SP 800-53, PS-6) (Base)	Yes
(U) Explanation: N/A		
8.2 (U) Please provide any additional information on the effectiveness of the organization's Remote Access Management that was <u>not noted</u> in the questions above.		
8.2 (U) Response: N/A		
8.3 (U) Does the organization have a policy to detect and remove unauthorized (rogue) connections?		Yes
This chart is UNCLASSIFIED		

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

9: (U) Contingency Planning		Answer
(U) <i>Please select Yes or No from the pull down menu.</i>		
9.1 (U) 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	(U) 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) (Base)	Yes
9.1.2	(U) The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (NIST SP 800-34) (Base)	Yes
9.1.3	(U) Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34) (Base)	Yes
9.1.4	(U) Testing of system-specific contingency plans (Base)	Yes
9.1.5	(U) The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34) (Base)	Yes
9.1.6	(U) Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53)(Base)	Yes
9.1.7	(U) Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans (Base)	Yes
9.1.8	(U) After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34) (Base)	Yes
This chart is UNCLASSIFIED		

(U) Fiscal Year 2014 Audit of Treasury's Compliance with the Federal Information Page 22 Security Management Act for Its Intelligence Systems (OIG-14-047)

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

9: (U) Contingency Planning		Answer
(U) <i>Please select Yes or No from the pull down menu.</i>		
9.1.9	(U) Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53) (Base)	Yes
9.1.10	(U) Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53)	Yes
9.1.11	(U) Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53) (Base)	Yes
9.1.12	(U) Contingency planning that considers supply chain threats (Base)	Yes
(U) Explanation: N/A		
9.2 (U) Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was <u>not noted</u> in the questions above.		
9.2 (U) Response: N/A		
This chart is UNCLASSIFIED		

10: (U) Contractor Systems		Answer
(U) <i>Please select Yes or No from the pull down menu.</i>		
10.1	(U) Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?	Yes
This chart is UNCLASSIFIED		

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

10: (U) Contractor Systems		Answer
(U) <i>Please select Yes or No from the pull down menu.</i>		
10.1.1	(U) Documented policies and procedures for information security oversight of systems operated on the organization’s behalf by contractors or other entities, including organization systems and services residing in a public cloud (Base)	Yes
10.1.2	(U) The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines (NIST SP 800-53: CA-2) (Base)	Yes
10.1.3	(U) A complete inventory of systems operated on the organization’s behalf by contractors or other entities, including organization systems and services residing in a public cloud (Base)	Yes
10.1.4	(U) The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5) (Base)	Yes
10.1.5	(U) 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 (Base)	Yes
10.1.6	(U) The inventory of contractor systems is updated at least annually (Base)	Yes
10.1.7	(U) Systems that are owned or operated by contractors or entities, including organization systems and services residing in a public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines (Base)	Yes
(U) Explanation: N/A		
10.2 (U) Please provide any additional information on the effectiveness of the organization’s Contractor Systems Program that was <u>not noted</u> in the questions above.		
10.2 (U) Response: N/A		
This chart is UNCLASSIFIED		

Appendix 3

(U) Responses to Intelligence Community Inspector General Questions

11: Security Capital Planning		Answer
<i>Please select Yes or No from the pull down menu.</i>		
11.1 (U) Has the organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		Yes
11.1.1	(U) Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process (Base)	Yes
11.1.2	(U) Includes information security requirements as part of the capital planning and investment process (Base)	Yes
11.1.3	(U) Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53: SA-2) (Base)	Yes
11.1.4	(U) Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3) (Base)	Yes
11.1.5	(U) Ensures that information security resources are available for expenditure as planned (Base)	Yes
Explanation: N/A		
11.2 (U) Please provide any additional information on the effectiveness of the organization's Security Capital Planning Program that was <u>not noted</u> in the questions above.		
11.2 (U) Response: N/A		
This chart is UNCLASSIFIED		

Appendix 4
(U) Major Contributors to this Report

(U) Office of Information Technology (IT) Audit

(U) Tram J. Dang, Director
(U) Larissa Klimpel, Audit Manager
(U) Dan Jensen, Auditor-in-Charge
(U) Jason Beckwith, Auditor-in-Charge
(U) Don'te Kelley, IT Specialist
(U) Mitul (Mike) Patel, IT Specialist
(U) Regina Morrison, Referencer

Appendix 5
(U) Report Distribution

(U) Department of the Treasury

(U) Office of Intelligence and Analysis
(U) Office of the Chief Information Officer

(U) Intelligence Community

(U) Office of the Inspector General for the Intelligence
Community