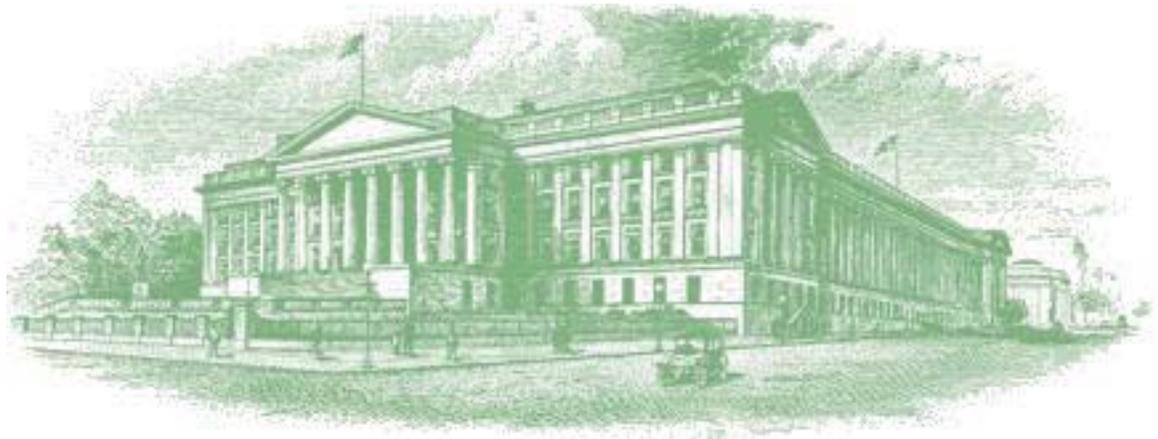




# Audit Report



OIG-12-008

INFORMATION TECHNOLOGY: The Department of the Treasury  
Federal Information Security Management Act Fiscal Year 2011  
Audit

November 10, 2011

Office of  
Inspector General  
Department of the Treasury

THIS PAGE INTENTIONALLY LEFT BLANK



DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

November 10, 2011

**MEMORANDUM FOR DAN TANGHERLINI**  
**ASSISTANT SECRETARY OF THE TREASURY FOR**  
**MANAGEMENT AND CHIEF FINANCIAL OFFICER**

**ROBYN EAST**  
**DEPUTY ASSISTANT SECRETARY FOR**  
**INFORMATION SYSTEMS AND CHIEF**  
**INFORMATION OFFICER**

**FROM:** Marla A. Freedman /s/  
Assistant Inspector General for Audit

**SUBJECT:** Audit Report – FY 2011 Audit of Treasury’s FISMA  
Implementation for Its Unclassified Systems

We are pleased to transmit the following reports:

- The Department of the Treasury Federal Information Security Management Act Fiscal Year 2010 Performance Audit, November 10, 2011 (Attachment 1)
- Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2011 (Audit No. 2011-20-116), September 20, 2011 (Attachment 2)

Attachment 1 presents the results of the performance audit of the Department of the Treasury’s (Treasury) compliance with the Federal Information Security Management Act (FISMA) for its unclassified systems. FISMA requires federal agencies, including the Department of the Treasury, to have an annual independent evaluation performed of their information security programs and practices and to report the results of the evaluations to the Office of Management and Budget (OMB). OMB has delegated its responsibility to the Department of Homeland Security (DHS) for the collection of annual FISMA responses. FISMA requires that the independent evaluation be performed by the agency Inspector General (IG) or an independent external auditor as determined by the IG. To meet our FISMA requirements, we contracted with KPMG LLP, an independent certified public accounting firm, to perform the FISMA audit of Treasury’s unclassified systems, except for those of the Internal Revenue Service (IRS), which was performed by the Treasury Inspector General for Tax Administration (TIGTA) and is presented as attachment 2. Appendix IV of attachment 1 includes our response to DHS’s FISMA

2011 Questions for Inspectors General and incorporates the responses from the TIGTA report. KPMG conducted its audit in accordance with generally accepted government auditing standards.

Based on the results reported by KPMG, TIGTA, and the financial statement audit report of the IRS conducted by the Government Accountability Office (GAO),<sup>1</sup> we determined that Treasury's information security program is in place and is generally consistent with FISMA, but could be more effective.

The KPMG audit of Treasury's unclassified systems (except for those of the IRS) identified a number of areas that could be improved. Specifically, KPMG reported that:

1. Logical account management activities were not fully documented or consistently performed at OCC, OTS, TIGTA, DO and FMS
2. Security incidents were not reported timely at the CDFI Fund, FMS, Mint, and TIGTA
3. System security plans at DO, Mint, and FMS did not fully adopt NIST recommended security controls from NIST SP 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations
4. FMS did not perform sufficient audit log reviews in accordance with NIST and Treasury standards
5. BPD did not properly inventory media scheduled for sanitization in accordance with BPD procedures
6. Plans of Action and Milestones (POA&Ms) were not tracked and remediated in accordance with NIST and Treasury requirements at FMS and OTS
7. Vulnerability scanning and remediation was not performed in accordance with Treasury requirements at the CDFI Fund, DO, OTS, and TIGTA
8. Contingency planning & testing and backup controls were not fully implemented or operating as designed at DO, FMS, TIGTA, and TTB
9. Outdated and unsupported software was utilized at OTS
10. TIGTA's risk management program was not consistent with NIST SP 800-37, Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems
11. The personnel termination procedures were not followed at FinCEN
12. The system configuration management programs were not implemented correctly at DO and TIGTA

KPMG is making 43 recommendations to the responsible officials to address the findings noted above.

---

<sup>1</sup> *FINANCIAL AUDIT: IRS's Fiscal Years 2010 and 2009 Financial Statements* (GAO-11-142, dated November 2010)

TIGTA reported that IRS was also generally consistent with FISMA requirements. However, TIGTA noted that the IRS information security program was not fully effective as a result of the conditions identified in configuration management, security training, plans of action and milestones, and identity and access management.

In addition, GAO reported a continuing material weakness in IRS's internal control over information security that resulted in IRS's inability to rely on the controls embedded in its automated financial management systems to provide reasonable assurance that (1) the financial statements are fairly stated in accordance with U.S. generally accepted accounting principles and the *GAO/PCIE Financial Audit Manual*; (2) financial information management relies on to support day-to-day decision-making is current, complete, and accurate; and (3) proprietary information processed by these automated systems is appropriately safeguarded. The new deficiencies identified during fiscal year 2010 and the unresolved deficiencies from prior audits continue to jeopardize the confidentiality, integrity, and availability of information processed by IRS's key systems, and increased the risk of material misstatement of financial reporting.

In connection with the contract with KPMG, we reviewed their report and related documentation and inquired of its representatives. Our review was differentiated from an audit performed in accordance with generally accepted auditing standards.

If you have any questions or require further information, you may contact me at (202) 927-5400 or Joel A. Grover, Deputy Assistant Inspector General for Financial Management and Information Technology Audit, at (202) 927-5768.

#### Attachments

cc: Edward A. Roback  
Associate Chief Information Officer  
Cyber Security

THIS PAGE INTENTIONALLY LEFT BLANK

## **ATTACHMENT 1**

The Department of the Treasury  
Federal Information Security Management Act  
Fiscal Year 2011 Performance Audit,  
November 10, 2011

THIS PAGE INTENTIONALLY LEFT BLANK

The Department of the Treasury  
Federal Information Security Management Act  
Fiscal Year 2011 Performance Audit

November 10, 2011



KPMG LLP  
2001 M Street, NW  
Washington, DC 20036

**The Department of the Treasury  
Federal Information Security Management Act Fiscal Year 2011 Performance Audit**

**Table of Contents**

**FISMA Performance Audit Report**

BACKGROUND .....	4
Federal Information Security Management Act (FISMA).....	4
Federal Standards and Guidelines.....	4
Treasury Bureaus/Offices (Bureaus).....	5
Treasury Information Security Management Program.....	6
OVERALL AUDIT RESULTS .....	9
FINDINGS.....	12
1. Logical account management activities were not fully documented or consistently performed at OCC, OTS, TIGTA, DO and FMS .....	12
2. Security incidents were not reported timely at the CDFI Fund, FMS, Mint, and TIGTA .....	13
3. System security plans at DO, Mint, and FMS did not fully adopt NIST recommended security controls from NIST SP 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations .....	16
4. FMS did not perform sufficient audit log reviews in accordance with NIST and Treasury standards.....	17
5. BPD did not properly inventory media scheduled for sanitization in accordance with BPD procedures .....	18
6. Plans of Action and Milestones (POA&Ms) were not tracked and remediated in accordance with NIST and Treasury requirements at FMS and OTS .....	18
7. Vulnerability scanning and remediation was not performed in accordance with Treasury requirements at the CDFI Fund, DO, and OTS.....	19
8. Contingency planning & testing and backup controls were not fully implemented or operating as designed at DO, FMS, TIGTA, and TTB .....	20
9. Outdated and unsupported software was utilized at OTS .....	22
10. TIGTA’s risk management program was not consistent with NIST SP 800-37, Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems .....	23
11. The personnel termination procedures were not followed at FinCEN.....	23
12. The system configuration management programs were not implemented correctly at DO and TIGTA.....	24
MANAGEMENT RESPONSE TO DRAFT REPORT .....	25

**Appendices**

APPENDIX I – TREASURY FISMA COMPLIANCE SUMMARY.....	41
APPENDIX II – OBJECTIVE, SCOPE & METHODOLOGY .....	43
APPENDIX III – STATUS OF PRIOR YEAR FINDINGS .....	47
APPENDIX IV – THE DEPARTMENT OF THE TREASURY’S CONSOLIDATED RESPONSE TO DHS’S FISMA 2011 QUESTIONS FOR INSPECTORS GENERAL.....	53
APPENDIX V – APPROACH TO SELECTION OF SUBSET OF SYSTEMS.....	70
APPENDIX VI – SELECTED SECURITY CONTROL CLASSES AND FAMILIES .....	72
APPENDIX VII – SUMMARY OF OTHER IT FINDINGS FROM TREASURY FINANCIAL STATEMENT AUDITS.....	77
APPENDIX VIII – LIST OF ACRONYMS .....	80



**KPMG LLP**  
2001 M Street, NW  
Washington, DC 20036

Honorable Eric Thorson  
Inspector General, Department of the Treasury  
1500 Pennsylvania Avenue, N.W.  
Room 4436  
Washington, DC 20220

**Re: The United States Department of the Treasury Federal Information Security Management Act  
Fiscal Year 2011 Performance Audit**

Dear Mr. Thorson:

This report presents the results of our independent evaluation of the U.S. Department of the Treasury's information security program and practices. The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies, including the Department of the Treasury, to have an annual independent evaluation performed of their information security programs and practices and to report the results of the evaluations to the Office of Management and Budget (OMB). OMB has delegated its responsibility to Department of Homeland Security (DHS) for the collection of annual FISMA responses. FISMA requires that the independent evaluation be performed by the agency Inspector General (IG) or an independent external auditor as determined by the IG. The Department of the Treasury Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct this independent evaluation (referred to herein as a "performance audit").

We conducted our performance audit in accordance with generally accepted government auditing standards (GAGAS) issued by the Comptroller General of the United States (U.S.). 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 the performance audit is to determine the effectiveness of the Department of the Treasury's information security program and practices for its unclassified systems, including the Department of the Treasury's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We based our work, in part, on a sample of bureau-wide security controls and system specific security controls across 15 sampled Treasury information systems. The scope of our work did not include the Internal Revenue Service (IRS), as the component was audited by the Treasury Inspector General for Tax Administration (TIGTA) or bureau wide security controls at the Office of Thrift Supervision (OTS) as it ceased operations due to the *Dodd-Frank Wall Street Reform and Consumer Protection Act* (Pub. L. No. 111-203). Additional details regarding the scope of our performance audit are included in the *Objective, Scope, and Methodology* section of this report.



Based on our audit work, we concluded that the U.S. Department of the Treasury's information security program and practices for its non-IRS bureaus' unclassified systems were generally consistent with the FISMA legislation, OMB information security requirements, and related information security standards published by the National Institute of Standards and Technology (NIST). While the information security program was generally consistent with the FISMA legislation, the program was not fully effective as reflected in the findings identified in the following areas:

1. Logical account management activities were not fully documented or consistently performed at OCC, OTS, TIGTA, DO and FMS.
2. Security incidents were not reported timely at CDFI Fund, FMS, Mint, and TIGTA.
3. System Security Plans at DO, FMS, and Mint did not fully adopt NIST-recommended security controls from NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*.
4. FMS did not perform sufficient audit log reviews in accordance with NIST and Treasury standards.
5. BPD did not properly inventory media scheduled for sanitization in accordance with BPD procedures.
6. POA&Ms were not tracked and remediated in accordance with NIST and Treasury requirements at FMS and OTS.
7. Vulnerability scanning and remediation were not performed in accordance with Treasury requirements at CDFI Fund, DO, and OTS.
8. Contingency planning & testing and backup controls were not fully implemented or operating as designed at DO, FMS, TIGTA, and TTB.
9. Outdated and unsupported software was utilized at OTS.
10. TIGTA's risk management program was not consistent with NIST SP 800-37, Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*.
11. The personnel termination procedures were not followed at FinCEN.
12. The system configuration management programs were not implemented correctly at DO and TIGTA.

We have made 43 recommendations related to these control deficiencies that, if addressed by management, will strengthen the respective bureaus, offices, and the Department's information security program. In a written response, Treasury agreed with all of our findings and recommendations and provided plans for corrective actions that are responsive to our recommendations (see *Management Response to Draft Report* on page 25). We tested controls that were implemented during the period July 1, 2010 to June 30, 2011. We caution that projecting the results of our audit to future periods is subject to the risks that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate.

Appendix I, *Treasury FISMA Compliance Summary*, summarizes the findings noted during the audit based on a sample of bureau-wide security controls (Table 1) and system specific security controls (Table 2) across 15 sampled Treasury information systems. Appendix II describes the FISMA audit's objective, scope, and methodology. Appendix III, *Status of Prior Year Findings*, summarizes the Treasury's progress in addressing prior year recommendations. Appendix IV provides *The Department of the Treasury's Consolidated Response to DHS's FISMA 2011 Questions for Inspectors General*.



Appendix V, *Approach to Selection of Subset of Systems*, describes how we selected systems for review. Appendix VI, *Selected Security Control Classes and Families*, describes the selected NIST Special Publication 800-53, Revision 3, security controls reviewed for each of the selected systems. Appendix VII summarizes IT security findings identified from the Treasury's financial statement audit at non-IRS bureaus and Appendix VIII contains a list of acronyms used in this report.

Sincerely,

**KPMG LLP**

November 10, 2011

## **BACKGROUND**

### **Federal Information Security Management Act (FISMA)**

Title III of the E-Government Act of 2002 (the Act), 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 IGs in complying with requirements of FISMA. The Act is supported by OMB, agency security policy, and risk-based standards and guidelines published by NIST related to information security practices.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of FISMA and related OMB policies and NIST procedures, standards, and guidelines. FISMA directs federal agencies to report annually to the OMB Director, Comptroller General, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. OMB has delegated some responsibility to DHS in memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, for the operational aspects of Federal cybersecurity such as establishing government-wide incident response and operating the tool to collect FISMA metrics. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG.

### **Federal Standards and Guidelines**

OMB has directed agencies to use NIST Federal Information Processing Standards (FIPS) Publication 199, *Security Categorization of Federal Information and Information Systems*, to apply a security categorization rating to an information system. This rating is assigned to an information system based on an evaluation of its confidentiality, integrity, and availability.

OMB has further directed that agencies use NIST FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, in order to apply a security controls baseline to the information system, based on the FIPS Publication 199 categorization. FIPS Publication 200 specifies the minimum security requirements for the information system and provides a risk-based process for determining the minimum security controls necessary for the information system. In addition, FIPS Publication 200 specifies 18 controls families that must be addressed when implementing security controls commensurate with the FIPS Publication 199 security categorization of the system.

NIST Special Publication (SP) 800-53 Revision (Rev.) 3 *Recommended Security Controls for Federal Information Systems and Organizations* further defines the 18 controls families outlined in FIPS Publication 200, by defining the minimum set of security controls for non-national security systems of all Federal agencies. NIST SP 800-53 Rev. 3 then divides the 18 controls families into three control classes (management, operational and technical security controls). Management controls are the safeguards or countermeasures, related to an information system, which focus on the management of risk and system security. Operational controls are the safeguards and countermeasures for an information system, but are

primarily implemented and executed by individuals (as opposed to information systems). Technical controls are also the safeguards or countermeasures for an information system, but are primarily implemented and executed by the system through mechanisms contained in the hardware, software, or firmware components of the system. Table 1 details the security control classes and families.

**Table 1: Selected Security Control Classes and Families**

Security Control Class	Security Control Family
<b>Management</b>	Planning
	Program Management
	Risk Assessment
	Security Assessment and Authorization
	System and Services Acquisition
<b>Operational</b>	Awareness and Training
	Configuration Management
	Contingency Planning
	Incident Response
	Maintenance
	Media Protection
	Personnel Security
	Physical and Environmental Protection
	System and Information Integrity
<b>Technical</b>	Access Control
	Audit and Accountability
	Identification and Authentication
	System and Communications Protection

Source: NIST SP 800-53 Rev. 3

**Treasury Bureaus/Offices (Bureaus)**

Treasury consists of 14 operating bureaus and offices, including:

1. **Alcohol and Tobacco Tax and Trade Bureau (TTB)** – Responsible for enforcing and administering laws covering the production, use, and distribution of alcohol and tobacco products. TTB also collects excise taxes for firearms and ammunition.
2. **Bureau of Engraving and Printing (BEP)** – Designs and manufactures U.S. currency (paper), securities, and other official certificates and awards.
3. **Bureau of the Public Debt (BPD)** – Borrows the money needed to operate the Federal government. It administers the public debt by issuing and servicing U.S. Treasury marketable, savings, and special securities.
4. **Community Development Financial Institution (CDFI) Fund** – Created to expand the availability of credit, investment capital, and financial services in distressed urban and rural communities.
5. **Departmental Offices (DO)** – Primarily responsible for policy formulation. The DO, while not a formal bureau, is composed of divisions headed by Assistant Secretaries, some of whom report to

Under Secretaries. These offices include domestic finance, economic policy, General Council, International Affairs, Legislative Affairs, Management, Public Affairs, Tax Policy, and Terrorism and Finance Intelligence. The Office of Cybersecurity, within the Office of Management, is responsible for the development of IT Security Policy.

6. **Financial Crimes Enforcement Network (FinCEN)** – Supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes. It also provides U.S. policy makers with strategic analyses of domestic and worldwide trends and patterns.
7. **Financial Management Service (FMS)** – Receives and disburses all public monies, maintains government accounts, and prepares daily and monthly reports on the status of government finances.
8. **Internal Revenue Service (IRS)** – Responsible for determining, assessing, and collecting internal revenue in the U.S.
9. **Office of the Comptroller of the Currency (OCC)** – Charters, regulates, and supervises national banks and thrift institutions to ensure a safe, sound, and competitive banking system that supports the citizens, communities, and economy of the United States.
10. **Office of the Inspector General (OIG)** – Conducts and supervises audits and investigations of Treasury programs and operations. The OIG also keeps the Secretary and the Congress fully and currently informed about problems, abuses, and deficiencies in Treasury programs and operations.
11. **Office of Thrift Supervision (OTS)** – The primary regulator of all Federal and many state-chartered thrift institutions, which include savings banks and savings and loan associations. OTS was consolidated into OCC and, as a result of the **Dodd–Frank Wall Street Reform and Consumer Protection Act**, ceased to exist as of July 21, 2011.
12. **United States Mint (Mint)** – Designs and manufactures domestic, bullion, and foreign coins as well as commemorative medals and other numismatic items. The Mint also distributes U.S. coins to the Federal Reserve banks as well as maintains physical custody and protection of our nation’s silver and gold assets.
13. **Special Inspector General for the Troubled Asset Relief Program (SIGTARP)** – Has the responsibility to conduct, supervise and coordinate audits and investigations of the purchase, management, and sale of assets under the Troubled Asset Relief Program (TARP). SIGTARP’s goal is to promote economic stability by assiduously protecting the interests of those who fund the TARP programs (i.e., the American taxpayers).
14. **Treasury Inspector General for Tax Administration (TIGTA)** – Conducts and supervises audits and investigations of IRS programs and operations. The TIGTA also keeps the Secretary and the Congress fully and currently informed about problems, abuses, and deficiencies in IRS programs and operations.

The scope of KPMG’s 2011 FISMA audit did not include the IRS.

## **Treasury Information Security Management Program**

### Treasury Office of the Chief Information Officer (OCIO)

The Treasury Chief Information Officer (CIO) is responsible for providing Treasury-wide leadership and direction for all areas of information and technology management, as well as the oversight of a number of 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 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 and Program Performance Measurement** – Manages and coordinates the Departmental cyber security policy for sensitive (unclassified) systems throughout the Department, 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 Department-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 Department and meet our oversight responsibilities.
4. **Enterprise-wide Security** – Works with the Bureaus’ and Treasury’s Government Security Operations Center to deploy new Department-wide capabilities or integrate those already in place, as appropriate, to strengthen the overall protection of the Department. Examples include implementation of Domain Name Service Security Extensions (DNSSEC), an automated asset inventory, and Department-wide security-related audit findings. Includes addressing the Department’s strategies and plans to mitigate cyber security risks from configuration and other vulnerabilities.
5. **Understanding Security Risks and Opportunities from New Technologies** – New information and security technologies present both 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 the Department’s advantage. Vulnerability Analysis, Configuration and Planning: analyzes current and emerging technologies and Cyber Critical Infrastructure Protection. Implements cyber-related requirements of Homeland Security Presidential Directive No. 7, “Critical Infrastructure Identification, Prioritization, and Protection,” focusing on the protection of Department-owned cyber assets.
6. **Treasury Computer Security Incident Response Capability (TCSIRC)** – Provides incident reporting with external reporting entities and conducts performance monitoring and analyses of CSIRCs within the Department.
7. **National Security Systems** – Manages and coordinates the Department-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 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. The ACIOCS and the Cyber Security Program have established Treasury Directive Publication (TD P) 85-01, *Treasury Information Technology Security Program*, as the Treasury-wide 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 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 Treasury. The ACIOCS and the Cyber Security Program are also responsible for promoting and coordinating a Treasury-wide 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 information technology assets.

Bureau Chief Information Officers (CIOs)

Organizationally, the Treasury has established bureau-level and office Chief Information Officers (CIOs). The CIOs are responsible for managing the IT security program for their 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 Treasury OCIO 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.

Treasury – Bureau OCIO Collaboration

The Treasury OCIO has established the Treasury 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-wide 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, bureau CIO organizations, as well as the OIG – Office of IT Audits and TIGTA – Office of Audits.

## **OVERALL AUDIT RESULTS**

We concluded that the Department's information security program and practices for its non-IRS bureaus' unclassified systems were generally consistent<sup>1</sup> with the FISMA legislation and related information security policies, standards, and guidelines. However, they were not fully effective resulting in the identification of 12 categories of control weaknesses and 43 recommendations that the bureaus, offices, and the Treasury Department should address to strengthen their information security management programs. The *Findings* section of this report presents the detailed findings and associated recommendations.

Additionally, we evaluated all prior year findings from the fiscal year (FY) 2010 FISMA Evaluation and determined that the bureaus implemented all recommendations, with the exception of FMS Prior Year Finding #3 for POA&Ms, which FMS partially addressed. We reissued this exception as FY 2011 FMS Finding #6. See Appendix II, *Status of Prior Year Findings*, for additional details.

Summaries of the 12 categories of control weaknesses follow:

**1. Logical account management activities were not fully documented or consistently performed at OCC, OTS, TIGTA, DO and FMS**

We noted that account management activities were not fully documented at OCC, OTS, and TIGTA. Additionally, we noted account management activities were not consistently performed at DO and FMS. By not defining access control policies and procedures, there is an increased risk that potentially unauthorized access could occur within the IT infrastructure.

**2. Security incidents were not reported timely at the CDFI Fund, FMS, Mint, and TIGTA**

We identified an inconsistent implementation of incident reporting security controls at four Treasury bureaus. These bureaus had reported security incidents after the reporting deadlines lapsed. By not reporting security incidents in a timely manner, these bureaus increased the risk posed to their information systems while the incidents were unreported.

**3. System security plans at DO, Mint, and FMS did not fully adopt NIST recommended security controls from NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations***

We noted three Treasury bureaus' information systems relied on security plans that were not compliant with NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*. NIST SP 800-53, Rev 3, was issued in August 2009 and agencies were required to implement this guidance one year after issuance. Accordingly, these systems' security plans utilized outdated security policies from NIST SP 800-53 Rev 2 to protect their information and assets. Failing to select the proper baseline of security controls has a negative effect on subsequent security activities in the NIST Risk Management Framework. Therefore, system security controls may not appropriately or sufficiently protect the confidentiality, integrity, and availability of sensitive bureau information.

---

<sup>1</sup> TIGTA will provide a separate report evaluating the IRS's implementation of the U.S. Treasury's information security program.

**4. FMS did not perform sufficient audit log reviews in accordance with NIST and Treasury standards**

FMS did not document their review of their audit logs and actions taken in response to unusual log events or suspicious transactions during the audit period for one sampled information system. While FMS took actions previously to address a similar issue identified from the prior year financial statement audit, the limited scope of FMS's corrective actions did not include a risk analysis necessary to identify significant audit events worthy of review and subsequent investigations, as required by NIST SP 800-53 security control AU-2 *Auditable Events*.

By not identifying additional significant audit events to monitor, system owners could be unable to identify and mitigate all significant threats to the information system. This could cause FMS personnel to remain unaware of security incidents that have already taken place, leaving the system in a compromised state for an extended period of time.

**5. BPD did not properly inventory media scheduled for sanitization in accordance with BPD procedures**

BPD did not follow all aspects of its bureau media sanitization policies. BPD's media sanitization process did not ensure a clear chain of custody and full accounting of hard drives, backup tapes, and other digital media throughout the entire media sanitization process. By not appropriately securing the IT hardware that are intended to be degaussed, or reconciling all such IT hardware against known inventory listings, it is impossible to determine the accuracy and completeness of the sanitization and destruction process for hardware and media.

**6. POA&Ms were not tracked and remediated in accordance with NIST and Treasury requirements at FMS (Repeat Finding) and OTS**

FMS did not record and update security vulnerabilities in a timely manner for three sampled systems. For the sampled systems, we noted that FMS did not review and revise expected completion dates for corrective actions, record known high-risk vulnerabilities that could not be closed in 60 days, or correctly report the completion status on outstanding POA&M items. This has been an on-going issue at FMS, with similar findings reported in the FY 2009 and 2010 FISMA Audits.

OTS employees were aware of a high-risk security vulnerability in one of the sampled information systems for over 30 days and did not record a correction action plan for it in their POA&M.

By not timely recording and updating identified security vulnerabilities in their respective systems, bureau and Treasury management would not be able to exercise their oversight responsibilities to modify funding levels, human resources, and requested priorities in response to identified security weaknesses.

**7. Vulnerability scanning and remediation were not performed in accordance with Treasury requirements at the CDFI Fund, DO, and OTS**

We noted during the audit that three Treasury bureaus did not conduct monthly vulnerability scans required by their IT security policy. Without knowledge of missing security patches, insecure configurations, or application vulnerabilities, Treasury bureaus could not take steps to mitigate potential vulnerabilities in their information systems.

**8. Contingency planning & testing and backup controls were not fully implemented or operating as designed at DO, FMS, TIGTA, and TTB**

We noted during the audit that four Treasury bureaus did not fully implement NIST Contingency Planning (planning, testing, and backup) controls as required by NIST and Treasury guidance. A lack of frequent, successful backups can have a significant negative effect on Treasury information systems if a disaster (i.e., hard-drive failure, natural disaster, national emergency, etc.) were to occur. Data that has not been stored off-site on tape or other media can be lost if a disaster were to occur. Additionally, disaster failover tests are paramount in assuring that in emergencies, the critical infrastructure protection (CIP) systems can remain operational with the least amount of down time possible. Failure to appropriately test Contingency Plans could result in the unavailability of critical Treasury information and information systems.

**9. Outdated and unsupported software was utilized at OTS**

We noted that OTS utilized an unsupported and out-dated server operating system that was no longer NIST-approved. By not maintaining vendor-supported operating system software, information system availability, confidentiality, and integrity could be compromised.

**10. TIGTA's risk management program was not consistent with NIST SP 800-37, Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems***

TIGTA had not updated their risk assessment program to comply with NIST 800-37 Rev 1 at the time of the 2011 FISMA audit. As NIST SP 800-37, Rev 1, was issued in February 2010, OMB requires federal agencies to adopt this NIST guidance within one year of issuance. An insufficient risk management program can lead to ineffective risk-based decision-making and untimely implementation of system-level controls.

**11. The personnel termination procedures were not followed at FinCEN**

FinCEN was unable to provide completed personnel separation forms for 18 of 25 separated employees and contractors as evidence that it completed its exit clearance procedures. Without separation forms as evidence that FinCEN supervisors and others completed the separation process, FinCEN could not demonstrate that it consistently executed its separation procedures and collected all government issued property.

**12. The system configuration management programs were not implemented correctly at DO and TIGTA**

We noted during the course of the audit evaluation that DO and TIGTA lacked appropriately defined and implemented system Configuration Management programs as required by Treasury's TD P 85-01, *Treasury Information Technology Security Program*. By not adequately implementing their systems' Configuration Management programs, Treasury bureaus reduce their

ability to track and maintain version control, protect against harmful or subversive code implementation, and recover from a disaster or service interruption.

## **FINDINGS**

### **1. Logical account management activities were not fully documented or consistently performed at OCC, OTS, TIGTA, DO and FMS**

KPMG identified an inconsistent implementation of logical access controls at five bureaus including the OCC, OTS, TIGTA, DO, and FMS. KPMG noted the following:

1. Account Management activities were not fully documented as required by Treasury Directive Publication (TD P) 85-01, *Treasury Information Technology Security Program*, and bureau-specific policies at OCC, OTS, and TIGTA.
  - OCC did not have documented approvals to grant all new bank examiners access to a certain business application. OCC network administrators explained that a former OCC official gave verbal approval for all new bank examiners to access this business application an unknown-number of years ago. Thus, sampled new users for the OCC system lacked evidence of management approval for the level of access granted to the system. (*See Recommendation #1*)
  - OTS management did not establish a process to review system administrators and application service accounts for continued appropriateness for a sampled OTS application. Additionally, OTS did not document in the SSP or other application configuration document the required application service accounts for the application to function properly, thus limiting OTS' ability to identify unnecessary service accounts. (*See Recommendations # 2 and 3*)
  - TIGTA did not fully document account management activities (e.g., review frequency, inactivity limits, use of shared accounts) in their SSPs. TIGTA management was unaware of the lack of documentation until a 2010 security assessment was conducted. In response to the security assessment, TIGTA established four corrective actions in the system's POA&Ms with scheduled completion dates of October 2011, April 2012, July 2012, and December 2012. These security weaknesses continued to exist at the time of KPMG's FY 2011 FISMA audit.
2. Account Management activities were not consistently performed as required by TD P 85-01, *Treasury Information Technology Security Program*, and bureau-specific policies at DO and FMS.
  - For a sampled DO system, new users were granted access without formal authorization, and DO did not review existing users' access for appropriateness concerning user privileges. DO officials did not have an effective process for authorizing new users and were unaware that a periodic review of user access for continued appropriateness was required. (*See Recommendations #4 and 5*)
  - For a sampled FMS payment management system, 12 user accounts out of 2950 inappropriately remained active following 90 days of inactivity. Additionally, 920 user accounts out of 2950 did not have a last login date recorded, suggesting these accounts may never have been used by the account owner. KPMG noted a similar finding in a FY 2010 financial statement audit for the sampled system, but FMS's corrective actions to implement a fully automated solution to disable inactive accounts were not fully effective. FMS attributed the noted conditions to human error during the transition to an automated solution. Prior to and after the transition to a fully automated solution, FMS did not monitor if the automated solution was working as intended. (*See Recommendations #6 and 7*)

These control deficiencies all demonstrate that these bureaus did not appropriately develop written policies and procedures, or did not implement defined policies for reviewing user access, and disabling or deleting unnecessary user or system administrator access. By not defining access management policies and procedures, there is an increased risk that IT staff could improperly implement identity and access controls. By not implementing a periodic review of all user and administrator accounts for inactivity and disabling inactive accounts according to policy, there is an increased risk that users could gain or retain unauthorized access and/or perform unauthorized transactions on their respective systems.

We recommend that OCC management:

1. Document the process for granting access to the newly hired bank examiners, including the associated user roles and required management approvals.

We recommend that OCC, in its capacity managing prior OTS systems:

2. Add the review of system administrator and application service accounts for the sampled system to the review of external user accounts.
3. Document the purpose and use of application service accounts in the SSP or other publication.

Based on TIGTA's planned corrective actions, we are not making a recommendation.

We recommend that DO management:

4. Perform an annual review of end user accounts that addresses appropriateness of user access rights. As stated in the DO SSP, the Information System Security Officers (ISSOs) and/or the system administrators of each minor application should perform this review.
5. Develop and implement a formal account approval process. A formal approval form should exist for all system users, including contractors. These forms should be properly tracked and stored to ensure that documentation is not lost or deleted.

We recommend that FMS management:

6. Continue to monitor the automated solution to disable user accounts after 90 days of inactivity in order to confirm the automated solution is working in all cases.
7. Perform a manual monthly review of all user accounts, and disable or delete (as appropriate) accounts that have not logged into the system within the prior 90 days until the manual, monthly review demonstrates that the automated solution is working for three consecutive months.

## **2. Security incidents were not reported timely at the CDFI Fund, FMS, Mint, and TIGTA**

Treasury bureaus are required to submit all security incidents to the Treasury Computer Security Incident Response Center (TCSIRC) within specified time frames categorized by incident severity. The audit identified an inconsistent implementation of incident reporting security controls at four bureaus including the CDFI Fund, FMS, Mint, and TIGTA. KPMG noted that all four bureaus

reported security incidents later than the deadlines required by TD P 85-01, *Treasury Information Technology Security Program*. Specifically, KPMG noted that:

- The CDFI Fund did not report its single security incident to TCSIRC within the required one-hour time period for a Category 1 incident. Several factors contributed to the late reporting. First, the incident occurred outside of normal working hours. Second, the incident was reported in a monthly report, 36 days late. The delay in reporting was caused by CDFI Fund's officials incorrectly categorizing the incident. A CDFI Fund official also attributed the untimely reporting to the infrequent nature of security incidents and the staff's unfamiliarity with required reporting time frames for Category 1 incidents. (See Recommendations # 8, 9, and 10)
- FMS employees did not immediately report 10 of 10 confirmed security incidents to FMS's help desk as required by FMS policy. Additionally, FMS's information security group did not report seven of these confirmed security incidents to TCSIRC within the required one-hour time period for Category 1 incidents (three security incidents were reported in one day, two were reported in two days, and the remaining three were reported in three days). Rather than report all suspected and confirmed incidents, FMS failed to notify TCSIRC until sufficient evidence was gathered and approved by FMS Executives as required by FMS policies and procedures. Contributing to the untimely reporting was a lack of after-hours coverage by the incident response personnel. Additionally, KPMG attributes the untimely reporting by FMS employees to a lack of sufficient awareness and training. (See Recommendations # 11, 12, 13, and 14)
- Mint did not report one of the 15 sampled security incidents to TCSIRC within the required one-hour time period for a Category 1 incident (the incident took 25 hours to report). The delay in reporting was caused by the assigning of a ticket to a Mint Computer Security Incident Response Capability (CSIRC) employee who was not in the office when the incident was reported. When the Mint CSIRC employee returned to work, the required time frame to report the security incident had passed. (See Recommendations # 15 and 16)
- TIGTA did not report one of the 15 security incidents to TCSIRC within the required one day time period for a Category 3 incident (the incident took five days to report). The untimely reporting of the security incident was caused by reduced staffing over a holiday period. Upon return, the employee failed to take action within the required reporting time frame for Category 3 incidents. (See Recommendations # 17, 18, and 19)

By not reporting security incidents in a timely manner, these bureaus increase the risk posed to their information system's availability, integrity, and confidentiality, while the incident is unreported. Additionally, by not reporting incidents, the bureaus can impair Treasury and United States Computer Emergency Readiness Team (US-CERT)'s ability to track, analyze, and act on aggregated incident data.

We recommend that the CDFI Fund Management:

8. Provide additional incident response training to increase awareness of the CDFI Fund's policies and procedures.
9. Remind all CDFI Fund staff of their responsibility to timely report security incidents, including events such as the loss of mobile devices with one hour, to the CDFI Fund's IT team. Such reminders could be incorporated into employee's annual security awareness training or be included in periodic reminders to employees to protect sensitive information and report the loss of mobile devices to the CDFI Fund's IT team.

10. Provide the CDFI Fund employees the capability to report security incidents to the IT team outside of normal working hours by establishing a shared incident response e-mail account and / or phone number for reporting purposes.

We recommend that FMS Management:

11. Revise the current incident reporting process and associated written procedures to ensure timely reporting. This could include the FMS incident response management notifying TCSIRC with suspected or confirmed security events without the need for further FMS Executive management approvals.
12. Provide additional training to FMS security personnel regarding FMS's revised incident response policies and procedures to ensure these policies and procedures are consistently implemented.
13. Consider, if feasible, a Distributed Incident Response Team or a Partially Outsourced Team to achieve 24x7x365 coverage, per the NIST SP 800-61, *Computer Security Incident Handling Guide*. Such a strategy could involve sharing TSIRC resources with other Treasury bureaus.
14. Improve FMS employee awareness to report both confirmed and suspected security incidents to the FMS Service Desk. FMS could create awareness through periodic reminders via e-mail, posting security posters in common employee areas, and through increased emphasis in annual security and awareness training.

We recommend that Mint Management:

15. Have all tickets sent to the CSIRC group mailbox as opposed to individual members to ensure that tickets are tracked properly.
16. Ensure a backup CSIRC member in place during the absence and/or unavailability of the primary individual. The backup CSIRC member should be notified if the primary individual has not acknowledged the ticket within a designated time period.

We recommend that TIGTA Management:

17. Assign an additional individual as a back-up resource to the TIGTA CSIRC for periods of reduced staffing.
18. Provide the TIGTA CSIRC the ability to receive and address security incidents outside of normal working hours by establishing a shared incident response e-mail account and / or phone number for reporting purposes. Additionally, consider participating in a shared Incident Response team with another Treasury bureau to provide increased capabilities outside of normal working hours.
19. Provide the TIGTA CSIRC additional incident response training to ensure they are aware of TIGTA's policies and procedures, including their responsibility to timely report security incidents.

**3. System security plans at DO, Mint, and FMS did not fully adopt NIST recommended security controls from NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations***

NIST and Treasury guidance require that Treasury SSPs remain up-to-date and current with the NIST Risk Management Framework and required NIST SP 800-53 security controls. KPMG noted that three sampled information systems from DO, Mint, and FMS utilized outdated NIST guidance (Rev. 2). Specifically, the SSPs did not include all required security controls as specified in NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, dated August 2009. OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, attachment *FY 2010 Frequently Asked Questions on Reporting for FISMA* states that “for legacy information systems, agencies are expected to be in compliance with NIST standards and guidelines within one year of the publication date unless otherwise directed by OMB.”

KPMG noted that the conditions, cited above for DO and Mint, had various factors including:

1. The bureau and vendor’s misunderstanding of contract requirements to maintain compliance with all NIST standards (DO), (*See Recommendation # 20*)
2. Mint management had a informal policy to only update SSPs during reaccreditation, therefore the sampled SSPs had not be updated since the next reaccreditation cycle had not begun. (*See Recommendations # 21 and 22*)

During the audit period, FMS revised their SSP template and associated checklist to incorporate NIST SP 800-53, Rev. 3 controls. However, the sampled system’s SSP utilized older Rev 2 controls and FMS’s quality control process did not reject this sampled SSP. (*See Recommendation # 23*)

Failing to select an up-to-date baseline of security controls may have a negative effect on subsequent security activities as required by the NIST Risk Management Framework. Specifically, DO, FMS, and Mint may not be able to properly implement, assess, authorize, and monitor the security controls for the sampled systems; therefore, the system security controls may not be sufficient to protect the confidentiality, integrity, and availability of sensitive bureau information.

We recommend that DO management:

20. Instruct the vendor to update the SSPs to include NIST SP 800-53, Rev. 3 security controls and associated control enhancements.

We recommend that Mint management:

21. Update their Information Security Program’s policies and procedures to require that all SSPs are updated to include the latest NIST SP 800-53 controls and control enhancements one year after issued.
22. Ensure that all existing SSPs are 800-53, Revision 3 compliant.

We recommend that FMS management:

23. Ensure that System Owners and ISSOs review and update SSPs by using the FMS-approved SSP template and baseline security requirements, which incorporate NIST SP 800-53, Rev. 3 security controls.

#### **4. FMS did not perform sufficient audit log reviews in accordance with NIST and Treasury standards**

NIST and Treasury guidance, specifically SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, and TD P 85-01, *Treasury Information Technology Security Program*, require that government information systems owners and security managers identify significant auditable events in order to protect the confidentiality, integrity, and availability of the information system. These audit logs need to be generated and reviewed by IT personnel on a regular basis if security incidents are to be discovered and acted upon in a timely manner and should be appropriately stored for security and historical purposes.

For a sampled application, FMS did not document their weekly review of failed login events during the FISMA audit period. While FMS took actions to address a similar issue in a prior year financial statement audit by developing audit log review procedures for failed login attempts, the limited scope of FMS's corrective actions did not include a risk analysis necessary to identify significant audit events worthy of review and subsequent investigations, as suggested by NIST SP 800-53 security control AU-2 *Auditable Events*. The audit log review and SSP did not address broader user account activities such as the creation of new accounts with administrative capabilities or changes in user account permissions. In addition, the proposed audit log review procedures did not include monitoring changes to specific information system components such as the database, sensitive files, or production source code. Finally, the implemented audit log procedures did not address potentially suspicious or unusual transactions that could be performed in the sampled payment management system.

Several factors contributed to the condition described above. These factors included other operational priorities and responsibilities for the application's security officer, delays implementing documented manual procedures for the audit log review, and lack of an automated tool to view log events at the third party hosting provider. By not adhering to the FMS required audit log review policies, the system owner could be unable to identify and mitigate significant threats to the information system. As FMS did not perform a risk assessment to determine the most significant audit events to review and investigate for the sampled system, FMS may be focusing its limited resources monitoring less significant audit log events. This could cause FMS personnel to remain unaware of security incidents that have already taken place, leaving the system in a compromised state for an extended period of time.

We recommend that FMS management:

24. Identify and document significant audit events that warrant review and further investigation.
25. Update the SSP in order to reflect the results of the risk analysis and clearly assign ownership and responsibility for implementing the agreed upon audit log review procedures.
26. Ensure that sufficient resources are available to implement audit log review procedures.

**5. BPD did not properly inventory media scheduled for sanitization in accordance with BPD procedures**

The physical IT hardware and digital media (i.e., hard drives, backup tapes, and CD / DVDs) that store BPD information must be protected against unauthorized access and disclosure. When IT hardware or other media is to be disposed, NIST SP 800-53 Rev. 3, NIST SP 800-88 Rev. 1, *Guidelines for Media Sanitization*, and TD P 85-01, *Treasury Information Technology Security Program* media sanitization guidance require bureaus to carefully track and appropriately secure the IT hardware and media to prevent accidental disclosure of sensitive information. BPD developed Baseline Security Requirements (BLSR) and procedures that incorporated NIST guidance and Treasury requirements. However, BPD's media sanitization process did not ensure a clear chain of custody and full accounting of the media throughout the entire media sanitization process. Additionally, we observed four unsecured cardboard boxes, containing over 150 hard drives waiting to be sanitized, adjacent to the cubicle of the IT specialist responsible for media sanitization. These boxes of hard drives were not stored in a secured container or secured room that restricted access to only individuals involved in the media sanitization process.

Several factors contributed to the condition described above. These included individuals unclear on certain BPD security requirements and BPD management's perception that existing practices for storing and then sanitizing media were sufficient. By not appropriately securing the media waiting sanitization, or reconciling all such media against known inventory listings, BPD's records of sanitized media may be inaccurate and incomplete. Without a clear chain of control throughout the media sanitization process that includes inventorying media, it is impossible to determine if access to sensitive media was limited to authorized individuals and all media was appropriately sanitized.

We recommend that BPD management:

27. Implement its BLSRs and associated procedures on maintaining a clear chain of custody, properly securing media when stored, and reconciliation of media received and sent for destruction.
28. Train BPD IT specialists on the BPD media sanitization policies and procedures in order to protect the confidentiality of the bureau's sensitive information.

**6. Plans of Action and Milestones (POA&Ms) were not tracked and remediated in accordance with NIST and Treasury requirements at FMS and OTS**

Treasury has provided guidance on POA&M creation and tracking through its directive TD P 85-01, *Treasury Information Technology Security Program*. This policy requires Treasury bureaus to maintain these POA&Ms in order to help remediate weaknesses identified through audits, security assessments, and other risk management activities. POA&Ms document the responsible parties, time frames for mitigation, and additional necessary resources.

FMS did not record and update security vulnerabilities in a timely manner for three sampled systems. For the sampled systems, we noted that FMS did not review and revise expected completion dates for corrective actions, record known high-risk vulnerabilities that FMS could not close in 60 days, or correctly report the completion status on outstanding POA&M items. In both the FY 2009 and FY 2010 FISMA audits at FMS, we noted similar POA&M weaknesses for different information systems. FMS took corrective actions to resolve the immediate instances of noncompliance; however, FMS did not resolve bureau wide challenges to accurately and sufficiently report all system security

weaknesses in POA&Ms. A lack of System Owner and ISSO accountability, as indicated in their Appointment Letter, and communication issues between ISSO and FMS's information security group contributed to the conditions described above. (See Recommendations # 29, 30, 31 and 32)

At OTS, we observed that OTS system administrators were aware of a high-risk security vulnerability in one of the sampled information systems for over a 30-day period and did not record this weakness in the system's POA&M. Regarding the untimely update of the POA&M at OTS, management indicated that other operational priorities, associated with the transition of bank supervisory responsibilities to the Office of the Comptroller of the Currency, were a higher priority.

By not recording identified information security weaknesses in POA&Ms, these weaknesses may be forgotten and subsequently exploited by an attacker. Additionally, by not timely recording and updating identified system security vulnerabilities in their POA&M, Treasury bureaus' summary-level security metrics under-report the true number of known security weaknesses to the Department of Treasury. Additionally, senior Treasury management would not be able to exercise its oversight responsibilities to potentially adjust funding levels, human resources, and requested priorities in response to identified security weaknesses.

We recommend that FMS management:

29. Perform a comprehensive study of FMS's POA&M management practices to resolve ongoing auditor-identified POA&M challenges. Based on the outcome of this study, FMS should implement corrective actions designed to ensure complete, accurate and timely reporting of POA&M items.
30. Strengthen FMS's existing policies and procedures regarding POA&Ms based on the outcome of FMS's study. The revised FMS policies and procedures should define roles, responsibilities, and expected communication frequency among key participants and decision makers.
31. Promote increased involvement by FMS executives and Authorizing Officials in the POA&M management process. Such actions could include establishing performance metrics and associated incentives and/or disincentives for FMS management personnel to accurately report and resolve noted security weaknesses in their portfolio of information systems.
32. Promote personal accountability for executing information security responsibilities, such as those listed in the ISSO and System Owner Appointment Letters, by incorporating those responsibilities and expected outcomes in the employees' Annual Performance Plan.

We have no recommendation for OTS management to improve the POA&M process as OTS ceased operations on July 21, 2011 due to the *Dodd-Frank Wall Street Reform and Consumer Protection Act*.

## **7. Vulnerability scanning and remediation was not performed in accordance with Treasury requirements at the CDFI Fund, DO, and OTS**

Treasury's directive TD P 85-01, *Treasury Information Technology Security Program*, and NIST SP 800-53, Rev. 3 require that bureaus conduct vulnerability scanning of their IT assets at least monthly. Additionally, high-risk weaknesses identified in this manner are required to be remediated in a timely manner, or, if this is not possible, tracked in a POA&M until the remediation actions are complete. KPMG noted that three bureaus did not implement Treasury policy adequately.

- The CDFI Fund did not ensure that its service provider, TTB, conducted monthly vulnerability scans of its Web server as required by Treasury and the CDFI Fund's IT security policy. Although the CDFI Fund outsourced the hosting of its infrastructure to TTB, the CDFI Fund did not require TTB to conduct monthly vulnerability scans of the CDFI Fund Web server in their Interconnection Security Agreement. (*See Recommendations # 33 and 34*)
- A DO system's vulnerability scan report from October 2010 contained multiple high-risk vulnerabilities that were not remediated 30 days after discovery as required by DO's Information Technology Security policy. For the sampled information system, DO's vendor deemed certain devices to not be essential to the successful operation of the information system, and therefore did not patch those devices. (*See Recommendation # 35*)
- OTS did not consistently scan its application servers on a monthly basis as required by NIST and Treasury requirements and OTS Continuous Monitoring procedures. OTS personnel verbally outlined to KPMG a risk-based set of scanning frequencies that was not documented and not verifiable at the system level. Further, KPMG noted that OTS management was aware of these flaws and indicated to KPMG that it lacked the resources to scan more frequently.

Without knowledge of missing security patches, insecure configurations, or application vulnerabilities, Treasury bureaus may not take steps to mitigate potential vulnerabilities in their information systems. These vulnerabilities could lead to their systems and/or applications being compromised and sensitive information being released or altered.

We recommend that the CDFI Fund management:

33. Revise the Interconnection Security Agreement with TTB to define clear roles and responsibilities for providing services and implementing associated security controls such as vulnerability scanning.
34. Enhance the continuous monitoring strategy for outsourced information systems to ensure that NIST and Treasury required security controls are implemented and operating effectively. As part of the strategy, share the results with appropriate CDFI Fund System Owners and IT management.

We recommend that DO management:

35. Direct personnel charged with remediating vulnerabilities to track open, unresolved vulnerabilities in system POA&Ms when the anticipated remediation will exceed 30 days.

We are not making a recommendation to OTS Management as this finding relates to process gaps in the OTS vulnerability scanning procedures and OTS ceased operations on July 21, 2011 due to the *Dodd-Frank Wall Street Reform and Consumer Protection Act*.

## **8. Contingency planning & testing and backup controls were not fully implemented or operating as designed at DO, FMS, TIGTA, and TTB**

Treasury guidance requires its bureaus to protect their information systems in the event of a disaster. Bureaus must plan for system recovery, test these plans, and store redundant data to assist in such a system recovery. Several Treasury bureaus did not fully implement contingency planning (planning, testing, and backup) controls as required by Treasury's directive TD P 85-01, *Treasury Information Technology Security Program*, and NIST SP 800-53, Rev. 3 guidance. While these controls do not

affect normal, daily operations, they are invaluable in quickly recovering from a disaster or service interruption.

- Daily incremental and weekly fully backups of DO data to tape for one sampled DO system was not performed by DO Operations as defined by the DO SSP and the *DO Information Technology Security Handbook*. Both the DO SSP and *DO Information Technology Security Handbook* require incremental daily backups and full weekly backups. DO Operations only performed successful incremental backups to tapes three to four times a month beginning in January 2011. The infrequency of backups was due to an insufficient backup system, whose server had to be continually restarted (i.e., rebooted). Prior to January 2011, DO did not retain the data or records from backups. This was due to a lack of sufficient storage on tapes. Additionally, backups were not tested to determine if they were reliable and complete. Finally, for another sampled DO system, DO lacked a backup process for configuration files residing in firewalls, intrusion prevention systems and Transport Support Devices (e.g., routers, switches, etc.). KPMG observed that DO management was unaware of this issue. Once informed of this significant security weakness, DO management created a POA&M item to track the issue to closure. (See *Recommendations # 36, 37, 38 and 39*)
- FMS did not complete a failover, and contingency plan test for two Critical Infrastructure Protection (CIP) payment management systems residing at FMS in accordance with FMS security standards and *NIST SP 800-53 Rev 3 requirements*. During the nine-month period from October 1, 2010 through June 30, 2011, these two CIP systems processed 911 million payments totaling \$1.93 trillion dollars. These two systems process approximately all Social Security Administration payments, Medicare and Medicaid payments, IRS tax refunds, Veteran Affairs payments, and other US government vendor payments. However, these two systems had only undergone a tabletop disaster recovery test during the Fiscal Year 2010 and 2011 and had not completed a full disaster recovery test at the recovery site in the prior two years. Per FMS and NIST SP 800-34 requirements, disaster recovery simulation exercises, such as tabletop exercises, are sufficient for “Moderate” systems but not “High” impact systems. FMS categorized these CIP systems as having a “High” FIPS 199 impact rating with a two-hour recovery time objective. This designation requires FMS to perform a failover, recovery and reconstitution (including communications with applications and third-parties) of critical systems at an alternate site on an annual basis. FMS delayed failover contingency plan tests in FY 2011 and FY2010 due to operational priorities to relocate and consolidate data centers. (See *Recommendations # 40*)
- The selected TIGTA system lacked sufficient documentation regarding the system’s contingency plan and contingency plan testing. Specifically, the documentation did not include certain key software used. TIGTA management identified these weaknesses during a 2010 security assessment and established two POA&M items with scheduled completion dates of January 2012 and June 2012.
- Backups were not consistently successful or completed on a scheduled basis at TTB. For the sampled TTB system, 69 (42 percent) of the 164 sampled scheduled jobs were unsuccessful. Additionally, daily backups did not occur on 39 (11 percent) of 365 days. TTB system backups were performed by a service provider and TTB management did not have policies and procedures in place to detect the backup failures or require their service provider to notify TTB when scheduled backups were not performed or backup jobs failed. (See *Recommendations # 41*)

Lack of frequent, successful backups can have a significant negative effect on Treasury information systems if a disaster (i.e., hard-drive failure, natural disaster, national emergency, etc.) were to occur. Data can be lost and successful system restoration thwarted if backup tapes are not available.

Additionally, disaster failover tests, as required by NIST SP 800-34, are paramount in assuring that Treasury information systems can remain operational with the least amount of downtime possible in emergencies. Failure to appropriately test recovery capabilities could result in the unavailability of critical Treasury information and information systems. For the sampled payment management systems at FMS, the U.S. Government may not be able to process time-sensitive, critical payments and a prolonged system outage could potentially harm the broader U.S. economy.

We recommend that DO management:

36. Adhere to the defined frequency of backup jobs as stated by the DO SSP. Incremental backups to tape should be performed on a daily basis while full backups should be performed on a weekly basis.
37. Determine whether an upgraded version of DO's backup solution or a different backup tool will remediate unexpected server shutdowns and restarts.
38. Perform a monthly test of physical tapes to verify their reliability and integrity as defined within the DO SSP. If the tapes fail, replace the tapes as needed.
39. Increase backup storage capacity to ensure that archived data is not overwritten prematurely and data retention standards are observed.

We recommend that FMS management:

40. Expedite the planned disaster recovery testing at the alternate recovery site to confirm that (a) FMS can resume mission critical functions within the stated two-hour recovery window and (b) the applications can operate successfully and communicate with other essential applications and third parties.

We recommend that TTB management:

41. Develop and implement policies and procedures to detect backup failures and remediate unsuccessful backups.

Based on TIGTA's planned corrective actions, we are not making a recommendation.

## **9. Outdated and unsupported software was utilized at OTS**

OTS utilized an unsupported operating system whose vendor ceased releasing new security patches to resolve new security exploits and software flaws. Although the application server resided behind the OTS firewall, the application server was vulnerable to new security exploits and viruses due to an outdated operating system.

According to OTS management, operational and staffing constraints associated with the transition of bank supervision responsibility to OCC permitted the condition to exist. Not maintaining fully patched and vendor supported operating system software exposes the OTS information system to a potential loss of availability, confidentiality, and integrity. As such, it is important to patch and update software as required.

Following the notification and discussion of the vulnerability with OTS IT personnel, OTS moved the application server to a virtual machine running a supported operating system. OTS also provided evidence that all required security patches were installed. We are not making a recommendation to OTS management as they took corrective actions to resolve the noted vulnerability.

**10. TIGTA’s risk management program was not consistent with NIST SP 800-37, Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems***

TIGTA was aware of the requirement to comply with NIST SP 800-37, Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, by February 2011, but had not updated the risk management program at the time of the FY 2011 FISMA audit. As NIST SP 800-37 Rev 1 was issued in February 2010, OMB requires federal agencies to adopt this NIST guidance within one year of issuance. KPMG did not determine a cause as the weakness was self-reported. TIGTA created a POA&M item to address identified gaps and developed corrective actions to become compliant, with a completion date of August 2014. An insufficient risk management program can lead to ineffective risk-based decision-making and untimely implementation of system-level controls.

Based on TIGTA’s planned corrective actions, we are not making a recommendation.

**11. The personnel termination procedures were not followed at FinCEN**

Treasury’s TD P 85-01, *Treasury Information Technology Security Program* requires its bureaus to implement personnel termination procedures in order to protect Treasury information from departing individuals and to recover government property. FinCEN Directive 901.02, *Personnel Separation Process*, defined the separation form required for departing personnel. FinCEN was unable to provide completed personnel separation forms for 18 of 25 separated employees and contractors sampled as evidence that it completed its exit clearance procedures. For 14 of the 18 individuals missing a separation form, additional evidence, substantiating that these individuals returned all government issued property, was inconclusive. FinCEN indicated that these forms were likely lost or misplaced as the employee and contractor separation process was manual and involved a paper, rather than electronic, form. Nevertheless, FINCEN asserted the separation process was followed for all departing employees, regardless of the missing forms.

Varying human factors in a complex process contributed to the condition above. Without separation forms as evidence that FinCEN supervisors and others completed the separation process, FinCEN could not demonstrate that it consistently executed its separation procedures and collected all government issued property. FinCEN asserted that all government property was returned by departing employees and cited mitigating controls such as the semi-annual inventory of all IT assets as evidence that IT assets were not missing.

We recommend that the FinCEN management:

42. Provide training on the requirements of FinCEN’s Personnel Separations Process Directive regarding employee separation to all parties involved in the exit process.
43. Maintain the employee exit forms in accordance with Treasury records management requirements.

## **12. The system configuration management programs were not implemented correctly at DO and TIGTA**

Treasury's TD P 85-01, *Treasury Information Technology Security Program*, requires its bureaus to sufficiently plan and implement procedures protecting Treasury information systems from unwarranted changes. In addition, bureaus must protect and maintain information system baseline configurations in order to ensure proper, secure operation. DO and TIGTA did not fully define or implement Configuration Management plans for its in-scope systems. In order to protect information integrity and confidentiality, it is important for bureaus to document and control their systems' configurations. The specific findings were as follows:

- A sampled DO system did not implement FDCC configurations for its desktops or obtain a waiver to implement a different standard. DO management self-reported this weakness and created a POA&M for it.
- The sampled TIGTA system lacked formal documentation in certain areas of configuration management. TIGTA management identified this weakness in a 2010 security assessment and created POA&M remediation actions to address the weaknesses identified with a completion date of May 2012.

By not adequately implementing their systems' Configuration Management programs, Treasury bureaus reduce their ability to track and maintain version control, protect against harmful or subversive code implementation, and recover from a disastrous event or service interruption.

Based on DO's and TIGTA's planned corrective actions, we are not making a recommendation.

**MANAGEMENT RESPONSE TO DRAFT REPORT**

The following is the OCIO's response, dated November 7, 2011, to the draft FY 2011 FISMA Performance Audit Report.

November 7, 2011

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

**FROM:** Robyn East /s/  
Deputy Assistant Secretary for Information Systems  
and Chief Information Officer (CIO)

**SUBJECT:** Management Response to Draft Audit Report – “FY 2011  
Audit of Treasury’s Federal Information Security Management  
Act (FISMA) Implementation for Its Unclassified Systems”

Thank you for the opportunity to comment on the draft audit report entitled, “FY 2011 Audit of Treasury’s Federal Information Security Management Act (FISMA) Implementation for Its Unclassified Systems.” The audit focuses on the adequacy of the Department’s information security program and practices for its unclassified systems. We appreciate your acknowledgement that our security program is in place and is generally consistent with FISMA. We have carefully reviewed the draft and are in agreement with all findings and recommendations. Please refer to the attachment for further details on our planned corrective actions.

The Department is committed to continual improvement of its security program and meeting requirements of FISMA. We have made notable progress over the past year. For example, we closed all but one finding and all but one of the twenty-nine recommendations from last year’s FISMA audit. We implemented the Risk Management Framework within the Department to improve the manner in which we manage risk for our information technology systems and associated sensitive data. Looking forward, we are focused on the new White House security priorities, Trusted Internet Connections, Personal Identity Verification and Continuous Monitoring, and have set the groundwork to meet our Fiscal Year 2012 goals.

We appreciate the audit recommendations, as they will help improve our security posture. If you have any questions, feel free to call Edward Roback, Associate CIO for Cyber Security at 202-622-2593.

Attachment

cc: Joel A. Grover, Deputy Assistant Inspector General for Financial Management  
and Information Technology Audit  
Edward A. Roback, Associate CIO for Cyber Security and Chief Information  
Security Officer

**Management Response to the Office of the Inspector General (OIG)  
Recommendations**

**(U) OIG Finding 1: Logical account management activities were not fully documented or consistently performed at OCC, OTS, TIGTA, DO and FMS**

**(U) OIG Recommendation 1:** For the Office of the Comptroller of the Currency (OCC), we recommend that management: Document the process for granting access to the newly hired bank examiners, including the associated user roles and required management approvals.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. OCC management is in the process of formalizing and codifying additional account management policy that will define and document the informal policy cited as a weakness by the OIG/KPMG. Additionally, OCC management has taken corrective action in documenting and implementing improved procedures for account provisioning and privilege modification. These enhanced procedures have been adopted to better validate a user's need for access to the information system referenced in the OIG's audit. Completed: October 31, 2011

**(U) Responsible Official:** Chief Information Security Officer (CISO)/Chief Privacy Officer (CPO), OCC

**(U) OIG Recommendation 2:** For the OCC, we recommend that OCC in its capacity of managing prior Office of Thrift Supervision (OTS) systems: Add the review of system administrator and application service accounts for the sampled system to the review of external user accounts.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. OCC management has taken steps to evaluate the state of the entire OTS Federal Information Security Management Act (FISMA) inventory, and is currently taking steps to incorporate systems formerly maintained by OTS into the OCC programs to ensure secure and compliant operations. Current integration efforts include prudent steps to update account management processes where necessary, in accordance with the disposition schedule for each system. Target completion: May 31, 2012.

**(U) Responsible Official:** CISO/CPO, OCC

**(U) OIG Recommendation 3:** For the OCC, we recommend that OCC, in its capacity of managing prior OTS systems: Document the purpose and use of application service accounts in the System Security Plan (SSP) or other publication.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. OCC management has taken steps to evaluate the state of the entire OTS FISMA

inventory, and is currently taking steps to incorporate systems formerly maintained by OTS into the OCC programs to ensure secure and compliant operations. Current integration efforts include prudent steps to update system documentation where necessary, in accordance with the disposition schedule for each system. Target completion: May 31, 2012.

**(U) Responsible Official:** CISO/CPO, OCC

**(U) OIG Recommendation 4:** For Departmental Offices (DO), we recommend that Management: Perform an annual review of end user accounts that addresses appropriateness of user access rights. As stated in the DO SSP, the Information System Security Officers (ISSOs) and/or the system administrators of each minor application should perform this review.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. DO and Office of Foreign Assets Control (OFAC) will enhance the account management process by developing more formalized account management procedures to include performing an annual review of OFAC's system accounts. Target completion: November 30, 2011.

**(U) Responsible Official:** ISSO, OFAC

**(U) OIG Recommendation 5:** For Departmental Offices (DO), we recommend that Management: Develop and implement a formal account approval process. A formal approval form should exist for all system users, including contractors. These forms should be properly tracked and stored to ensure that documentation is not lost or deleted.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. DO and OFAC will enhance the account management process by developing more formalized account management procedures for OFAC's systems to include an approval form for all users. These forms will be stored and tracked appropriately. Target completion: December 30, 2011.

**(U) Responsible Official:** ISSO, OFAC

**(U) OIG Recommendation 6:** For Financial Management Service (FMS), we recommend that Management: Continue to monitor the automated solution to disable user accounts after 90 days of inactivity in order to confirm the automated solution is working in all cases.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS continues to monitor the automated solution to disable users after 90 days of inactivity. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, Bureau of the Public Debt (BPD) and FMS

**(U) OIG Recommendation 7:** For FMS, we recommend that Management: Perform a manual monthly review of all user accounts, and disable or delete (as appropriate) accounts that have not logged into the system within the prior 90 days until the manual,

monthly review demonstrates that the automated solution is working for three consecutive months.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will perform manual monthly reviews for three consecutive months until the reviews demonstrate that the automated solution is working. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Finding 2: Security incidents were not reported timely at the CDFI Fund, FMS, Mint, and TIGTA**

**(U) OIG Recommendation 8:** For Community Development Financial Institution Fund (CDFI), we recommend that Management: Provide additional incident response training to increase awareness of the CDFI Fund's policies and procedures.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. The CDFI Fund CIO will ensure that additional incident response training is provided to increase awareness of the CDFI Fund's policies and procedures. Target completion: October 31, 2011.

**(U) Responsible Official:** CIO, CDFI Fund

**(U) OIG Recommendation 9:** For CDFI, we recommend that Management: Remind all CDFI Fund staff of their responsibility to timely report security incidents, including events such as the loss of mobile devices with one hour, to the CDFI Fund's Information Technology (IT) team. Such reminders could be incorporated into employee's annual security awareness training or be included in periodic reminders to employees to protect sensitive information and report the loss of mobile devices to the CDFI Fund's IT team.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. The CDFI Fund CIO will ensure that CDFI Fund staff are reminded of their responsibility to timely report security incidents, including events such as the loss of mobile devices within one hour, to the CDFI Fund's IT team. Target completion: October 31, 2011.

**(U) Responsible Official:** CIO, CDFI Fund

**(U) OIG Recommendation 10:** For CDFI, we recommend that Management: Provide the CDFI Fund employees the capability to report security incidents to the IT team outside of normal working hours by establishing a shared incident response e-mail account and/or phone number for reporting purposes.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. The CDFI Fund CIO will ensure that CDFI Fund employees have the capability to

report security incidents to the IT team outside of normal working hours by establishing a shared incident response e-mail account and list of IT team phone numbers for reporting purposes. Target completion: October 31, 2011.

**(U) Responsible Official:** CIO, CDIF Fund

**(U) OIG Recommendation 11:** For FMS, we recommend that Management: Revise the current incident reporting process and associated written procedures to ensure timely reporting. This could include the FMS incident response management notifying Treasury's Computer Security Incident Response Center (TCSIRC) with suspected or confirmed security events without the need for further FMS Executive management approvals.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will revise the current incident reporting process and procedures. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Recommendation 12:** For FMS, we recommend that Management: Provide additional training to FMS security personnel regarding FMS's revised incident response policies and procedures to ensure these policies and procedures are consistently implemented.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will revise the current incident reporting process and procedures and provide additional training to security personnel to ensure timely reporting. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Recommendation 13:** For FMS, we recommend that Management: Consider, if feasible, a Distributed Incident Response Team or a Partially Outsourced Team to achieve 24x7x365 coverage, per the NIST SP 800-61, *Computer Security Incident Handling Guide*. Such a strategy could involve sharing TSIRC resources with other Treasury bureaus.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will explore the feasibility of implementing a Distributed Incident Response Team or a Partially Outsourced Team to achieve 24x7x365 coverage. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Recommendation 14:** For FMS, we recommend that Management: Improve FMS employee awareness to report both confirmed and suspected security incidents to the FMS Service Desk. FMS could create awareness through periodic reminders via e-

mail, posting security posters in common employee areas, and through increased emphasis in annual security and awareness training.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will provide additional training to security personnel to ensure timely reporting. FMS plans to add mandatory incident response training to TLMS and post security posters in common employee areas and create periodic reminders via email to improve employee awareness in security incident reporting. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Recommendation 15:** For Mint, we recommend that Management: Have all tickets sent to the CSIRC group mailbox as opposed to individual members to ensure that tickets are tracked properly.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. Notification of Category 1 incidents to the entire Mint Computer Security Incident Response Center team has been and is currently required. This recommendation was addressed in August 2010. We consider this issue to be closed.

**(U) Responsible Official:** CISO, U.S. Mint

**(U) OIG Recommendation 16:** For Mint, we recommend that Management: Ensure a backup CSIRC member in place during the absence and/or unavailability of the primary individual. The backup CSIRC member should be notified if the primary individual has not acknowledged the ticket within a designated time period.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. Notification of Category 1 incidents to the entire Mint CSIRC team has been and is currently required. This recommendation was addressed in August 2010. The Mint management implemented a change to require that all Category 1 incidents require documented acknowledgement of receipt by the CSIRC team. The recommendation concerns a problem in documentation created prior to August 2010. We consider this issue to be closed.

**(U) Responsible Official:** CISO, U.S. Mint

**(U) OIG Recommendation 17:** For Treasury Inspector General for Tax Administration (TIGTA), we recommend that Management: Assign an additional individual as a back-up resource to the TIGTA Computer Security Incident Response Center (CSIRC) for periods of reduced staffing.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. TIGTA plans to evaluate various options for providing after hours incident response reporting capabilities. The options to be evaluated include using a

contractor, in-house staff, or shared Bureau services. Additional funding to implement the after hours reporting capabilities will be requested in next year's budget submission. Target completion: January 31, 2013.

**(U) Responsible Official:** CISO, TIGTA

**(U) OIG Recommendation 18:** For TIGTA, we recommend that Management: Provide the TIGTA CSIRC the ability to receive and address security incidents outside of normal working hours by establishing a shared incident response e-mail account and/or phone number for reporting purposes. Additionally, consider participating in a shared Incident Response team with another Treasury bureau to provide increased capabilities outside of normal working hours.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. TIGTA plans to evaluate various options for providing after hours incident response reporting capabilities. The options to be evaluated include using a contractor, in-house staff, or shared Bureau services. Additional funding to implement the after hours reporting capabilities will be requested in next year's budget submission. Target completion: January 31, 2013.

**(U) Responsible Official:** CISO, TIGTA

**(U) OIG Recommendation 19:** For TIGTA, we recommend that Management: Provide the TIGTA CSIRC additional incident response training to ensure they are aware of TIGTA's policies and procedures, including their responsibility to timely report security incidents.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. TIGTA has distributed and discussed incident reporting procedures with its CSIRC team members. TIGTA CSIRC team members will start holding monthly meetings to discuss the reporting process. Target completion: November 30, 2011.

**(U) Responsible Official:** CISO, TIGTA

**(U) OIG Finding 3: System security plans at DO, Mint, and FMS did not fully adopt NIST recommended security controls from *NIST SP 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations***

**(U) OIG Recommendation 20:** For DO, we recommend that Management: Instruct the vendor to update the SSPs to include NIST SP 800-53, Rev. 3 security controls and associated control enhancements.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. DO and the audited system's Program Management Office will direct the vendor

to comply with the latest version of NIST SP 800-53 guidance and revise the System's Security Plan as appropriate. Target completion: February 30, 2012.

**(U) Responsible Official:** ISSO, Treasury Network

**(U) OIG Recommendation 21:** For Mint, we recommend that Management: Update their Information Security Program's policies and procedures to require that all SSPs are updated to include the latest NIST SP 800-53 controls and control enhancements one year after issued.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. Mint is reviewing and updating its policies and procedures to require that all SSPs are updated to include the latest NIST SP 800-53 controls and control enhancements no later than one year after issued. Target completion: March 31, 2012.

**(U) Responsible Official:** CISO, Mint

**(U) OIG Recommendation 22:** For Mint, we recommend that Management: Ensure that all existing SSPs are 800-53, Revision 3 compliant.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. Mint is ensuring that all existing SSPs are 800-53, Revision 3 compliant. Target completion: March 31, 2012.

**(U) Responsible Official:** CISO, Mint

**(U) OIG Recommendation 23:** For FMS, we recommend that Management: Ensure that System Owners and ISSOs review and update SSPs by using the FMS-approved SSP template and baseline security requirements, which incorporate NIST SP 800-53, Rev. 3 security controls.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will ensure SSPs are updated in accordance with NIST and FMS guidance. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Finding 4: FMS did not perform sufficient audit log reviews in accordance with NIST and Treasury standards**

**(U) OIG Recommendation 24:** For FMS, we recommend that Management: Identify and document significant audit events that warrant review and further investigation.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will identify and document significant audit events that warrant further investigation. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Recommendation 25:** For FMS, we recommend that Management: Update the SSP in order to reflect the results of the risk analysis and clearly assign ownership and responsibility for implementing the agreed upon audit log review procedures.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will update the SSP to reflect risk analysis results and assign responsibility for implementing the agreed upon audit log review procedures. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Recommendation 26:** For FMS, we recommend that Management: Ensure that sufficient resources are available to implement audit log review procedures.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will ensure sufficient resources are available to implement audit log review procedures. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Finding 5: BPD did not properly inventory media scheduled for sanitization in accordance with BPD procedures**

**(U) OIG Recommendation 27:** For the Bureau of the Public Debt (BPD), we recommend that Management: Implement its BLSRs and associated procedures on maintaining a clear chain of custody, properly securing media when stored, and reconciliation of media received and sent for destruction.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. BPD has updated Office of Information Technology (OIT) Standard Operating Procedures 2.2.85 to clarify the chain of custody requirements, coordinated the excess process with the Office of Management Services/Property Management Section, and added a locked box for more secure storage as recommended. Completed: September 30, 2011

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Recommendation 28:** For BPD, we recommend that Management: Train BPD IT specialists on the BPD media sanitization policies and procedures in order to protect the confidentiality of the bureau's sensitive information.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. Responsible BPD IT Specialists have been trained on the updated media sanitization policies and procedures. Completion date was September 30, 2011. Completed: September 30, 2011

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Finding 6: Plans of Action and Milestones (POA&Ms) were not tracked and remediated in accordance with NIST and Treasury requirements at FMS and OTS**

**(U) OIG Recommendation 29:** For FMS, we recommend that Management: Perform a comprehensive study of FMS's POA&M management practices to resolve ongoing auditor-identified POA&M challenges. Based on the outcome of this study, FMS should implement corrective actions designed to ensure complete, accurate and timely reporting of POA&M items.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will perform a comprehensive study of FMS's POA&M management practices and: establish performance metrics to report and resolve security weaknesses. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Recommendation 30:** For FMS, we recommend that Management: Strengthen FMS's existing policies and procedures regarding POA&Ms based on the outcome of FMS's study. The revised FMS policies and procedures should define roles, responsibilities, and expected communication frequency among key participants and decision makers.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will perform comprehensive study of FMS's POA&M management practices and: define roles, responsibilities and expected communication frequency among key participants and decision makers in POA&M policies and procedures. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Recommendation 31:** For FMS, we recommend that Management: Promote increased involvement by FMS executives and Authorizing Officials in the POA&M management process. Such actions could include establishing performance metrics and associated incentives and/or disincentives for FMS management personnel to accurately report and resolve noted security weaknesses in their portfolio of information systems.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will perform comprehensive study of FMS's POA&M management practices and: establish performance metrics to report and resolve security weaknesses; and explore incorporating Authorizing Official, System Owner and ISSO responsibilities and expected outcomes in performance plans. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Recommendation 32:** For FMS, we recommend that Management: Promote personal accountability for executing information security responsibilities, such as those listed in the ISSO and System Owner Appointment Letters, by incorporating those responsibilities and expected outcomes in the employees' Annual Performance Plan.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will establish performance metrics to report and resolve security weaknesses, and explore incorporating Authorizing Official, System Owner and ISSO responsibilities and expected outcomes in performance plans. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Finding 7: Vulnerability scanning and remediation was not performed in accordance with Treasury requirements at the CDFI Fund, DO, and OTS**

**(U) OIG Recommendation 33:** For CDFI, we recommend that Management: Revise the Interconnection Security Agreement with Alcohol Tobacco Tax and Trade Bureau (TTB) to define clear roles and responsibilities for providing services and implementing associated security controls such as vulnerability scanning.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. The CDFI Fund CIO will ensure that the Interconnection Security Agreement with TTB is revised to define clear roles and responsibilities for providing services and implementing associated security controls such as vulnerability scanning. Target completion: November 30, 2011.

**(U) Responsible Official:** CIO, CDFI Fund

**(U) OIG Recommendation 34:** For CDFI, we recommend that Management: Enhance the continuous monitoring strategy for outsourced information systems to ensure that NIST and Treasury required security controls are implemented and operating effectively. As part of the strategy, share the results with appropriate CDFI Fund System Owners and IT management.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. The CDFI Fund CIO will ensure that the continuous monitoring strategy for

outsourced information systems is enhanced to ensure that NIST and Treasury required security controls are implemented and operating effectively. Completed: October 31, 2011

**(U) Responsible Official:** CIO, CDFI Fund

**(U) OIG Recommendation 35:** For DO, we recommend that Management: Direct personnel charged with remediating vulnerabilities to track open, unresolved vulnerabilities in system POA&Ms when the anticipated remediation will exceed 30 days.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. DO and the audited system's Program Management Office will direct personnel charged with remediating vulnerabilities to add open vulnerabilities of more than 30 days to the POA&M report in the Trusted Agent FISMA tool for all devices that are part of the audited system. Completed: October 30, 2011

**(U) Responsible Official:** ISSO, DO Audited Systems

**(U) OIG Finding 8: Contingency planning & testing and backup controls were not fully implemented or operating as designed at DO, FMS, TIGTA, and TTB**

**(U) OIG Recommendation 36:** For DO, we recommend that Management: Adhere to the defined frequency of backup jobs as stated by the DO SSP. Incremental backups to tape should be performed on a daily basis while full backups should be performed on a weekly basis.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. DO will adhere to the defined frequency of backup jobs as stated by the DO System Security Plan. Target completion: November 30, 2011.

**(U) Responsible Official:** Director, Information Technology (IT) Infrastructure Operations, DO

**(U) OIG Recommendation 37:** For DO, we recommend that Management: Determine whether an upgraded version of DO's backup solution or a different backup tool will remediate unexpected server shutdowns and restarts.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. DO will upgrade the backup software and hardware to remediate overflow issues. Target completion: June 30, 2012.

**(U) Responsible Official:** Director, IT Infrastructure Operations, DO

**(U) OIG Recommendation 38:** For DO, we recommend that Management: Perform a monthly test of physical tapes to verify their reliability and integrity as defined within the DO SSP. If the tapes fail, replace the tapes as needed.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. DO will upgrade the backup software and hardware to remediate overflow issues. Target completion: November 30, 2011.

**(U) Responsible Official:** Director, IT Infrastructure Operations, DO

**(U) OIG Recommendation 39:** For DO, we recommend that Management: Increase backup storage capacity to ensure that archived data is not overwritten prematurely and data retention standards are observed.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. DO will increase the storage of CDL tapes to ensure backup data is retained in accordance with retention standards. Completed: June 30, 2012.

**(U) Responsible Official:** Director, IT Infrastructure Operations, DO

**(U) OIG Recommendation 40:** For FMS, we recommend that Management: Expedite the planned disaster recovery testing at the alternate recovery site to confirm that (a) FMS can resume mission critical functions within the stated two-hour recovery window and (b) the applications can operate successfully and communicate with other essential applications and third parties.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FMS will expedite the disaster recovery testing at the alternate recovery site to confirm that applications can operate successfully, communicate with other essential applications, and that mission critical functions can be resumed within the two-hour recovery window. Target completion: June 29, 2012.

**(U) Responsible Official:** CISO, BPD and FMS

**(U) OIG Recommendation 41:** For the Alcohol and Tobacco Tax and Trade Bureau (TTB), we recommend that Management: Develop and implement policies and procedures to detect backup failures and remediate unsuccessful backups.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. Since this issue was identified, TTB no longer utilizes this service provider for backup (or hosting) services for the production environment. TTB has moved these services in house as of September 4, 2011, and all production servers are managed through our internal policy and procedures. We consider this issue to be closed.

**(U) Responsible Official:** CISO, TTB

**(U) OIG Finding 9: Outdated and unsupported software was utilized at OTS**

**(U) OIG:** We are not making a recommendation to OTS management as they took corrective actions to resolve the noted vulnerability.

**(U) OIG Finding 10: TIGTA's risk management program was not consistent with NIST SP 800-37, Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems***

**(U) OIG:** Based on TIGTA's planned corrective actions, we are not making a recommendation.

**(U) OIG Finding 11: The personnel termination procedures were not followed at FinCEN**

**(U) OIG Recommendation 42:** For the Financial Crimes Enforcement Network (FinCEN), we recommend that Management: Provide training on the requirements of FinCEN's Personnel Separations Process Directive regarding employee separation to all parties involved in the exit process.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FinCEN plans to remediate this finding by streamlining the *FinCEN Directive 901.02, Personnel Separation Process* to reduce duplicative efforts and maintain a single repository of Fin015 documentation. Once the modified directive is approved, FinCEN will ensure that all responsible parties (e.g. office supervisors, COTRs, etc...) are aware of the updated process and responsibilities defined in the Directive. Target completion: January 31, 2012.

**(U) Responsible Official:** CISO, FinCEN

**(U) OIG Recommendation 43:** For the FinCEN, we recommend that Management: Maintain the employee exit forms in accordance with Treasury records management requirements.

**(U) Treasury Response:** Treasury agrees with this finding and recommendation. FinCEN plans to remediate this finding by streamlining the *FinCEN Directive 901.02, Personnel Separation Process* to reduce duplicative efforts and maintain a single repository of Fin015 documentation. Once the modified directive is approved, FinCEN will ensure that all responsible parties (e.g. office supervisors, COTRs, etc...) are aware of the updated process and responsibilities defined in the Directive. Target completion: January 31, 2012.

**(U) Responsible Official:** CISO, FinCEN

**(U) OIG Finding 12: The system configuration management programs were not implemented correctly at DO and TIGTA**

**(U) OIG:** Based on DO's and TIGTA's planned corrective actions, we are not making a recommendation.

**APPENDIX I – TREASURY FISMA COMPLIANCE SUMMARY**

**Table 1: Summary Phase B Test Results**

The following table presents KPMG’s summary test results for non-IRS Bureau-level control tests based on DHS’s FISMA 2011 Questions for Inspectors General. As the table indicates, most Treasury Bureaus had established and implemented common security policies and procedures based on NIST, Treasury, and Bureau guidelines. The results presented below were obtained from a nonstatistical sample of Treasury information systems. These results cannot be extrapolated to the entire population of Treasury information systems. Additionally, we caution that projecting the results of our audit to future periods is subject to risks as controls may become inadequate due to changes in technology or the deterioration of control compliance.

<b>PHASE B - Bureau Level Control Testing</b>	BEP	BPD	CDFI	DO	FinCEN	FMS	OCC	OIG	Mint	TIGTA	TTB	Total
Risk Management	1	1	1	1	1	1	1	1	1	0	1	10
Configuration Management	1	1	1	1	1	1	1	1	1	1	1	11
Incident Response and Reporting	1	1	0	1	1	0	1	1	0	0	0	6
Security Training	1	1	1	1	1	1	1	1	1	1	1	11
Plans of Actions and Milestones	1	1	1	1	1	1	1	1	1	1	1	11
Remote Access Management	1	1	1	1	1	1	1	1	1	1	1	11
Identity and Access Management	1	1	1	1	1	1	1	1	1	1	1	11
Continuous Monitoring Management	1	1	1	1	1	1	1	1	1	1	1	11
Contingency Planning	1	1	1	1	1	1	1	1	1	1	1	11
Contractor Systems	1	1	0	1	1	1	1	1	1	1	1	10
Security Capital Planning	1	1	1	1	1	1	1	1	1	1	1	11
<b>Total</b>	<b>11</b>	<b>11</b>	<b>9</b>	<b>11</b>	<b>11</b>	<b>10</b>	<b>11</b>	<b>11</b>	<b>10</b>	<b>9</b>	<b>10</b>	<b>114</b>

**Legend:**

1 = Sampled NIST SP 800-53 security control generally compliant with NIST, Treasury, and Bureau policy.

0 = Sampled NIST SP 800-53 control did not meet NIST, Treasury, or Bureau policy.

OTS results were not included as OTS ceased operations on July 21, 2011.

**Table 2: Summary Phase C Test Results for Sampled System Level Security Controls**

The following table presents the summary test results for the 15 non-IRS information systems that we sampled as indicated in the table below. Security controls related to Account Management and Vulnerability Scanning showed the lowest, overall compliance of tested controls.

PHASE C - System Level Control Testing	BEP	BPD	CDFI	DO			FinCEN	FMS			OCC	OTS	Mint	TIGTA	TTB	Total
				A	B	C		A	B	C						
<b>System:</b>	A	A	A	A	B	C	A	A	B	C	A	A	A	A		
Account Management	1	1	1	0	1	1	1	1	1	0	0	1	0	1	10	
Separation of Duties	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15	
Auditable Events	1	1	1	1	1	1	1	1	1	0	1	1	1	1	14	
Audit Generation	1	1	1	1	0	1	1	1	1	1	1	1	1	1	14	
Security Assessments	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15	
Plan of Action and Milestones	1	1	1	1	1	1	1	0	0	0	1	0	1	1	11	
Security Authorization	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15	
Continuous Monitoring	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15	
Baseline Configuration	1	1	1	1	0	1	1	1	1	1	1	1	0	1	13	
Configuration Settings	1	1	1	1	1	1	1	1	1	1	1	1	0	1	14	
Contingency Plan	1	1	1	1	1	1	1	1	1	1	1	1	0	1	14	
Contingency Plan Testing and Exercises	1	1	1	1	1	1	1	0	0	1	1	1	0	1	13	
Information System Backup	1	1	1	0	0	1	1	1	1	1	1	1	0	0	11	
User Identification and Authentication	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15	
Device Identification and Authentication	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15	
System Security Plan	1	1	1	1	0	1	1	0	1	1	1	0	1	1	12	
Security Categorization	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15	
Risk Assessment	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15	
Vulnerability Scanning	1	1	0	1	0	1	1	0	0	1	1	0	1	1	10	
Flaw Remediation	1	1	1	1	0	1	1	1	0	1	1	0	1	1	12	
<b>System Specific Total</b>	<b>20</b>	<b>20</b>	<b>19</b>	<b>1</b>	<b>1</b>	<b>8</b>	<b>4</b>	<b>20</b>	<b>17</b>	<b>16</b>	<b>17</b>	<b>19</b>	<b>14</b>	<b>19</b>	<b>268</b>	
Media Sanitization - Common Control	1	0	1	1	1	1	1	1	1	1	1	*	1	1	9	
Visitor Control - Common Control	1	1	1	1	1	1	1	1	1	1	1	*	1	1	10	
Personnel Termination - Common Control	1	1	1	1	1	1	0	0	1	1	1	*	1	1	9	
Use of Cryptography - Common Control	1	1	1	1	1	1	1	1	1	1	1	*	1	1	10	
<b>Bureau / Common Control Total</b>	<b>4</b>	<b>3</b>	<b>4</b>	<b>4</b>	<b>4</b>	<b>3</b>	<b>3</b>	<b>4</b>	<b>4</b>	<b>4</b>	<b>4</b>	<b>N/A</b>	<b>4</b>	<b>4</b>	<b>38</b>	

**Legend:**

1 = Sampled NIST SP 800-53 security control generally compliant with NIST, Treasury, and Bureau policy.

0 = Sampled NIST SP 800-53 control did not meet NIST, Treasury, or Bureau policy.

A = First sampled bureau system; B=Second Sampled System; C=Third Sampled System

\* - OTS ceased operations in July 2011 and thus KPMG did not test common controls for OTS.

---

**APPENDIX II – OBJECTIVE, SCOPE & METHODOLOGY**

The objectives for this performance audit were to determine the effectiveness of Treasury’s information security programs and practices for the period July 1, 2010 to June 30, 2011 for Treasury’s unclassified systems, and to determine whether non-IRS Treasury bureaus had implemented:

- An information security program, consisting of policies, procedures, and security controls consistent with the FISMA legislation.
- The security controls catalog contained in NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*.

We conducted our performance audit in accordance with generally accepted government auditing standards (GAGAS) issued by the Comptroller General of the United States (U.S.). 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 objective.

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation, Presidential directives, DHS *FY 2011 Inspector General Federal Information Security Management Act Reporting*, OMB Memorandum 11-33, *FY 2011 Reporting Instructions for Federal Information Security Management Act and Agency Privacy Management*, and NIST standards and guidelines as outlined in the *Criteria* section. We reviewed the Treasury information security program from both the Department-level perspective for Treasury-wide program-level controls and the Bureau-level implementation perspective. We considered each area above to reach an overall conclusion regarding Treasury’s information security program and practices.

KPMG took a phased approach to satisfy the audit’s objective as listed below:

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

To gain an overall enterprise-level understanding, we assessed management, policies, and guidance for the overall Treasury-wide information security program per requirements defined in FISMA and DHS *FY 2011 Inspector General Federal Information Security Management Act Reporting*, NIST SPSP 800-53, as well as Treasury guidelines developed in response to FISMA. This included program controls applicable to information security governance, 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, contingency planning, and contractor systems.

**PHASE B: Assessment of Bureau-Level Compliance**

To gain an overall bureau-level understanding, we assessed the implementation of the guidance for the 12<sup>2</sup> bureau and office wide information security programs according to requirements defined in FISMA and OMB Memorandum 11-33, NIST SPSP 800-53, as well as Treasury guidelines developed in response to FISMA. This included program controls applicable to information security governance, certification and accreditation, security configuration management, incident response and reporting, security training, POA&M, remote access, account and identity management, continuous monitoring, contingency planning, and contractor systems.

---

<sup>2</sup> We did not assess OTS’s bureau-level compliance due to the bureau’s planned closure in July 2011. TIGTA assessed IRS’s bureau-level compliance.

---

**PHASE C: Assessment of the Implementation of Select Security Controls from the NIST SP 800-53 Rev. 3**

To gain an overall understanding of how effective the bureaus implemented information security controls at the system level, we assessed the implementation of a selection of security controls from the NIST SP 800-53 Rev. 3 for a representative subset of Treasury information systems (see Appendix V).

To conclude on the audit's objectives, our scope included evaluating the information security practices and policies established by the Treasury OCIO. In addition, we evaluated the information security practices, policies, and procedures in use across 313 bureaus of the Treasury, excluding the IRS.

We also tested a representative subset of 15 information systems from a total population of 117 non-IRS major applications and general support systems as of May 11, 2011.<sup>3</sup> We tested the 15 information systems to determine whether bureaus were effective in implementing Treasury's security program and meeting the FIPS 200 minimum security standards to protect information and information systems. Appendix IV, *Approach to Selection of Subset of Systems*, provides additional details regarding our system selection. The subset of systems encompassed systems managed and operated by 12 of 14 Treasury bureaus, excluding IRS and OIG.<sup>4</sup>

Our criteria for selecting security controls within each system were based on the following:

- Controls that were shared across a number of information systems, such as common controls,
- Controls that were likely to change over time (i.e., volatile) and require human intervention, and
- Controls that were identified in prior audits as requiring management's attention.

#### Other Considerations

In performing our control evaluations, we interviewed key Treasury OCIO personnel who had significant information security responsibilities as well as personnel across the 13 non-IRS bureaus. We also evaluated Treasury 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, D.C., and bureau locations in Washington, D.C.; Hyattsville, Maryland; McLean, Virginia; and Parkersburg, West Virginia during the period of April 26, 2011, through August 31, 2011. During our performance audit, we met with Treasury management to discuss our preliminary conclusions.

---

<sup>3</sup> A representative subset of information systems refers to KPMG's approach of stratifying the population of non-IRS Treasury information system and selecting an information system from each Treasury bureau, excluding IRS and OIG, rather than selecting a random sample of information systems that might exclude a Treasury bureau.

<sup>4</sup> KPMG inspected only one OIG or TIGTA information system every year. In FY 2011 TIGTA was selected as the OIG was selected in FY 2010.

---

**Criteria**

We focused our FISMA performance audit approach on federal information security guidance developed by NIST and OMB. NIST Special Publications provide guidelines that are considered essential to the development and implementation of agencies' security programs.<sup>5</sup> The following is a listing of the criteria used in the performance of the Fiscal Year (FY) 2011 FISMA performance audit:

- OMB Circular A-130, *Management of Federal Information Resources*;
- NIST FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;
- NIST FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;
- NIST Special Publications:
  - 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*
  - 800-18 Rev. 1, *Guide for Developing Security Plans for Information Technology Systems*
  - 800-30, *Risk Management Guide for Information Technology Systems*
  - 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*
  - 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*
  - 800-39, *Managing Risk from Information Systems: An Organizational, Mission and Information System View*
  - 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*
  - 800-53A Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*
  - 800-60 Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
  - 800-61 Rev. 1, *Computer Security Incident Handling Guide*
  - 800-70 Rev. 2, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*
- OMB Memoranda:
  - 04-04, *E-Authentication Guidance for Federal Agencies*
  - 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*
  - 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*
  - 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
  - 07-18, *Ensuring New Acquisitions Include Common Security Configurations*

---

<sup>5</sup> Note (per OMB instructions M-11-33 *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*): While agencies are required to follow NIST standards and guidance in accordance with OMB policy, there is flexibility within NIST's guidance documents in how agencies apply the guidance. However, NIST Special Publication 800-53 is mandatory because FIPS 200 specifically requires it. Unless specified by additional implementing policy by OMB, guidance documents published by NIST generally allow agencies latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable and compliant with the guidance.

- 08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)*
- 11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
  
- Treasury Guidance:
  - TD P 85-01, *Treasury Information Technology Security Program*

**APPENDIX III – STATUS OF PRIOR YEAR FINDINGS**

Finding Number	Prior Year Condition	Recommendation(s)	Status
<p><b>Prior Year FY 2010 Finding #1 –</b>  <b>a. Office of Chief Information Officer</b>                      Logical and Physical Account Management Activities were not Consistently Performed</p>	<p>The audit identified inconsistent implementation of account management and physical access security controls at six bureaus including the Bureau of Engraving and Printing (BEP), Departmental Offices (DO), Financial Crimes Enforcement Network (FinCEN), Office of the Comptroller of the Currency (OCC), Office of the Inspector General (OIG), and the Office of Thrift Supervision (OTS). This finding indicated that the Treasury OCIO had not provided sufficient oversight to enforce and monitor compliance with Treasury and National Institute of Standards and Technology (NIST) identify and access management standards and guidelines.</p>	<p>We recommend that OCIO management provide sufficient oversight by the Treasury OCIO Cyber Security Program over the NIST SPSP 800-53 security controls around Account Management, Physical Access Authorization, and Physical Access Control to ensure that the bureaus implement these controls. This can be accomplished by reviewing the implementation of these controls during the next OCIO review at each bureau.</p>	<p><b>Implemented/Closed.</b>                      OCIO updated the Treasury Directive Publication (TD P) 85-01 to reflect new account management procedures based on NIST SPSP 800-53 Rev. 3.</p>
<p><b>Prior Year FY 2010 Finding #1 –</b>  <b>b. Bureau of Engraving and Printing</b>                      Logical and Physical Account Management Activities were not Consistently Performed</p>	<p>BEP did not document its review of user accounts for the selected system in accordance with their system security plan.</p>	<p>We recommend that the BEP management perform and document user access reviews for their system in accordance with their system security plan.</p>	<p><b>Implemented/Closed.</b>                      BEP reviewed and documented access review of users for the selected system.</p>
<p><b>Prior Year FY 2010 Finding #1 –</b>  <b>c. Departmental Offices</b>                      Logical and Physical Account Management Activities were not Consistently Performed</p>	<p>The DO systems had user and administrator accounts that had been inactive for over 90 days and had not been disabled. These accounts are created and maintained by the OCIO, who uses the system for performance of their Treasury-wide FISMA oversight role.</p>	<p>We recommend that OCIO management:</p> <ol style="list-style-type: none"> <li>1. Ensure administrators for the reviewed DO system review user accounts and disable inactive accounts in accordance with TD P 85-01 (as a minimum) and any applicable bureau policy.</li> <li>2. Review administrator accounts for inactivity on a quarterly basis and disable accounts per</li> </ol>	<p><b>Implemented/Closed.</b>                      The sampled DO system is reviewed for inactivity by administrators on a quarterly basis and inactive accounts are disabled. OCIO Management send outs quarterly training/awareness e-mails with</p>

Finding Number	Prior Year Condition	Recommendation(s)	Status
<p><b>Prior Year FY 2010 Finding #1 –</b>  <b>d. Financial Crimes Enforcement Network</b>                      Logical and Physical Account Management Activities were not Consistently Performed</p>	<p>Physical access to the FinCEN data center was not reviewed annually and access approval forms were not maintained.</p>	<p>the TD P 85-01 for the reviewed DO system.                      3. Train the reviewed DO system’s administrators on how to review the accounts of the users assigned to their respective bureaus on a quarterly basis and disable the accounts that exceed 90 days of inactivity.</p> <p>We recommend that FinCEN management:</p> <ol style="list-style-type: none"> <li>1. Perform review and validation of physical access to restricted areas, annually.</li> <li>2. Document and approve all employees’ physical access requirements.</li> <li>3. Document and approve the door “zone” configuration of the physical access control system.</li> <li>4. Develop a documented procedure for the approval, administration, review, and validation of access to restricted areas.</li> </ol>	<p>instructions on how to review and disable accounts to every Bureau Administrator.</p> <p><b>Implemented/Closed.</b>                      FinCEN performed a review and approval of the physical access to restricted areas. FinCEN changed the door “zone” configuration of the physical access control system. FinCEN documented their physical access control procedures for the approval, administration, review, and validation of access to restricted areas.</p>
<p><b>Prior Year FY 2010 Finding #1 –</b>  <b>e. Office of the Comptroller of the Currency</b>                      Logical and Physical Account Management Activities were not Consistently Performed</p>	<p>The OCC system did not have an automated control in place to automatically deactivate users’ accounts after the bureau-defined period of inactivity.</p>	<p>We recommend that OCC management develop and implement an automated means to disable inactive user accounts from the reviewed system after 60 days for Federal employees and 30 days for contractors.</p>	<p><b>Implemented/Closed.</b>                      OCC management implemented an alternative corrective action by implementing a weekly review of accounts for the selected system.</p>
<p><b>Prior Year FY 2010 Finding #1 –</b>  <b>f. Office of the Inspector General</b></p>	<p>The OIG systems had user and administrator accounts that had been inactive for over 90 days and had not been disabled. In addition, the OIG Local Area Network (LAN) room’s access list was not reviewed annually and users, who no longer</p>	<p>We recommend that OIG management:</p> <ol style="list-style-type: none"> <li>1. Ensure domain user accounts are reviewed for inactivity on an annual basis and domain administrator accounts are reviewed for inactivity on a semiannual basis, and any</li> </ol>	<p><b>Implemented/Closed.</b>                      OIG reviews physical access list at least annually and performs a quarterly review of user accounts. OIG follows the</p>

Finding Number	Prior Year Condition	Recommendation(s)	Status
<p>Logical and Physical Account Management Activities were not Consistently Performed</p>	<p>need access, were not removed in a timely manner.</p>	<p>accounts that exceed 90 days of inactivity are disabled.</p> <ol style="list-style-type: none"> <li>Develop policies and procedures and document them in the system security plan for the annual review of OIG LAN room access.</li> <li>Conduct a review of users' access to the OIG LAN room annually and remove access privileges for those individuals that do not need access.</li> </ol>	<p>TD P 85-01 policies and procedures for annual review of physical access to its facilities.</p>
<p><b>Prior Year FY 2010 Finding #1 – g. Office of Thrift Supervision</b> Logical and Physical Account Management Activities were not Consistently Performed</p>	<p>The periodic review of the OTS application users' access did not include reviewing users' privileges within the application in order to determine if they were appropriate based on users' roles at the OTS. The review of access only had accessed whether users were active employees at the organization.</p>	<p>We recommend that OTS management:</p> <ol style="list-style-type: none"> <li>Develop and implement a training program that outlines how the six-month user privileges review should be performed.</li> <li>Develop and implement a mechanism to track completion of the six-month user privileges review.</li> </ol>	<p><b>Implemented/Closed.</b> OTS prepared procedures and instructions on how to review accounts for inactivity and appropriateness, and conducted a six-month user review.</p>
<p><b>Prior Year FY 2010 Finding #2 – a. Financial Management Service</b> Communication Gaps and IT Governance Concern with Financial Agent in Information System Security Officer (ISSO) Position</p>	<p>Financial Management Service (FMS) transferred the ISSO role from a government employee to a bank employee for an outsourced information system in March 2010 by utilizing an existing financial agent agreement with a large national bank. The outsourcing of the ISSO role created two IT governance concerns. First, KPMG noted that the appointed ISSO, a bank employee, could not fully perform his assigned information security duties. Second, the transfer of the ISSO role from a FMS employee to a bank employee created additional concerns regarding IT governance. Specifically, the new ISSO, a bank employee, reported to the Operations Manager for the outsourced information system.</p>	<p>We recommend that FMS Management:</p> <ol style="list-style-type: none"> <li>Provide the ISSO with the network connectivity that will allow the bank employee access to FMS internal resources such as Treasury's FISMA collection and reporting tool, current FMS IT security policy and security templates, and ability to receive FMS e-mail alerts regarding changes to FMS IT security policy and security templates.</li> <li>Create FMS official guidance covering the appointment of the ISSO position at external providers. In such circumstances, FMS should confirm that communication requirements and needs are satisfied prior to outsourcing the ISSO position. Additionally, the guidance should address reporting</li> </ol>	<p><b>Implemented/Closed.</b> FMS provided the ISSO access to necessary systems to allow the ISSO to perform assigned duties, as well as included guidance in the FMS <i>ISSO Appointment Process</i> procedural documentation for the assignment of external ISSOs. In addition, the financial agent relocated their ISSO under the Project Management Office and Controls Organization in order to remediate any conflict of interest with the Operations Manager as of January 1, 2011.</p>

Finding Number	Prior Year Condition	Recommendation(s)	Status
<p><b>Prior Year FY 2010 Finding #3 - a. Financial Management Service</b></p> <p>Untimely Recording of Plans of Actions and Milestones (POA&amp;M) in Trusted Agent FISMA (TAF)</p>	<p>Two of the three FMS systems reviewed, previously identified security weaknesses and associated remediation plans were not added timely (i.e., within 30 days<sup>6</sup>) to the POA&amp;Ms of record as required by Office of Management and Budget (OMB) M-10-15, Treasury policy, and FMS policy.</p>	<p>relationships that might impact the ISSO's objectivity and clearly identify monitoring activities and assignment of responsibility to an FMS employee to mitigate potential conflicts.</p> <p>3. Evaluate solutions to mitigate concerns over ISSO-management reporting relationships, which could include, for example, establishing or modifying internal controls, implementing monitoring tools, realigning the ISSO position under the bank's Information Security team or elsewhere within the bank, contracting for ISSO services through a different provider such as independent verification and validation contractor, or reassigning ISSO responsibilities back to an FMS employee.</p>	<p><b>Partially Implemented/Open.</b></p> <p>KPMG determined that Recommendation 1 of the FY 2010 POA&amp;M NFR has been addressed. However, KPMG noted similar control deficiencies with the associated POA&amp;Ms for the three FMS sampled systems. See Finding #6 – Financial Management Service.</p>
<p><b>Prior Year FY 2010 Finding #3 – b. Office of Comptroller of Currency</b></p>	<p>For one OCC system, previously identified security weaknesses and associated remediation plans were not added timely to the POA&amp;M as required by OMB M-10-15, Treasury policy, and bureau standards. Specifically, OCC did not update, submit,</p>	<p>We recommend that FMS Management:</p> <ol style="list-style-type: none"> <li>1. Direct ISSOs to develop and record POA&amp;M items in TAF within the designated time period when security vulnerabilities are identified. (Closed)</li> <li>2. Provide additional oversight across all FMS systems to ensure that the POA&amp;M process is managed in accordance with FMS, Treasury, and OMB policy and guidance. (Open)</li> </ol> <p>We recommend that OCC:</p> <ol style="list-style-type: none"> <li>1. Populate the information system's POA&amp;M to include vulnerabilities found in all applicable IT security reviews and audits, including vulnerabilities identified from</li> </ol>	<p><b>Implemented/Closed.</b></p> <p>OCC developed and documented a new POA&amp;M process that tracks all weaknesses across all bureau</p>

<sup>6</sup> FMS policy requires that POA&M items be entered within 30 days for information systems with a FIPS 199 High-impact classification.

Finding Number	Prior Year Condition	Recommendation(s)	Status
<p>Maintenance of OCC system POA&amp;M</p>	<p>and include all necessary POA&amp;M elements for an information system.</p>	<p>annual assessments, audit reports, Treasury ACIOCS reviews, or internal bureau evaluations.</p> <ol style="list-style-type: none"> <li>2. Populate the information system's POA&amp;M with the information required by Treasury and OCC.</li> <li>3. Develop and implement a training program for all individuals tasked with implementing the OCC POA&amp;M process.</li> </ol>	<p>systems and provides training on the new process.</p>
<p><b>Prior Year FY 2010 Finding #4 – a. Bureau of Public Debt</b> Incident Reporting</p>	<p>Of 13 incidents documented by BPD during the reporting period, KPMG determined that four of the incidents were not reported to Treasury Computer Security Incident response Center (TCSIRC) within the required time period.</p>	<p>We recommend that BPD Management ensure that all incidents and potential incidents are reported to TCSIRC within the required time period.</p>	<p><b>Implemented/Closed.</b> BPD updated incident response procedures to ensure time requirements were met. No incidents in FY11 were reported untimely.</p>
<p><b>Prior Year FY 2010 Finding #4 – b. Alcohol and Tobacco Tax and Trade Bureau</b> Incident Reporting</p>	<p>Of 15 incidents documented by Alcohol and Tobacco Tax and Trade Bureau (TTB) during the reporting period, KPMG determined that two of the incidents were not reported to TCSIRC within the required time period.</p>	<p>We recommend that TTB management ensure that all potential and actual security incidents are reported to TCSIRC within the required time period.</p>	<p><b>Implemented/Closed.</b> TTB updated incident response procedures to reflect Treasury defined time requirements. No incidents in FY11 were reported untimely.</p>
<p><b>Prior Year FY 2010 Finding #5 – a. Bureau of Engraving and Printing</b> The Review of Audit Logs</p>	<p>BEP did not document reviews of audit logs for the system we reviewed in accordance with NIST SPSP 800-53 and Treasury policy. The lack of monitoring and regular review of audit logs can increase the risk that unauthorized access to the information system may go undetected.</p>	<p>We recommend that BEP management develop and implement a process to review audit log information on a monthly basis for the information system that includes a requirement to document the reviews performed.</p>	<p><b>Implemented/Closed.</b> BEP performed audit log reviews and documented audit log review process.</p>
<p><b>Prior Year FY 2010 Finding #6 – a. Financial Crimes Enforcement Network</b></p>	<p>FinCEN did not adequately follow their information systems security program for media sanitization, which requires media to be physically secured when both stored and transported, and that appropriate audit trail</p>	<p>We recommend that FinCEN management:</p> <ol style="list-style-type: none"> <li>1. Secure and restrict access to media scheduled to be destroyed in accordance with their media sanitization policies.</li> </ol>	<p><b>Implemented/Closed.</b> FinCEN implemented all three recommendations by implementing a new process</p>

Finding Number	Prior Year Condition	Recommendation(s)	Status
<p>Electronic Media Destruction Process is not fully compliant with FinCEN Policy</p>	<p>records be maintained.</p>	<ol style="list-style-type: none"> <li>2. Maintain a list identifying the device, serial number, and physical location of media that is scheduled to be destroyed.</li> <li>3. Reconcile the destroyed hardware and electronic recording media with the list of items to be destroyed.</li> </ol>	<p>that included scanning, logging, and tracking the media, then storing it in the secure data center.</p>
<p><b>Prior Year FY 2010 Finding #7 – a. Bureau of Public Debt</b>                      Password Settings Were Not Properly Configured to Lockout for a BPD System</p>	<p>Administrative accounts on a BPD information system were not locked after a defined number of invalid login attempts in accordance with NIST SPSP 800-53 and system documentation.</p>	<p>BPD management updated the system configurations to remediate this finding, no recommendations were necessary.</p>	<p><b>Implemented/Closed.</b>                      BPD updated its password lockout configuration settings.</p>

**APPENDIX IV – THE DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS'S FISMA 2011 QUESTIONS FOR INSPECTORS GENERAL**

The information included in Appendix III represents the Department of the Treasury's consolidated responses to DHS's FISMA 2011 questions for Inspectors General. KPMG prepared responses to DHS questions based on an assessment of 15 information systems across 13 Treasury components, excluding the IRS and OIG. TIGTA performed audit procedures over the IRS information systems and provided their answers to the Treasury OIG and KPMG for consolidation. The information provided by TIGTA has not been subjected to KPMG audit procedures and, accordingly, we express no opinion on it.

**1: Risk Management**

Status of Risk Management Program [check one: 1.a, 1.b, 1.c]	X	<p><b>1.a.</b> The Agency has established and is maintaining a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the Office of Inspector General (OIG), the program includes the following attributes:</p> <p><b>1.a(1).</b> Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.</p> <p><b>1.a(2).</b> Addresses risk from an <i>organization</i> perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev.1</p> <p><b>1.a(3).</b> Addresses risk from a <i>mission and business process</i> perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev.1.</p> <p><b>1.a(4).</b> Addresses risk from an <i>information system</i> perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1.</p> <p><b>1.a(5).</b> Categorizes information systems in accordance with government policies.</p> <p><b>1.a(6).</b> Selects an appropriately tailored set of baseline security controls.</p> <p><b>1.a(7).</b> Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.</p> <p><b>1.a(8).</b> 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.</p> <p><b>1.a(9).</b> 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.</p> <p><b>1.a(10).</b> Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness,</p> <p><b>1.a(11).</b> Information system specific risks (tactical), mission/business specific risks and organizational-level (strategic) risks are communicated to appropriate levels of the organization.</p> <p><b>1.a(12).</b> Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., Chief Information Security Officer (CISO)).</p> <p><b>1.a(13).</b> Prescribes the active involvement of information system owners and common control providers, chief</p>
--	---	---

**1: Risk Management**

	<p>information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.</p> <p><b>1.a(14).</b> Security authorization package contains system security plan, security assessment report, and Plan of Actions and Milestones (POA&amp;M) in accordance with government policies.</p> <p><b>Comments - Treasury OIG:</b> TIGTA was still in the process of making its risk management program compliant with NIST SP 800-37 Rev.1. <i>Guide for Applying the Risk Management Framework to Federal Information Systems</i>. We also found that SSPs at FMS, DO, and Mint were not compliant with NIST SP 800-53 Rev. 3. This was not significant enough to warrant a Treasury-wide control failure. (See Findings # 3, 10)</p>
	<p><b>1.b.</b> The Agency has established and is maintaining a risk management program. However, the Agency needs to make significant improvements as noted below.</p>
<p>If 1.b. is checked above, check areas that need significant improvement:</p>	<p><b>1.b(1).</b> Risk management policy is not fully developed.</p>
	<p><b>1.b(2).</b> Risk management procedures are not fully developed, sufficiently detailed (SP 800-37, SP 800-39, SP 800-53).</p>
	<p><b>1.b(3).</b> Risk management procedures are not consistently implemented in accordance with government policies (SP 800-37, SP 800-39, SP 800-53).</p>
	<p><b>1.b(4).</b> A comprehensive governance structure and Agency-wide risk management strategy has not been fully developed in accordance with government policies (SP 800-37, SP 800-39, SP 800-53).</p>
	<p><b>1.b(5).</b> Risks from a mission and business process perspective are not addressed (SP 800-37, SP 800-39, SP 800-53).</p>
	<p><b>1.b(6).</b> Information systems are not properly categorized (FIPS 199/SP 800-60).</p>
	<p><b>1.b(7).</b> Appropriately tailored baseline security controls are not applied to information systems in accordance with government policies (FIPS 200/SP 800-53).</p>
	<p><b>1.b(8).</b> Risk assessments are not conducted in accordance with government policies (SP 800-30).</p>
	<p><b>1.b(9).</b> Security control baselines are not appropriately tailored to individual information systems in accordance with government policies (SP 800-53).</p>
	<p><b>1.b(10).</b> The communication of information system specific risks, mission/business specific risks, and organizational-level (strategic) risks to appropriate levels of the organization is not in accordance with government policies.</p>
	<p><b>1.b(11).</b> The process to assess security control effectiveness is not in accordance with government policies (SP800-53A).</p>
	<p><b>1.b(12).</b> The process to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate is not in accordance with government policies (SP 800-37).</p>
	<p><b>1.b(13).</b> The process to continuously monitor changes to information systems that may necessitate reassessment of control effectiveness is not in accordance with government policies (SP 800-37).</p>
	<p><b>1.b(14).</b> Security plan is not in accordance with government policies (SP 800-18, SP 800-37).</p>

**1: Risk Management**

	<b>1.b(15).</b> Security assessment report is not in accordance with government policies (SP 800-53A, SP 800-37).
	<b>1.b(16).</b> Accreditation boundaries for agency information systems are not defined in accordance with government policies.
	<b>1.b(17).</b> Other
	<b>1.b(17ex).</b> Explanation for Other
	<b>1.c.</b> The Agency has not established a risk management program.

**2: Configuration Management**

Status of Configuration Management Program [check one: 2.a, 2.b, 2.c]		<p><b>2.a.</b> The Agency has established and is maintaining a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>2.a(1).</b> Documented policies and procedures for configuration management.</p> <p><b>2.a(2).</b> Standard baseline configurations defined.</p> <p><b>2.a(3).</b> Assessing for compliance with baseline configurations.</p> <p><b>2.a(4).</b> Process for timely, as specified in agency policy or standards, remediation of scan result deviations.</p> <p><b>2.a(5).</b> For Windows-based components, Federal Desktop Core Configuration (FDCC)/United States Government Configuration Baseline (USGCB) secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.</p> <p><b>2.a(6).</b> Documented proposed or actual changes to hardware and software configurations.</p> <p><b>2.a(7).</b> Process for timely and secure installation of software patches.</p>
	X	<p><b>2.b.</b> The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.</p> <p><b>2.b(1).</b> Configuration management policy is not fully developed (NIST 800-53: CM-1)</p> <p><b>2.b(2).</b> Configuration management procedures are not fully developed (NIST 800-53: CM-1).</p> <p><b>2.b(3).</b> Configuration management procedures are not consistently implemented (NIST 800-53: CM-1).</p> <p><b>Comments - TIGTA:</b> In March 2011, the Government Accountability Office (GAO-11-308) reported that the IRS had newly identified and unresolved weaknesses related configuration management that continue to jeopardize the confidentiality, integrity, and availability of the financial and sensitive taxpayer information processed by the IRS's systems.</p> <p><b>2.b(4).</b> Standard baseline configurations are not identified for software components (NIST 800-53: CM-2).</p>
If 2.b. is checked above, check areas that need significant improvement:	X	<p><b>Comments - Treasury OIG:</b> TIGTA did not identify standard baseline configurations for all software components. (See Finding # 12)</p>

**2: Configuration Management**

X	<p><b>2.b(5).</b> Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).  <b>Comments - Treasury OIG:</b> Standard baseline configurations were not identified for all hardware at TIGTA. (See Finding # 12)</p>
X	<p><b>2.b(6).</b> Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).  <b>Comments - Treasury OIG:</b> TIGTA did not fully implement standard baseline configurations. (See Finding # 12)  <b>Comments - TIGTA:</b> To correct configuration management deficiencies, the IRS is in the process of implementing an Enterprise Configuration Management System, with planning dates through Fiscal Year 2014, which will provide oversight and enforcement of configuration and change management processes.</p>
X	<p><b>2.b(7).</b> FDCC/USGCB is not fully implemented (OMB) and/or all deviations are not fully documented (NIST 800-53: CM-6).  <b>Comments - Treasury OIG:</b> A DO system did not implement FDCC configurations for its desktops or obtain a waiver to implement a different standard. (See Finding # 12)</p>
X	<p><b>2.b(8).</b> Software assessing (scanning) capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).  <b>Comments - Treasury OIG:</b> The CDFI Fund had a contractor-operated system that was not scanned according to NIST and FISMA requirements. (See Finding # 7)</p>
X	<p><b>Comments - TIGTA:</b> In May 2011, TIGTA reported (Reference Number 2011-20-044) that the IRS had not fully implemented its plans to complete vulnerability scans of databases within its enterprise.  <b>2.b(9).</b> Configuration-related vulnerabilities, including scan findings, have not been remediated in a timely manner, as specified in agency policy or standards (NIST 800-53: CM-4, CM-6, RA-5, SI-2).  <b>Comments - Treasury OIG:</b> OTS ran a system on an unsupported operating system, but the system was upgraded to a newer operating system after auditor notification. A DO system had vulnerabilities that were not remediated timely. (See Findings # 7, 9)</p>
X	<p><b>Comments - TIGTA:</b> The IRS has been unable to establish an enterprise-wide process for timely remediation of weaknesses reported by vulnerabilities scans because of the limited information it gets from the scan results.  <b>2.b(10).</b> Patch management process is not fully developed, as specified in agency policy or standards (NIST 800-53: CM-3, SI-2).  <b>Comments - TIGTA:</b> In May 2011, the TIGTA reported (Reference Number 2011-20-044) that</p>

**2: Configuration Management**

	nonmainframe databases containing taxpayer data were not always configured in a secure manner and were running out-of-date software that no longer received security patches and other vendor support.
	<b>2.b(11).</b> Other
	<b>2.b(11ex).</b> Explanation for Other:
	<b>2.c.</b> The Agency has not established a security configuration management program.

**3: Incident Response and Reporting**

Status of Incident Response & Reporting Program [check one: 3.a, 3.b, 3.c]	<b>3.a.</b> The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: <b>3.a(1).</b> Documented policies and procedures for detecting, responding to, and reporting incidents. <b>3.a(2).</b> Comprehensive analysis, validation and documentation of incidents. <b>3.a(3).</b> When applicable, reports to United States Computer Emergency Response Team (US-CERT) within established time frames. <b>3.a(4).</b> When applicable, reports to law enforcement within established time frames. <b>3.a(5).</b> Responds to and resolves incidents in a timely manner, as specified in agency policy or standards, to minimize further damage. <b>3.a(6).</b> Is capable of tracking and managing risks in a virtual/cloud environment, if applicable. <b>3.a(7).</b> Is capable of correlating incidents.
	<b>3.b.</b> The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below.
If 3.b. is checked above, check areas that need significant improvement:	<b>3.b(1).</b> Incident response and reporting policy is not fully developed (NIST 800-53: IR-1). <b>3.b(2).</b> Incident response and reporting procedures are not fully developed or sufficiently detailed (NIST 800-53: IR-1). <b>3.b(3).</b> Incident response and reporting procedures are not consistently implemented in accordance with government policies (NIST 800-61, Rev 1). <b>3.b(4).</b> Incidents were not identified in a timely manner, as specified in agency policy or standards (NIST 800-53, 800-61, and OMB M-07-16, M-06-19). <b>3.b(5).</b> Incidents were not reported to the US-CERT as required (NIST 800-53, 800-61 and OMB M-07-16, M-06-19). <b>Comments – Treasury OIG:</b> See 3.b(12ex) (See Finding # 2) <b>3.b(6).</b> Incidents were not reported to law enforcement as required (SP 800-86). <b>3.b(7).</b> Incidents were not resolved in a timely manner (NIST 800-53, 800-61 and OMB M-07-16, M-06-19). <b>3.b(8).</b> Incidents were not resolved to minimize further damage (NIST 800-53, 800-61 and OMB M-07-16, M-

**3: Incident Response and Reporting**

	06-19).
	<b>3.b(9).</b> There is insufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61 and OMB M-07-16, M-06-19).
	<b>3.b(10).</b> The agency cannot or is not prepared to track and manage incidents in a virtual/cloud environment.
	<b>3.b(11).</b> The agency does not have the technical capability to correlate incident events.
	<b>3.b(12).</b> Other
X	<b>Comments - Treasury OIG:</b> Unimely Incident Reporting (See Finding # 2) <b>3.b(12ex).</b> Explanation for Other:
	<b>Comments - Treasury OIG:</b> The CDFI Fund did not report 1 of 1 security incident within the time frame. DO did not report 1 of 15 sampled incidents within the time frame. FMS did not report 7 of 10 incidents within the time frame. Mint did not report 1 of 15 sampled incidents within the time frame. TIGTA did not report 1 of 13 incidents within the required time frame. (See Finding #2)
	<b>3.c.</b> The Agency has not established an incident response and reporting program.
Comments:	

**4: Security Training**

Status of Security Training Program [check one: 4.a, 4.b, 4.c]		<p><b>4.a.</b> The Agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>4.a(1).</b> Documented policies and procedures for security awareness training.</p> <p><b>4.a(2).</b> Documented policies and procedures for specialized training for users with significant information security responsibilities.</p> <p><b>4.a(3).</b> Security training content based on the organization and roles, as specified in agency policy or standards.</p> <p><b>4.a(4).</b> Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other agency users) with access privileges that require security awareness training.</p> <p><b>4.a(5).</b> Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other agency users) with significant information security responsibilities that require specialized training.</p>
	X	<p><b>4.b.</b> The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below.</p> <p><b>4.b(1).</b> Security awareness training policy is not fully developed (NIST 800-53: AT-1).</p> <p><b>4.b(2).</b> Security awareness training procedures are not fully developed and sufficiently detailed (NIST 800-53: AT-1).</p> <p><b>4.b(3).</b> Security awareness training procedures are not consistently implemented in accordance with government policies (NIST 800-53: AT-2).</p>
If 4. b. is checked above, check areas that need significant improvement:		

**4: Security Training**

	<p><b>4.b(4).</b> Specialized security training policy is not fully developed (NIST 800-53: AT-3).</p> <p><b>4.b(5).</b> Specialized security training procedures are not fully developed or sufficiently detailed in accordance with government policies (SP 800-50, SP 800-53).</p> <p><b>4.b(6).</b> Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).</p> <p><b>4.b(7).</b> Identification and tracking of the status of security awareness training for personnel (including employees, contractors, and other agency users) with access privileges that require security awareness training is not adequate in accordance with government policies (SP 800-50, SP 800-53).</p> <p><b>4.b(8).</b> Identification and tracking of the status of specialized training for personnel (including employees, contractors, and other agency users) with significant information security responsibilities is not adequate in accordance with government policies (SP 800-50, SP 800-53).</p>
X	<p><b>Comments - TIGTA:</b> In June 2011, the TIGTA reported (Reference Number 2011-20-060) that the IRS was unable to track whether employees with disaster recovery roles attend required annual disaster recovery training. The IRS plans to develop a process for identifying and tracking the completion of training for employees with disaster recovery roles by December 31, 2011. In addition, the IRS did not identify or track contractors that require specialized training for the Fiscal Year 2011 FISMA year, but plans to begin collecting and tracking information on contractor completion of specialized training for the Fiscal Year 2012 FISMA year. Contractors will self identify and report the completion of specialized training where required and provide these data to the IRS.</p> <p><b>4.b(9).</b> Training content for individuals with significant information security responsibilities is not adequate in accordance with government policies (SP 800-53, SP 800-16).</p> <p><b>4.b(10).</b> Less than 90% of personnel (including employees, contractors, and other agency users) with access privileges completed security awareness training in the past year.</p> <p><b>4.b(11).</b> Less than 90% of employees, contractors, and other users with significant security responsibilities completed specialized security awareness training in the past year.</p> <p><b>4.b(12).</b> Other</p> <p><b>4.b(12ex).</b> Explanation for Other</p>
	<p><b>4.c.</b> The Agency has not established a security training program.</p>

**5: POA&M**

<p>Status of Plan of Action &amp; Milestones (POA&amp;M) Program [check one: 5.a, 5.b, 5.c]</p>		<p><b>5.a.</b> The Agency has established and is maintaining a POA&amp;M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <ul style="list-style-type: none"> <li><b>5.a(1).</b> Documented policies and procedures for managing Information Technology (IT) security weaknesses discovered during security control assessments and requiring remediation.</li> <li><b>5.a(2).</b> Tracks, prioritizes and remediates weaknesses.</li> <li><b>5.a(3).</b> Ensures remediation plans are effective for correcting weaknesses.</li> <li><b>5.a(4).</b> Establishes and adheres to milestone remediation dates.</li> <li><b>5.a(5).</b> Ensures resources are provided for correcting weaknesses.</li> <li><b>5.a(6).</b> Program officials and contractors report progress on remediation to the Chief Information Officer (CIO) on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&amp;M activities at least quarterly.</li> </ul>
	X	<p><b>5.b.</b> The Agency has established and is maintaining a POA&amp;M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.</p>
<p>If 5.b. is checked above, check areas that need significant improvement:</p>		<p><b>5.b(1).</b> POA&amp;M Policy is not fully developed.</p>
		<p><b>5.b(2).</b> POA&amp;M procedures are not fully developed and sufficiently detailed.</p>
	X	<p><b>5.b(3).</b> POA&amp;M procedures are not consistently implemented in accordance with government policies.</p> <p><b>Comments – Treasury OIG:</b> FMS did not record and update security vulnerabilities timely. (See Finding # 6)</p>
		<p><b>5.b(4).</b> POA&amp;Ms do not include security weaknesses discovered during assessments of security controls and requiring remediation (OMB M-04-25).</p>
	X	<p><b>Comments - Treasury OIG:</b> OTS did not include an out of date operating systems in their POA&amp;M despite this vulnerability being well known for several months by system administrators. One FMS system POA&amp;M did not include five high-risk vulnerabilities identified in the March 2011 and June 2011 vulnerability scans. (See Finding # 6)</p>
	X	<p><b>5.b(5).</b> Remediation actions do not sufficiently address weaknesses in accordance with government policies (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls).</p>
		<p><b>Comments – Treasury OIG:</b> See 5.b(8) (See Finding # 6)</p>
		<p><b>5.b(6).</b> Source of security weaknesses are not tracked (OMB M-04-25).</p>
		<p><b>5.b(7).</b> Security weaknesses are not appropriately prioritized (OMB M-04-25).</p>

**5: POA&M**

		<p><b>5.b(8).</b> Milestone dates are not adhered to (OMB M-04-25).</p> <p><b>Comments - Treasury OIG:</b> At FMS, one POA&amp;M identified two high-impact vulnerabilities from the Fiscal Year 2009 security assessment that were marked as Delayed and two years overdue without an updated completion date. Another POA&amp;M did not provide justification for the delayed security weaknesses. Eight POA&amp;M items from one system and five POA&amp;M items from a second were marked as Delayed without an updated completion date. (See Finding # 6)</p> <p><b>5.b(9).</b> Initial target remediation dates are frequently missed (OMB M-04-25).</p> <p><b>5.b(10).</b> POA&amp;Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).</p> <p><b>5.b(11).</b> Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25).</p>
X		<p><b>Comments - TIGTA:</b> Of the 10 IRS systems selected for the Fiscal Year 2011 FISMA evaluation, 13 (39 percent) of 33 closed weaknesses and 24 (31 percent) of 77 open weaknesses, maintained in the systems' Fiscal Year 2011 POA&amp;Ms, did not have costs associated with remediating the weaknesses in accordance with IRS policy. (See Finding # 6)</p> <p><b>5.b(12).</b> Agency CIO does not track and review POA&amp;Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).</p> <p><b>5.b(13).</b> Other</p> <p><b>5.b(13ex).</b> Explanation for Other</p>
		<p><b>5.c.</b> The Agency has not established a POA&amp;M program.</p>
<p>Comments:</p>		

**6: Remote Access Management**

<p>Status of Remote Access Management Program [check one: 6.a, 6.b, 6.c]</p>	X	<p><b>6.a.</b> The Agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>6.a(1).</b> Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.</p> <p><b>6.a(2).</b> Protects against unauthorized connections or subversion of authorized connections.</p> <p><b>6.a(3).</b> Users are uniquely identified and authenticated for all access.</p> <p><b>6.a(4).</b> If applicable, multifactor authentication is required for remote access.</p> <p><b>6.a(5).</b> Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.</p> <p><b>6.a(6).</b> Defines and implements encryption requirements for information transmitted across public networks.</p> <p><b>6.a(7).</b> Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity</p>

**6: Remote Access Management**

	<p>after which reauthentication is required.</p>
<p>If 6.b. is checked above, check areas that need significant improvement:</p>	<p><b>6.b.</b> The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.</p> <p><b>6.b(1).</b> Remote access policy is not fully developed (NIST 800-53: AC-1, AC-17).</p> <p><b>6.b(2).</b> Remote access procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1, AC-17).</p> <p><b>6.b(3).</b> Remote access procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-1, AC-17).</p> <p><b>6.b(4).</b> Telecommuting policy is not fully developed (NIST 800-46, Section 5.1).</p> <p><b>6.b(5).</b> Telecommuting procedures are not fully developed or sufficiently detailed in accordance with government policies (NIST 800-46, Section 5.4).</p> <p><b>6.b(6).</b> Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, Section 5.1).</p> <p><b>6.b(7).</b> Multifactor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).</p> <p><b>6.b(8).</b> Agency has not identified all remote devices (NIST 800-46, Section 2.1).</p> <p><b>6.b(9).</b> Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46, Section 3.1 and 4.2).</p> <p><b>6.b(10).</b> Agency does not adequately monitor remote devices when connected to the 'agency's networks remotely in accordance with government policies (NIST 800-46, Section 3.2).</p> <p><b>6.b(11).</b> Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).</p> <p><b>6.b(12).</b> Remote access rules of behavior are not adequate in accordance with government policies (NIST 800-53, PL-4).</p> <p><b>6.b(13).</b> Remote access user agreements are not adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6).</p> <p><b>6.b(14).</b> Other</p> <p><b>6.b(14ex).</b> Explanation for Other</p> <p><b>6.c.</b> The Agency has not established a program for providing secure remote access.</p>

**7: Identity and Access Management**

<p>Status of Account and Identity Management Program [check one: 7.a, 7.b, 7.c]</p>		<p><b>7.a.</b> The Agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>7.a(1).</b> Documented policies and procedures for account and identity management.</p> <p><b>7.a(2).</b> Identifies all users, including Federal employees, contractors, and others who access Agency systems.</p> <p><b>7.a(3).</b> Identifies when special access requirements (e.g., multifactor authentication) are necessary.</p> <p><b>7.a(4).</b> If multifactor authentication is in use, it is linked to the Agency's Personal Identity Verification (PIV) program where appropriate.</p> <p><b>7.a(5).</b> Ensures that the users are granted access based on needs and separation of duties principles.</p> <p><b>7.a(6).</b> Identifies devices that are attached to the network and distinguishes these devices from users.</p> <p><b>7.a(7).</b> Ensures that accounts are terminated or deactivated once access is no longer required.</p> <p><b>7.a(8).</b> Identifies and controls use of shared accounts.</p>
	X	<p><b>7.b.</b> The Agency has established and is maintaining an identity and access management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.</p>
<p>If 7.b. is checked above, check areas that need significant improvement:</p>	X	<p><b>7.b(1).</b> Account management policy is not fully developed (NIST 800-53: AC-1).</p> <p><b>7.b(2).</b> Account management procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1).</p>
		<p><b>Comments - Treasury OIG:</b> DO lacked an account management process for one system; TIGTA lacked documentation for some account management activities. (See Finding # 1)</p>
		<p><b>7.b(3).</b> Account management procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-2).</p>
	X	<p><b>Comments - Treasury OIG:</b> Account management procedures were not consistently implemented for systems at DO, FMS, OCC, and OTS. (See Finding # 1)</p>
		<p><b>Comments - TIGTA:</b> In March 2011, the Government Accountability Office (GAO-11-308) reported that the IRS had newly identified and unresolved weaknesses related access controls that continue to jeopardize the confidentiality, integrity, and availability of the financial and sensitive taxpayer information processed by the IRS's systems. Our review of the 10 IRS systems selected for the Fiscal Year 2011 FISMA evaluation found that all systems needed improvement in implementing NIST baseline access controls and identity and authentication controls.</p>
		<p><b>7.b(4).</b> Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).</p>
		<p><b>7.b(5).</b> Accounts are not properly issued to new users (NIST 800-53, AC-2).</p>
	X	<p><b>Comments - Treasury OIG:</b> OCC did not have documented approval for new accounts for one system. (See Finding # 1)</p>

**7: Identity and Access Management**

X	<p><b>7.b(6).</b> Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).</p> <p><b>Comments - Treasury OIG:</b> FMS did not deactivate inactive accounts for one system. (See Finding #1)</p> <p><b>Comments - TIGTA:</b> In May 2011, the TIGTA reported (Reference Number 2011-20-046) that user accounts on the bankruptcy case tracking system were not properly terminated when users no longer required access.</p> <p><b>7.b(7).</b> Agency does not use multifactor authentication where required (NIST 800-53, IA-2).</p> <p><b>7.b(8).</b> Agency has not adequately planned for implementation of PIV for logical access in accordance with government policies (Homeland Security Presidential Directive (HSPD) 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).</p> <p><b>7.b(9).</b> Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).</p>
X	<p><b>Comments - Treasury OIG:</b> OTS did not review system and administrator accounts for one system. (See Finding # 1)</p> <p><b>Comments - TIGTA:</b> In May 2011, the TIGTA reported (Reference Number 2011-20-046) that access controls had not been implemented or were not operating effectively on an IRS bankruptcy case tracking system, on which many IRS employees had excessive privileges.</p> <p><b>7.b(10).</b> Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).</p> <p><b>7.b(11).</b> Network devices are not properly authenticated (NIST 800-53, IA-3).</p> <p><b>7.b(12).</b> The process for requesting or approving membership in shared privileged accounts is not adequate in accordance to government policies.</p> <p><b>7.b(13).</b> Use of shared privileged accounts is not necessary or justified.</p> <p><b>7.b(14).</b> When shared accounts are used, the Agency does not renew shared account credentials when a member leaves the group.</p> <p><b>7.b(15).</b> Other</p> <p><b>7.b(15ex).</b> Explanation for Other</p> <p><b>7.c.</b> The Agency has not established an identity and access management program.</p>

**8: Continuous Monitoring Management**

Status of Continuous Monitoring Program [check one: 8.a, 8.b, 8.c]	X	<p><b>8.a.</b> The Agency has 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. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>8.a(1).</b> Documented policies and procedures for continuous monitoring.</p> <p><b>8.a(2).</b> Documented strategy and plans for continuous monitoring.</p> <p><b>8.a(3).</b> Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.</p> <p><b>8.a(4).</b> Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&amp;M additions and updates with the frequency defined in the strategy and/or plans.</p>
		<p><b>8.b.</b> The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.</p>
If 8.b. is checked above, check areas that need significant improvement:		<p><b>8.b(1).</b> Continuous monitoring policy is not fully developed (NIST 800-53: CA-7).</p>
		<p><b>8.b(2).</b> Continuous monitoring procedures are not fully developed (NIST 800-53: CA-7).</p>
		<p><b>8.b(3).</b> Continuous monitoring procedures are not consistently implemented (NIST 800-53: CA-7; 800-37 Rev 1, Appendix G).</p>
		<p><b>8.b(4).</b> Strategy or plan has not been fully developed for enterprise-wide continuous monitoring (NIST 800-37 Rev 1, Appendix G).</p>
		<p><b>8.b(5).</b> Ongoing assessments of security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).</p>
		<p><b>8.b(6).</b> The following were not provided to the authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&amp;Ms (NIST 800-53, NIST 800-53A).</p>
		<p><b>8.b(7).</b> Other</p>
		<p><b>8.b(7ex).</b> Explanation for Other</p>
		<p><b>8.c.</b> The Agency has not established a continuous monitoring program.</p>

**9: Contingency Planning**

<p>Status of Contingency Planning Program [check one: 9.a, 9.b, 9.c]</p>		<p><b>9.a.</b> The Agency established and is maintaining an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:  <b>9.a(1).</b> Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.  <b>9.a(2).</b> The agency has performed an overall Business Impact Analysis (BIA).  <b>9.a(3).</b> Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.  <b>9.a(4).</b> Testing of system specific contingency plans.  <b>9.a(5).</b> The documented business continuity and disaster recovery plans are in place and can be implemented when necessary.  <b>9.a(6).</b> Development of test, training, and exercise (TT&amp;E) programs.  <b>9.a(7).</b> Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans.</p>
	X	<p><b>9.b.</b> The Agency has established and is maintaining an enterprise-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.</p>
<p>If 9.b. is checked above, check areas that need significant improvement:</p>		<p><b>9.b(1).</b> Contingency planning policy is not fully developed contingency planning policy is not consistently implemented (NIST 800-53: CP-1).</p>
		<p><b>9.b(2).</b> Contingency planning procedures are not fully developed (NIST 800-53: CP-1).</p>
		<p><b>9.b(3).</b> Contingency planning procedures are not consistently implemented (NIST 800-53; 800-34).</p>
		<p><b>9.b(4).</b> An overall business impact assessment has not been performed (NIST SP 800-34).</p>
		<p><b>9.b(5).</b> Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).</p>
		<p><b>9.b(6).</b> A business continuity/disaster recovery plan has not been developed (FCDI, NIST SP 800-34).</p>
		<p><b>9.b(7).</b> A business continuity/disaster recovery plan has been developed but not fully implemented (FCDI, NIST SP 800-34).</p>
		<p><b>9.b(8).</b> System contingency plans missing or incomplete (FCDI, NIST SP 800-34, NIST SP 800-53).</p>
	X	<p><b>Comments - Treasury OIG:</b> TIGTA did not have a new operating system integrated into its contingency plan, though there were plans to add the information to the contingency plan. (See Finding # 8)</p>
	X	<p><b>Comments - Treasury OIG:</b> At FMS, a full recovery and reconstitution of the information system was not completed at the alternate recovery site for a Critical Infrastructure Protection (CIP) and FIPS 199 "high-impact" system in accordance with FMS policy and NIST SP 800-53 Rev. 3 security controls. The new CIP system only underwent a tabletop disaster recovery test during the Fiscal Years 2011 and 2010. (See Finding # 8)</p>

**9: Contingency Planning**

	<p><b>9.b(10).</b> Test, training, and exercise programs have not been developed (FCDI, NIST SP 800-34, NIST 800-53).</p> <p><b>9.b(11).</b> Test, training, and exercise programs have been developed, but are not fully implemented (FCDI, NIST SP 800-34, NIST SP 800-53).</p> <p><b>9.b(12).</b> After-action report did not address issues identified during contingency/disaster recovery exercises (FCDI, NIST SP 800-34).</p> <p><b>9.b(13).</b> Systems do not have alternate processing sites (FCDI, NIST SP 800-34, NIST SP 800-53).</p> <p><b>9.b(14).</b> Alternate processing sites are subject to the same risks as primary sites (FCDI, NIST SP 800-34, NIST SP 800-53).</p> <p><b>9.b(15).</b> Backups of information are not performed in a timely manner (FCDI, NIST SP 800-34, NIST SP 800-53).</p> <p><b>Comments - Treasury OIG:</b> One DO system did not create system backups regularly. Another DO system did not backup system configuration information. (See Finding # 8)</p> <p><b>9.b(16).</b> Backups are not appropriately tested (FCDI, NIST SP 800-34, NIST SP 800-53).</p> <p><b>Comments - Treasury OIG:</b> One DO system did not appropriately test backups on tape. TTB did not create and test backup tapes on a regular basis. (See Finding # 8)</p> <p><b>9.b(17).</b> Backups are not properly secured and protected (FCDI, NIST SP 800-34, NIST SP 800-53).</p> <p><b>9.b(18).</b> Contingency planning does not consider supply chain threats.</p> <p><b>9.b(19).</b> Other</p> <p><b>9.b(19ex).</b> Explanation for Other</p> <p><b>9.c.</b> The Agency has not established a business continuity/disaster recovery program.</p>
X	
X	

**10: Contractor Systems**

<p>Status of Agency Program to Oversee Contractor Systems [check one: 10.a, 10.b, 10.c]</p>	<p>X</p>	<p><b>10.a.</b> The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>10.a(1).</b> Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.</p> <p><b>10.a(2).</b> The Agency obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and agency guidelines.</p> <p><b>10.a(3).</b> A complete inventory of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.</p> <p><b>10.a(4).</b> The inventory identifies interfaces between these systems and Agency-operated systems.</p> <p><b>10.a(5).</b> The agency requires appropriate agreements (e.g., Memoranda of Understanding (MOUs), Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.</p> <p><b>10.a(6).</b> The inventory of contractor systems is updated at least annually.</p> <p><b>10.a(7).</b> Systems that are owned or operated by contractors or entities, including Agency systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.</p> <p><b>Comments - Treasury OIG:</b> The CDFI Fund had a contractor-operated system that was not scanned according to NIST and FISMA requirements. (See Finding # 7)</p>
<p>If 10.b. is checked above, check areas that need significant improvement:</p>		<p><b>10.b.</b> The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in public cloud. However, the Agency needs to make significant improvements as noted below.</p> <p><b>10.b(1).</b> Policies to oversee systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud, are not fully developed.</p> <p><b>10.b(2).</b> Procedures to oversee systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud, are not fully developed.</p> <p><b>10.b(3).</b> Procedures to oversee systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud are not consistently implemented.</p> <p><b>10.b(4).</b> The inventory of systems owned or operated by contractors or other entities, including Agency systems and services residing in public cloud, is not complete in accordance with government policies (NIST 800-53; PM-5).</p> <p><b>10.b(5).</b> The inventory does not identify interfaces between contractor/entity-operated systems to Agency owned and operated systems.</p> <p><b>10.b(6).</b> The inventory of contractor/entity-operated systems, including interfaces, is not updated at least annually.</p>

**10: Contractor Systems**

		<b>10.b(7)</b> . Systems owned or operated by contractors and entities are not subject to NIST and OMB's FISMA requirements (e.g., security requirements).
		<b>10.b(8)</b> . Systems owned or operated by contractor's and entities do not meet NIST and OMB's FISMA requirements (e.g., security requirements).
		<b>10.b(9)</b> . Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained.
		<b>10.b(10)</b> . Other
		<b>10.b(10ex)</b> . Explanation for Other:
		<b>10.c</b> . The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in public cloud.

**11: Security Capital Planning**

Status of Agency Program to Oversee Security Capital Planning [check one: 11.a, 11.b, 11.c]	X	<b>11.a</b> . The Agency has established and maintains a security capital planning and investment program for information security. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: <b>11.a(1)</b> . Documented policies and procedures to address information security in the capital planning and investment control process. <b>11.a(2)</b> . Includes information security requirements as part of the capital planning and investment process. <b>11.a(3)</b> . Establishes a discrete line item for information security in organizational programming and documentation. <b>11.a(4)</b> . Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required. <b>11.a(5)</b> . Ensures that information security resources are available for expenditure as planned.
		<b>11.b</b> . The Agency has established and maintains a capital planning and investment program. However, the Agency needs to make significant improvements as noted below.
If 11.b. is checked above, check areas that need significant improvement:		<b>11.b(1)</b> . Capital Planning and Investment Control (CPIC) information security policy is not fully developed.
		<b>11.b(2)</b> . CPIC information security procedures are not fully developed.
		<b>11.b(3)</b> . CPIC information security procedures are not consistently implemented.
		<b>11.b(4)</b> . The Agency does not adequately plan for IT security during the CPIC process (SP 800-65).
		<b>11.b(5)</b> . The Agency does not include a separate line for information security in appropriate documentation (NIST 800-53: SA-2).
		<b>11.b(6)</b> . Exhibits 300/53 or business cases do not adequately address or identify information security costs (NIST 800-53: PM-3).
		<b>11.b(7)</b> . The Agency does not provide IT security funding to maintain the security levels identified.
		<b>11.b(8)</b> . Other
		<b>11.b(8ex)</b> . Explanation for Other
		<b>11.c</b> . The Agency does not have a capital planning and investment program.

**APPENDIX V – APPROACH TO SELECTION OF SUBSET OF SYSTEMS**

In Fiscal Year (FY) 2011, KPMG employed a risk-based approach to select a representative subset of United States Department of the Treasury (Treasury) information systems for the Federal Information Security Management Act (FISMA) audit. KPMG used the system inventory contained within Treasury’s Trusted Agent FISMA (TAF) to identify the population and stratified the population by bureau and office to select a representative subset of non-IRS Treasury applications. KPMG performed procedures throughout the fieldwork phase to determine the completeness and accuracy of the non-IRS Treasury inventory of information systems.

As agreed with the Treasury OIG, KPMG selected 15 information systems for the FY 2011 FISMA audit. KPMG selected the representative subset of non-IRS information systems from TAF on May 11, 2011, prior to the Treasury’s FISMA year-end on June 30, 2011. This advanced selection allowed us time to complete planning and prepare for the fieldwork phase, which commenced immediately after Treasury’s FISMA year-end.

In selecting the subset, we stratified the full population of Treasury major applications and general support systems by bureau and by Federal Information Processing Standards (FIPS) 199 system impact level. KPMG used a risk-based approach to select systems out of each stratum. KPMG considered the following factors to select systems:

- Total number of systems per bureau;
- Systems at smaller bureaus not historically included in FISMA audits or evaluations;
- Number of systems at each bureau with a FIPS system impact level of “High”;
- Location of the system;
- Whether the system is going to be decommissioned prior to December 31, 2011; and
- Whether the system was identified in a previous FISMA audits or evaluations within the past two years.

Lastly, the total number of financial systems selected in the representative subset did not exceed the percentage of systems the financial systems represent in the Treasury inventory of information systems. KPMG defined financial systems as those information systems designated as “Financial” or “Mixed Financial” systems in the Treasury’s TAF system.

Based on our analysis of the Treasury inventory of information systems as of May 11, 2011, we noted Treasury’s inventory included 192 major applications and general support systems. The following table provides our analysis of the composition of the Treasury’s inventory of major applications and general support systems.

	<b>Total</b>	<b>IRS</b>	<b>Non-IRS</b>	<b>Non-IRS Financial Systems</b>
<b>Major Applications</b>	132	51	32	49
<b>General Support Systems</b>	60	24	4	32
<b>Total</b>	192	75	36	81

From the analysis above, we determined that IRS systems comprised 39 percent of the total population of Major Applications and General Support systems, and Non-IRS systems accounted for 61 percent. Applying the subset size percentage of 13 percent to the total population of 192 yielded a total subset size

of 25 systems. When the IRS to Non-IRS weighting was applied to this total, the resulting sizes for the IRS and Non-IRS subsets were 10 and 15, respectively.

KPMG considered the ratio of Major Applications and General Support Systems as well as the ratio of financial to nonfinancial information systems to help determine what systems to select for review. Considering these ratios, we judgmentally selected a representative subset of information systems for testing during the 2011 FISMA audit. Based on these factors, KPMG determined the following composition for the representative subset of Non-IRS Major Applications and General Support Systems for the FY 2011 FISMA audit:

<b>Total Selected</b>	15
<b>Total Major Applications</b>	10
<b>Total General Support Systems</b>	5
<b>Total Systems with a FIPS 199 System Impact Level of “High”</b>	4
<b>Total Systems with a FIPS 199 System Impact Level of “Moderate”</b>	11
<b>Total Systems with a FIPS 199 System Impact Level of “Low”</b>	0
<b>Total Systems Designated as Financial</b>	7

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

<b>Bureau</b>	<b>Total Systems</b>	<b>Percentage of Total Non-IRS Population</b>	<b>Total Number of Non-IRS Systems to be Selected</b>
<b>BEP</b>	6	5%	1
<b>BPD</b>	14	12%	1
<b>CDFI Fund</b>	3	3%	1 (see note 1)
<b>DO</b>	22	19%	3
<b>FinCEN</b>	6	5%	1
<b>FMS</b>	34	29%	3
<b>Mint</b>	10	8%	1
<b>OCC</b>	8	7%	1
<b>OIG</b>	1	1%	0 (see note 2)
<b>OTS</b>	8	7%	1
<b>TIGTA</b>	2	2%	1 (see notes 1 and 2)
<b>TTB</b>	3	2%	1 (see note 1)
<b>Total</b>	117	100%	15

(**Note 1:** Using the stratification methodology, we initially did not select a system at these agencies. However, using our risk-based methodology, we selected at least one system for each of these bureaus.)

(**Note 2:** The OIG guided KPMG to inspect only one OIG information system every year. In FY 2011 TIGTA was selected because the OIG was selected in FY2010.)

**APPENDIX VI – SELECTED SECURITY CONTROL CLASSES AND FAMILIES**

Federal Information Security Management Act (FISMA) directs the National Institute of Standards and Technology (NIST) to develop and issue standards, guidelines, and other publications to assist federal agencies in defining minimum security requirements for non-national security systems used by agencies. NIST has developed such standards and guidelines as part of its implementation of FISMA. KPMG based its security evaluation on the security controls defined within NIST Special Publication (SP) 800-53 Rev. 3, *Recommended Security Control for the Federal Information Systems and Organizations*. NIST publications define a framework for protecting the confidentiality, integrity, and availability of federal information and information systems consisting of three general classes of controls (i.e., management, operational, and technical).

Tables on the following pages delineate the specific security controls we performed in accordance with NIST SPSP 800-53. KPMG selected specific test procedures that were applicable to the computing environment; therefore, not all available security controls within each control family were performed.

**Management Controls**

Management security controls for information systems focus on the management of risk and the management of information system security.

KPMG assessed the following management control areas:

- Security Assessments and Authorizations (CA)
- Planning (PL)
- Risk Assessment (RA)

*Security Assessments and Authorization:*

The organization develops, disseminates, and periodically reviews/updates (i) formal, documented, security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated assessment and authorization controls.

Security Controls	Title
CA-2	Security Assessments
CA-5	Plan of Action and Milestone
CA-6	Security Authorization
CA-7	Continuous Monitoring

*Planning:*

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Procedure	Title
PL-2	System Security Plan

*Risk Assessment:*

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented risk assessment policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Procedure	Title
RA-2	Security Categorization
RA-3	Risk Assessment
RA-5	Vulnerability Scanning

**Operational Controls**

The operational controls address security methods that focus primarily on mechanisms that people implement and execute (as opposed to systems).

KPMG assessed the following Operational control areas:

- Configuration Management (CM)
- Contingency Planning (CP)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Personnel Security (PS)
- System and Information Integrity (SI)

*Configuration Management:*

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, configuration management policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Procedure	Title
CM-2	Baseline Configuration
CM-6	Configuration Settings

*Contingency Planning:*

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, contingency planning policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Procedure	Title
CP-2	Contingency Plan
CP-4	Contingency Plan Testing and Exercises
CP-9	Information System Backup

*Media Protection:*

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, information system media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of the information system media protection policy and associated system media protection controls.

Procedure	Title
MP-6	Media Sanitization and Disposal

*Physical and Environmental Protection:*

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, information system physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of the information system physical and environmental protection policy and associated system physical and environmental protection controls.

Procedure	Title
PE-7	Visitor Control

*Personnel Security:*

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, physical security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of the physical security policy and associated personnel security controls.

Procedure	Title
PS-4	Personnel Termination

*System and Information Integrity:*

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of system and information integrity policy and associated system and information integrity controls.

Procedure	Title
SI-2	Flaw Remediation

## Technical Controls

Technical security controls for information systems focus on information systems that primarily control the implementation and execution of the information system through mechanisms contained in the hardware, software, or firmware of the system.

KPMG assessed the following Technical control areas:

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)
- System and Communication Protection (SC)

### *Access Control:*

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, access control policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Procedure	Title
AC-2	Account Management
AC-5	Separation of Duties

### *Audit and Accountability:*

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, audit and accountability policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Procedure	Title
AU-2	Auditable Events
AU-12	Audit Generation

### *Identification and Authentication:*

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, identification and authentication policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Procedure	Title
IA-2	User Identification and Authentication
IA-3	Device Identification and Authentication

*System and Communication Protection:*

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, system and communications protection policy that addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Procedure	Title
SC-13	Use of Cryptography

**APPENDIX VII – SUMMARY OF OTHER IT FINDINGS FROM TREASURY FINANCIAL STATEMENT AUDITS**

Treasury Management will provide responses to the security weakness noted below in a separate report as part of the financial statement audit.

NIST 800-53 Control Family	Condition	Recommendation
Access Control	<p>FMS has granted user accounts with excessive access to systems that support the payment functions of FMS, and thus did not adhere to the FMS and Department of Treasury principles of least privileges. Specifically, configuration weaknesses permitted updates to payment and system program files. While we observed improvements and further restrictions of access from 2010 to 2011, further work is necessary to properly secure payment files, control batch job submissions, and improve the user account recertification process.</p>	<p>We recommend that FMS Management continue to execute their planned corrective action steps to fully address the following recommendations:</p> <ol style="list-style-type: none"> <li>1. Complete efforts to update the FMS security software to reflect the FMS organizational structure.</li> <li>2. As part of the redesign effort, update configuration management documentation detailing the design, technical configurations, and basic settings for restricting access to payment and system resources.</li> <li>3. Provide training to security management to properly perform recertification procedures, including examining access to mainframe security profiles and access to data files.</li> <li>4. Develop tools and automated reports to further assist security management to evaluate access to their application and application files.</li> <li>5. Simplify the FMS security software's access control settings such that security management can readily determine who has excessive access to files either directly or indirectly.</li> <li>6. Implement recently revised Recertification Procedures for users, system accounts, and system programs. Confirm that the revised recertification procedures include steps to identify appropriate files and the responsible party for reviewing access.</li> <li>7. Review and restrict excessive access to system files to only those user accounts with a justifiable business need.</li> </ol>
Configuration Management	<p>FMS has not consistently documented their baseline configurations for FMS applications that support payment management functions. Specifically, FMS has not implemented monitoring procedures and automated controls over software changes to FMS's mainframe to confirm that all changes made to system software are appropriate and approved.</p>	<p>We recommend that FMS Management:</p> <ol style="list-style-type: none"> <li>1. Adhere to FMS baseline configuration standards by documenting all software that is approved by FMS for use on the FMS systems supporting payment functions.</li> <li>2. Implement an automated mechanism to enter and track baseline configurations of FMS mainframe that support payment applications and notify FMS Management when changes to the baseline configurations occur.</li> </ol>

NIST 800-53 Control Family	Condition	Recommendation
<p>Physical and Environmental Protection</p>	<p>FMS has not consistently enforced the principles of least privilege to protect critical resources in an FMS data center and system command center in accordance with FMS's least privilege policy. Specifically, eight of 71 individuals with full-time access to the data center and command center did not have appropriate business needs based on the roles and responsibilities required for their job descriptions. Physical security management identified that these job descriptions did not require access to the data center on a daily basis.</p>	<p>We recommend FMS Management:</p> <ol style="list-style-type: none"> <li>1. Establish and implement criteria for performing bi-annual reviews of access to the Data Center and the IT Command Center. The criteria should be based on documented business needs, frequency of use, and the principle of least privilege.</li> <li>2. Establish and implement a process that records the business need for granting permanent or temporary access to the Data Center or IT Command Center. Records should show the manager who approved the requested access, the Physical Security Specialist (or designee) providing the access, and the cardholder that was granted access. The Physical Security Specialist and direct supervisor should review these records regularly to confirm that the documented business needs remain valid based on the individual's frequency of use and assigned roles and responsibilities.</li> </ol>
<p>Access Control</p>	<p>FMS granted UserIDs of FMS systems that support payment functions indirect access to sensitive files. This is due to an overly complicated configuration that allows many UserIDs to perform jobs underneath another UserID without knowing the other UserIDs password..</p>	<p>We recommend that FMS management:</p> <ol style="list-style-type: none"> <li>1. Build a Separation of Duties (SoD) matrix that reflects FMS / Fiscal IT "principles" for computer operations. This SoD matrix will also drive the development and rearchitecture of mainframe security profiles, which will reflect the SoD matrix.</li> <li>2. Document and implement an additional check in the system account recertification process to include a review of system account permissions to ensure system accounts are obtaining rights in accordance with least privileges.</li> <li>3. Train security management to perform a thorough analysis in the recertification process to include reviewing authorizations that allow system accounts to obtain rights in accordance with least privileges.</li> <li>4. Review all programs that possess bypassing attributes. Where bypassing attributes exists, apply explicit restrictions to specific data files.</li> <li>5. Restrict system account's ability to update production code and source code libraries where feasible.</li> <li>6. Restrict system programmer's excessive access to production source code libraries and data files.</li> <li>7. Reviewing system accounts and confirming they perform either one of two functions – a) they are application related and only update application files or b) they are system related and perform system functions.</li> <li>8. Restrict access to production to the change management utility or Change Management</li> </ol>

NIST 800-53 Control Family	Condition	Recommendation
<p>Configuration Management</p>	<p>FMS has not consistently enforced the principles of segregation of duties and least privilege to protect critical resources used by FMS applications that support payment functions in accordance with FMS separation of duties standards. Specifically, 74 users had write access to source code in both Production and Development environments, which is in violation of FMS separation of duties principle. FMS management indicated that during their recertification process, they do not check whether user accounts had write access to both development and production environments.</p>	<p>staff.</p> <p>We recommend FMS Management:</p> <ol style="list-style-type: none"> <li>1. Document and implement a recertification process to review each account group and confirm that user accounts within each group do not have excessive access to source code in both development and production environments without a justified business need.</li> <li>2. Remove inappropriate user access to development and production environments for users without a justified business need.</li> <li>3. Provide training to security management to properly perform system recertification procedures including examining access to account groups and evaluating whether user accounts have access to both development and production files.</li> </ol>

**APPENDIX VIII – LIST OF ACRONYMS**

<b>Acronym</b>	<b>Definition</b>
AC	Access Control
ACIOCS	Associate CIO for Cyber Security
AU	Audit and Accountability
BEP	Bureau of Engraving and Printing
BLSR	Baseline Security Requirements
BPD	Bureau of the Public Debt
CA	Security Assessment and Authorization
CDFI Fund	Community Development Financial Institution Fund
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Planning
CPIC	Capital Planning and Investment Control
CSS	Cyber Security Sub-Council
DHS	Department of Homeland Security
DNSSEC	Domain Name Service Security Extensions
DO	Departmental Offices
FDCC	Federal Desktop Core Configuration
FinCEN	Financial Crimes Enforcement Network
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FMS	Financial Management Service
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
IA	Identification and Authentication
IG	Inspector General
IR	Incident Response
IRS	Internal Revenue Service
ISSO	Information System Security Officer
IT	Information Technology
KPMG	KPMG LLP
LAN	Local Area Network
Mint	United States Mint
MOU	<i>Memorandum of Understanding</i>
MP	Media Protection
NIST	National Institute of Standards and Technology

Acronym	Definition
OCC	Office of the Comptroller of the Currency
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OTS	Office of Thrift Supervision
PE	Physical and Environmental Protection
PL	Planning
POA&M	Plan of Action and Milestones
PS	Personnel Security
RA	Risk Assessment
SC	System and Communication Protection
SI	System and Information Integrity
SIGTARP	Special Inspector General for Troubled Asset Relief Program
SP	Special Publication
SSP	System Security Plan
TAF	Trusted Agent FISMA
TARP	Troubled Asset Relief Program
TCSIRC	Treasury Computer Security Incident Response Capability
TD	Treasury Directive
TD P	Treasury Directive Publication
TIGTA	Treasury Inspector General for Tax Administration
TTB	Alcohol and Tobacco Tax and Trade Bureau
US	United States
US-CERT	United States Computer Emergency Readiness Team

THIS PAGE INTENTIONALLY LEFT BLANK

## **ATTACHMENT 2**

Treasury Inspector General for Tax  
Administration–Federal Information Security  
Management Act Report for Fiscal Year 2011,  
(Audit # 2011-20-116),  
September 20, 2011

THIS PAGE INTENTIONALLY LEFT BLANK

---

---

**TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION**



***Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011***

**September 20, 2011**

**Reference Number: 2011-20-116**

This report remains the property of the Treasury Inspector General for Tax Administration (TIGTA) and may not be disseminated beyond the Internal Revenue Service without the permission of the TIGTA.

This report may contain confidential return information protected from disclosure pursuant to I.R.C. § 6103(a). Such information may be disclosed only to Department of the Treasury employees who have a need to know this information in connection with their official tax administration duties.

---

---

**Phone Number** | **202-622-6500**

**Email Address** | **[TIGTACommunications@tigta.treas.gov](mailto:TIGTACommunications@tigta.treas.gov)**

**Web Site** | **<http://www.tigta.gov>**



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

**DEPARTMENT OF THE TREASURY**  
**WASHINGTON, D.C. 20220**

September 20, 2011

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

*Michael R. Phillips*

**FROM:** Michael R. Phillips  
Deputy Inspector General for Audit

**SUBJECT:** Treasury Inspector General for Tax Administration – Federal  
Information Security Management Act Report for Fiscal Year 2011  
(Audit # 201120006)

We are pleased to submit the Treasury Inspector General for Tax Administration’s Federal Information Security Management Act (FISMA)<sup>1</sup> report for the Fiscal Year 2011 evaluation period.<sup>2</sup> The FISMA requires the Offices of Inspector General to perform an annual independent evaluation of each Federal agency’s information security program and practices. This report reflects our independent evaluation of the Internal Revenue Service’s (IRS) information security program for the period under review.

We based our evaluation of the IRS on the Department of Homeland Security’s (DHS) Fiscal Year 2011 Inspector General FISMA Reporting guidelines, issued June 1, 2011. During the Fiscal Year 2011 FISMA evaluation period, we conducted 14 audits, as shown in Appendix I, to evaluate the adequacy of information security in the IRS. We considered the results of these audits in our evaluation. In addition, we evaluated a representative sample of 10 major IRS information systems for our FISMA work. For each system in the sample, we assessed the quality of the security assessment and authorization process, the annual testing of controls for continuous monitoring, the testing of information technology contingency plans, and the quality of the plan of action and milestones process. We also conducted tests to evaluate processes over configuration management, incident response and reporting, security training, remote access

<sup>1</sup> 44 U.S.C. Sections 3541–3549.

<sup>2</sup> The FISMA evaluation period for the Department of the Treasury is July 1, 2010, through June 30, 2011. All subsequent references to 2011 refer to the FISMA evaluation period.

	Initiator	Proofreader	Reviewer	Reviewer	Reviewer	Reviewer	Reviewer	Reviewer
Office Symbols	IG:A:SITS	IG:A:SITS	IG:A:SITS	IG:A:SITS	IG:A			
Surname	Kitazono	Duncan	Sagara	Seeba	Stephens			
Date	9/9/11	9/12/11	9/9/2011	9/12/11	9/20/11			



***Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011***

---

management, identity and access management, contractor systems, and security architecture and capital planning. Major contributors to this report are listed in Appendix II.

Based on our Fiscal Year 2011 FISMA evaluation, we determined that the IRS's information security program is in place and generally compliant with the FISMA legislation, but improvements are needed. We determined that the following program areas met the level of performance specified by the DHS's 2011 FISMA checklist.

- Risk management.
- Incident response and reporting.
- Remote access management.
- Continuous monitoring management.
- Contingency planning.
- Contractor systems.
- Security capital planning.

We determined the following program areas were not fully effective as a result of the conditions identified that need improvement.

- Configuration management.
- Security training.
- Plans of action and milestones.
- Identity and access management.

Copies of this report are also being sent to the IRS managers affected by the report results. Please contact me at (202) 622-6510 if you have questions or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.



---

**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

---

**Table of Contents**

**Background**.....Page 1

**Results of Review** .....Page 2

**Appendices**

Appendix I – Treasury Inspector General for Tax Administration  
Information Technology Security Reports Issued During the  
Fiscal Year 2011 Evaluation Period .....Page 20

Appendix II – Major Contributors to This Report .....Page 22

Appendix III – Report Distribution List .....Page 23



---

***Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011***

---

## ***Abbreviations***

DHS	Department of Homeland Security
FCD1	Federal Continuity Directive 1
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information System Management Act
GAO	Government Accountability Office
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
TIGTA	Treasury Inspector General for Tax Administration
US-CERT	United States Computer Emergency Response Team
USGCB	United States Government Configuration Baseline



***Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011***

---

---

## ***Background***

The Internal Revenue Service (IRS) collects and maintains a significant amount of personal and financial information on each taxpayer. The IRS also relies extensively on computerized systems to support its responsibilities in collecting taxes, processing tax returns, and enforcing the Federal tax laws. As custodians of taxpayer information, the IRS has an obligation to protect the confidentiality of this sensitive information against unauthorized access or loss. Otherwise, taxpayers could be exposed to invasion of privacy and financial loss or damage from identity theft or other financial crimes.

The Federal Information Security Management Act (FISMA)<sup>1</sup> was enacted to strengthen the security of information and systems within Federal agencies. Under the FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of the FISMA, related Office of Management and Budget (OMB) policies, and National Institute of Standards and Technology (NIST) procedures, standards, and guidelines.

As part of this legislation, each Federal Government agency is required to report annually to the OMB on the adequacy and effectiveness of its information security program and practices and compliance with the FISMA. In addition, the FISMA requires the agencies to have an annual independent evaluation of their information security programs and practices performed by the agency Inspector General or an independent external auditor as determined by the Inspector General. The OMB uses the information from the agencies and independent evaluations in its FISMA oversight capacity to assess agency-specific and Federal Government-wide security performance, develop its annual security report to Congress, and assist in improving and maintaining adequate agency security performance. For the Fiscal Year 2011 FISMA evaluation, the Department of Homeland Security (DHS) issued the information security performance measures by which each agency was evaluated.

In compliance with the FISMA requirements, the Treasury Inspector General for Tax Administration (TIGTA) performs the annual independent evaluation of the information security program and practices of the IRS. Attached is the TIGTA's Fiscal Year 2011 FISMA report. The report was forwarded to the Treasury Inspector General for consolidation into a report issued to the Department of the Treasury Chief Information Officer.

---

<sup>1</sup> 44 U.S.C. Sections 3541–3549.



---

**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

---

## **Results of Review**

The DHS issued a checklist<sup>2</sup> for use by Offices of Inspectors General to assess the level of performance achieved by agencies in the specified program areas during the Fiscal Year 2011 FISMA evaluation period.<sup>3</sup> This report presents our completed DHS checklist for the IRS.

We determined the level of performance (a, b, or c) that the IRS had achieved for each of the program areas listed. As defined by the DHS, agencies achieve an “a” status for the program area if they have met all the attributes specified by DHS in the “a” section. Agencies achieve a “b” status if they have established the program area, but significant improvements were needed in regards to certain conditions specified by the DHS. The DHS listed the conditions in the “b” section that, if in need of significant improvement, would prevent agencies from achieving an “a” status. Agencies achieve a “c” status if they have not yet established the program area.

We checked IRS program areas as an “a” status where we determined that the IRS met all the program attributes specified by the DHS. We checked IRS program areas as a “b” status where we determined that one or more conditions listed by the DHS needed significant improvement at the IRS. Due to time and resource constraints, we were unable to test all conditions listed by the DHS in the “b” sections. Therefore, it is possible that more of these conditions exist at the IRS than those we have checked. We did not check any program areas as a “c” status because the IRS has established all program areas listed by the DHS.

For our FISMA work, we evaluated a representative sample of 10 major IRS information systems, which included 9 IRS systems and 1 contractor-managed system. Of these 10 systems, 1 system had a Federal Information Processing Standards 199 impact level of high, and 9 systems were of a moderate impact level. All 10 systems had a current security assessment and authorization, had security controls tested within the past year, and had contingency plans tested in accordance with policy. Of the 10 IRS systems the TIGTA selected for the Fiscal Year 2011 FISMA evaluation, 4 systems completed the security assessment and authorization process, and 6 systems completed annual testing of selected controls during the Fiscal Year 2011 FISMA evaluation period.

---

<sup>2</sup> Due to the nature of the list that follows, many abbreviations are used exactly as presented in the original document reproduced and are not defined therein. However, please see the Abbreviations page after the Table of Contents of this report for a list of abbreviations that we have defined.

<sup>3</sup> The FISMA evaluation period for the Department of the Treasury is July 1, 2010, through June 30, 2011. All subsequent references to 2011 refer to the FISMA evaluation period.



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

**RESPONSES TO FISCAL YEAR 2011  
DHS QUESTIONS FOR INSPECTOR GENERALS**

**1: Risk Management**

Status of Risk Management Program [check one]	<input checked="" type="checkbox"/>	<p><b>1.a.</b> The Agency has established and is maintaining a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the Office of the Inspector General (OIG), the program includes the following attributes:</p> <p><b>1.a(1).</b> Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.</p> <p><b>1.a(2).</b> Addresses risk from an <i>organization</i> perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev. 1.</p> <p><b>1.a(3).</b> Addresses risk from a <i>mission and business process</i> perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev. 1.</p> <p><b>1.a(4).</b> Addresses risk from an <i>information system</i> perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1.</p> <p><b>1.a(5).</b> Categorizes information systems in accordance with government policies.</p> <p><b>1.a(6).</b> Selects an appropriately tailored set of baseline security controls.</p> <p><b>1.a(7).</b> Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.</p> <p><b>1.a(8).</b> 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.</p> <p><b>1.a(9).</b> 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.</p> <p><b>1.a(10).</b> Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness.</p> <p><b>1.a(11).</b> Information system specific risks (tactical), mission/business specific risks, and organizational level (strategic) risks are communicated to appropriate levels of the organization.</p> <p><b>1.a(12).</b> Senior officials are briefed on threat activity on a regular basis by</p>
--	-------------------------------------	---



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

		<p>appropriate personnel. (e.g., Chief Information Security Officer (CISO)).</p> <p><b>1.a(13).</b> 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.</p> <p><b>1.a(14).</b> Security authorization package contains system security plan, security assessment report, and Plans of Action and Milestones (POA&amp;M) in accordance with government policies.</p>
		<b>1.b.</b> The Agency has established and is maintaining a risk management program. However, the Agency needs to make significant improvements as noted below.
If 1.b. is checked above, check areas that need significant improvement:		<b>1.b(1).</b> Risk management policy is not fully developed.
		<b>1.b(2).</b> Risk management procedures are not fully developed, sufficiently detailed (SP 800-37, SP 800-39, SP 800-53).
		<b>1.b(3).</b> Risk management procedures are not consistently implemented in accordance with government policies (SP 800-37, SP 800-39, SP 800-53).
		<b>1.b(4).</b> A comprehensive governance structure and Agency-wide risk management strategy has not been fully developed in accordance with government policies (SP 800-37, SP 800-39, SP 800-53).
		<b>1.b(5).</b> Risks from a mission and business process perspective are not addressed (SP 800-37, SP 800-39, SP 800-53).
		<b>1.b(6).</b> Information systems are not properly categorized (FIPS 199/ SP 800-60).
		<b>1.b(7).</b> Appropriately tailored baseline security controls are not applied to information systems in accordance with government policies (FIPS 200/ SP 800-53).
		<b>1.b(8).</b> Risk assessments are not conducted in accordance with government policies (SP 800-30).
		<b>1.b(9).</b> Security control baselines are not appropriately tailored to individual information systems in accordance with government policies (SP 800-53).
		<b>1.b(10).</b> The communication of information system specific risks, mission/business specific risks, and organizational level (strategic) risks to appropriate levels of the organization is not in accordance with government policies.
		<b>1.b(11).</b> The process to assess security control effectiveness is not in accordance with government policies (SP800-53A).
		<b>1.b(12).</b> The process to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate is not in accordance with government policies (SP 800-37).
		<b>1.b(13).</b> The process to continuously monitor changes to information systems that may necessitate reassessment of control effectiveness is not in accordance with government policies (SP 800-37).
		<b>1.b(14).</b> Security plan is not in accordance with government policies (SP 800-18, SP 800-37).
		<b>1.b(15).</b> Security assessment report is not in accordance with government policies (SP 800-53A, SP 800-37).
		<b>1.b(16).</b> Accreditation boundaries for agency information systems are not defined in accordance with government policies.



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

		<b>1.b(17).</b> Other
		<b>1.b(17ex).</b> Explanation for Other
		<b>1.c.</b> The Agency has not established a risk management program.
Comments:		

**2: Configuration Management**

Status of Configuration Management Program [check one]		<p><b>2.a.</b> The Agency has established and is maintaining a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>2.a(1).</b> Documented policies and procedures for configuration management.</p> <p><b>2.a(2).</b> Standard baseline configurations defined.</p> <p><b>2.a(3).</b> Assessing for compliance with baseline configurations.</p> <p><b>2.a(4).</b> Process for timely, as specified in agency policy or standards, remediation of scan result deviations.</p> <p><b>2.a(5).</b> For Windows-based components, Federal Desktop Core Configuration (FDCC)/United States Government Configuration Baseline (USGCB) secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.</p> <p><b>2.a(6).</b> Documented proposed or actual changes to hardware and software configurations.</p> <p><b>2.a(7).</b> Process for timely and secure installation of software patches.</p>
	✓	<p><b>2.b.</b> The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.</p>
If 2.b. is checked above, check areas that need significant improvement:		<b>2.b(1).</b> Configuration management policy is not fully developed (NIST 800-53: CM-1)
		<b>2.b(2).</b> Configuration management procedures are not fully developed (NIST 800-53: CM-1).
	✓	<b>2.b(3).</b> Configuration management procedures are not consistently implemented (NIST 800-53: CM-1).
		<b>2.b(4).</b> Standard baseline configurations are not identified for software components (NIST 800-53: CM-2).
		<b>2.b(5).</b> Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).
	✓	<b>2.b(6).</b> Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).
		<b>2.b(7).</b> FDCC/USGCB is not fully implemented (OMB) and/or all deviations are not fully documented (NIST 800-53: CM-6).
	✓	<b>2.b(8).</b> Software assessing (scanning) capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

✓	<b>2.b(9).</b> Configuration-related vulnerabilities, including scan findings, have not been remediated in a timely manner, as specified in agency policy or standards (NIST 800-53: CM-4, CM-6, RA-5, SI-2).
✓	<b>2.b(10).</b> Patch management process is not fully developed, as specified in agency policy or standards (NIST 800-53: CM-3, SI-2).
	<b>2.b(11).</b> Other
	<b>2.b(11ex).</b> Explanation for Other
	<b>2.c.</b> The Agency has not established a security configuration management program.
<p>Comments: In March 2011, the Government Accountability Office (GAO) reported<sup>4</sup> that the IRS had newly identified and unresolved weaknesses related to access controls, configuration management, and segregation of duties that continue to jeopardize the confidentiality, integrity, and availability of the financial and sensitive taxpayer information processed by the IRS’s systems. Considered collectively, these weaknesses were the basis for GAO’s determination that the IRS had a material weakness in internal control over its financial reporting related to information security in Fiscal Year 2010. In May 2011, the TIGTA reported<sup>5</sup> that nonmainframe databases containing taxpayer data were not always configured in a secure manner and were running out-of-date software that no longer received security patches and other vendor support. In addition, the TIGTA reported that the IRS had not fully implemented its plans to complete vulnerability scans of databases within its enterprise. Further, the IRS has been unable to establish an enterprise-wide process for timely remediation of weaknesses reported by vulnerabilities scans because of the limited information it gets from the scan results. To correct configuration management deficiencies, the IRS is in the process of implementing an Enterprise Configuration Management System, with planning dates through Fiscal Year 2014, that will provide oversight and enforcement of configuration and change management processes.</p>	

**3: Incident Response and Reporting**

Status of Incident Response & Reporting Program [check one]	<table border="1"> <tr> <td style="text-align: center;">✓</td> <td> <p><b>3.a.</b> The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>3.a(1).</b> Documented policies and procedures for detecting, responding to, and reporting incidents.</p> <p><b>3.a(2).</b> Comprehensive analysis, validation, and documentation of incidents.</p> <p><b>3.a(3).</b> When applicable, reports to United States Computer Emergency Response Team (US-CERT) within established timeframes.</p> <p><b>3.a(4).</b> When applicable, reports to law enforcement within established timeframes.</p> <p><b>3.a(5).</b> Responds to and resolves incidents in a timely manner, as specified in</p> </td> </tr> </table>	✓	<p><b>3.a.</b> The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>3.a(1).</b> Documented policies and procedures for detecting, responding to, and reporting incidents.</p> <p><b>3.a(2).</b> Comprehensive analysis, validation, and documentation of incidents.</p> <p><b>3.a(3).</b> When applicable, reports to United States Computer Emergency Response Team (US-CERT) within established timeframes.</p> <p><b>3.a(4).</b> When applicable, reports to law enforcement within established timeframes.</p> <p><b>3.a(5).</b> Responds to and resolves incidents in a timely manner, as specified in</p>
✓	<p><b>3.a.</b> The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>3.a(1).</b> Documented policies and procedures for detecting, responding to, and reporting incidents.</p> <p><b>3.a(2).</b> Comprehensive analysis, validation, and documentation of incidents.</p> <p><b>3.a(3).</b> When applicable, reports to United States Computer Emergency Response Team (US-CERT) within established timeframes.</p> <p><b>3.a(4).</b> When applicable, reports to law enforcement within established timeframes.</p> <p><b>3.a(5).</b> Responds to and resolves incidents in a timely manner, as specified in</p>		

<sup>4</sup> *INFORMATION SECURITY: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data* (GAO-11-308, dated March 2011).

<sup>5</sup> *Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected* (Reference Number 2011-20-044, dated May 4, 2011).



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

		<p>agency policy or standards, to minimize further damage.</p> <p><b>3.a(6).</b> Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.</p> <p><b>3.a(7).</b> Is capable of correlating incidents.</p>
		<b>3.b.</b> The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below.
If 3.b. is checked above, check areas that need significant improvement:		<b>3.b(1).</b> Incident response and reporting policy is not fully developed (NIST 800-53: IR-1).
		<b>3.b(2).</b> Incident response and reporting procedures are not fully developed or sufficiently detailed (NIST 800-53: IR-1).
		<b>3.b(3).</b> Incident response and reporting procedures are not consistently implemented in accordance with government policies (NIST 800-61, Rev 1).
		<b>3.b(4).</b> Incidents were not identified in a timely manner, as specified in agency policy or standards (NIST 800-53, 800-61 and OMB M-07-16, M-06-19).
		<b>3.b(5).</b> Incidents were not reported to the US-CERT as required (NIST 800-53, 800-61 and OMB M-07-16, M-06-19).
		<b>3.b(6).</b> Incidents were not reported to law enforcement as required (SP 800-86).
		<b>3.b(7).</b> Incidents were not resolved in a timely manner (NIST 800-53, 800-61 and OMB M-07-16, M-06-19).
		<b>3.b(8).</b> Incidents were not resolved to minimize further damage (NIST 800-53, 800-61 and OMB M-07-16, M-06-19).
		<b>3.b(9).</b> There is insufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61 and OMB M-07-16, M-06-19).
		<b>3.b(10).</b> The agency cannot or is not prepared to track and manage incidents in a virtual/cloud environment.
		<b>3.b(11).</b> The agency does not have the technical capability to correlate incident events.
		<b>3.b(12).</b> Other
		<b>3.b(12ex).</b> Explanation for Other
		<b>3.c.</b> The Agency has not established an incident response and reporting program.
Comments:		



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

**4: Security Training**

Status of Security Training Program [check one]		<p><b>4.a.</b> The Agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>4.a(1).</b> Documented policies and procedures for security awareness training.</p> <p><b>4.a(2).</b> Documented policies and procedures for specialized training for users with significant information security responsibilities.</p> <p><b>4.a(3).</b> Security training content based on the organization and roles, as specified in agency policy or standards.</p> <p><b>4.a(4).</b> Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other agency users) with access privileges that require security awareness training.</p> <p><b>4.a(5).</b> Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other agency users) with significant information security responsibilities that require specialized training.</p>
	✓	<p><b>4.b.</b> The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below.</p>
If 4.b. is checked above, check areas that need significant improvement:		<p><b>4.b(1).</b> Security awareness training policy is not fully developed (NIST 800-53: AT-1).</p>
		<p><b>4.b(2).</b> Security awareness training procedures are not fully developed and sufficiently detailed (NIST 800-53: AT-1).</p>
		<p><b>4.b(3).</b> Security awareness training procedures are not consistently implemented in accordance with government policies (NIST 800-53: AT-2).</p>
		<p><b>4.b(4).</b> Specialized security training policy is not fully developed (NIST 800-53: AT-3).</p>
		<p><b>4.b(5).</b> Specialized security training procedures are not fully developed or sufficiently detailed in accordance with government policies (SP 800-50, SP 800-53).</p>
		<p><b>4.b(6).</b> Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).</p>
		<p><b>4.b(7).</b> Identification and tracking of the status of security awareness training for personnel (including employees, contractors, and other agency users) with access privileges that require security awareness training is not adequate in accordance with government policies (SP 800-50, SP 800-53).</p>
	✓	<p><b>4.b(8).</b> Identification and tracking of the status of specialized training for personnel (including employees, contractors, and other agency users) with significant information security responsibilities is not adequate in accordance with government policies (SP 800-50, SP 800-53).</p>
		<p><b>4.b(9).</b> Training content for individuals with significant information security responsibilities is not adequate in accordance with government policies (SP 800-53, SP 800-16).</p>
		<p><b>4.b(10).</b> Less than 90% of personnel (including employees, contractors, and other agency users) with access privileges completed security awareness</p>



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

		training in the past year.
		<b>4.b(11).</b> Less than 90% of employees, contractors, and other users with significant security responsibilities completed specialized security awareness training in the past year.
		<b>4.b(12).</b> Other
		<b>4.b(12ex).</b> Explanation for Other
		<b>4.c.</b> The Agency has not established a security training program.
<p>Comments: In June 2011, the TIGTA reported<sup>6</sup> that the IRS was unable to track whether employees with disaster recovery roles attend required annual disaster recovery training. The IRS plans to develop a process for identifying and tracking the completion of training for employees with disaster recovery roles by December 31, 2011. In addition, the IRS did not identify or track contractors that require specialized training for the Fiscal Year 2011 FISMA year, but plans to begin collecting and tracking information on contractor completion of specialized training for the Fiscal Year 2012 FISMA year. Contractors will self identify and report the completion of specialized training where required and provide these data to the IRS.</p>		

**5: POA&M**

Status of Plan of Action & Milestones (POA&M) Program [check one]		<p><b>5.a.</b> The Agency has established and is maintaining a POA&amp;M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>5.a(1).</b> Documented policies and procedures for managing information technology security weaknesses discovered during security control assessments and requiring remediation.</p> <p><b>5.a(2).</b> Tracks, prioritizes, and remediates weaknesses.</p> <p><b>5.a(3).</b> Ensures remediation plans are effective for correcting weaknesses.</p> <p><b>5.a(4).</b> Establishes and adheres to milestone remediation dates.</p> <p><b>5.a(5).</b> Ensures resources are provided for correcting weaknesses.</p> <p><b>5.a(6).</b> Program officials and contractors report progress on remediation to the Chief Information Officer on a regular basis, at least quarterly, and the Chief Information Officer centrally tracks, maintains, and independently reviews/validates the POA&amp;M activities at least quarterly.</p>
	✓	<p><b>5.b.</b> The Agency has established and is maintaining a POA&amp;M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.</p>
If 5.b. is checked above, check areas that need significant improvement:		<b>5.b(1).</b> POA&M Policy is not fully developed.
		<b>5.b(2).</b> POA&M procedures are not fully developed and sufficiently detailed.

<sup>6</sup> *Corrective Actions to Address the Disaster Recovery Material Weakness Are Being Completed* (Reference Number 2011-20-060, dated June 27, 2011).



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

	<b>5.b(3).</b> POA&M procedures are not consistently implemented in accordance with government policies.
	<b>5.b(4).</b> POA&Ms do not include security weaknesses discovered during assessments of security controls and requiring remediation (OMB M-04-25).
	<b>5.b(5).</b> Remediation actions do not sufficiently address weaknesses in accordance with government policies (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls).
	<b>5.b(6).</b> Source of security weaknesses are not tracked (OMB M-04-25).
	<b>5.b(7).</b> Security weaknesses are not appropriately prioritized (OMB M-04-25).
	<b>5.b(8).</b> Milestone dates are not adhered to (OMB M-04-25).
	<b>5.b(9).</b> Initial target remediation dates are frequently missed (OMB M-04-25).
	<b>5.b(10).</b> POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).
✓	<b>5.b(11).</b> Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25).
	<b>5.b(12).</b> Agency Chief Information Officer does not track and review POA&Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).
	<b>5.b(13).</b> Other
	<b>5.b(13ex).</b> Explanation for Other
	<b>5.c.</b> The Agency has not established a POA&M program.
<p>Comments: Our review of the 10 IRS systems selected for the Fiscal Year 2011 FISMA evaluation found that improvements were needed to ensure costs associated with remediating weaknesses are identified.</p> <ul style="list-style-type: none"> <li>Thirteen (39 percent) of 33 closed weaknesses and 24 (31 percent) of 77 open weaknesses, maintained in the 10 IRS systems' Fiscal Year 2011 POA&amp;Ms, did not have costs associated with remediating the weaknesses in accordance with IRS policy.</li> </ul>	

**6: Remote Access Management**

Status of Remote Access Management Program [check one]	✓	<p><b>6.a.</b> The Agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>6.a(1).</b> Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.</p> <p><b>6.a(2).</b> Protects against unauthorized connections or subversion of authorized connections.</p> <p><b>6.a(3).</b> Users are uniquely identified and authenticated for all access.</p> <p><b>6.a(4).</b> If applicable, multi-factor authentication is required for remote access.</p> <p><b>6.a(5).</b> Authentication mechanisms meet NIST Special Publication 800-63</p>
---	---	---



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

		<p>guidance on remote electronic authentication, including strength mechanisms.</p> <p><b>6.a(6).</b> Defines and implements encryption requirements for information transmitted across public networks.</p> <p><b>6.a(7).</b> Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication is required.</p>
		<b>6.b.</b> The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.
If 6.b. is checked above, check areas that need significant improvement:		<b>6.b(1).</b> Remote access policy is not fully developed (NIST 800-53: AC-1, AC-17).
		<b>6.b(2).</b> Remote access procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1, AC-17).
		<b>6.b(3).</b> Remote access procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-1, AC-17).
		<b>6.b(4).</b> Telecommuting policy is not fully developed (NIST 800-46, Section 5.1).
		<b>6.b(5).</b> Telecommuting procedures are not fully developed or sufficiently detailed in accordance with government policies (NIST 800-46, Section 5.4).
		<b>6.b(6).</b> Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, Section 5.1).
		<b>6.b(7).</b> Multi-factor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).
		<b>6.b(8).</b> Agency has not identified all remote devices (NIST 800-46, Section 2.1).
		<b>6.b(9).</b> Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46, Section 3.1 and 4.2).
		<b>6.b(10).</b> Agency does not adequately monitor remote devices when connected to the agency's networks remotely in accordance with government policies (NIST 800-46, Section 3.2).
		<b>6.b(11).</b> Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).
		<b>6.b(12).</b> Remote access rules of behavior are not adequate in accordance with government policies (NIST 800-53, PL-4).
		<b>6.b(13).</b> Remote access user agreements are not adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6).
		<b>6.b(14).</b> Other
	<b>6.b(14ex).</b> Explanation for Other	
		<b>6.c.</b> The Agency has not established a program for providing secure remote access.
Comments:		



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

**7: Identity and Access Management**

<p>Status of Account and Identity Management Program [check one]</p>		<p><b>7.a.</b> The Agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>7.a(1).</b> Documented policies and procedures for account and identity management.</p> <p><b>7.a(2).</b> Identifies all users, including Federal employees, contractors, and others who access Agency systems.</p> <p><b>7.a(3).</b> Identifies when special access requirements (e.g., multi-factor authentication) are necessary.</p> <p><b>7.a(4).</b> If multi-factor authentication is in use, it is linked to the Agency’s personal identity verification program where appropriate.</p> <p><b>7.a(5).</b> Ensures that the users are granted access based on needs and separation of duties principles.</p> <p><b>7.a(6).</b> Identifies devices that are attached to the network and distinguishes these devices from users.</p> <p><b>7.a(7).</b> Ensures that accounts are terminated or deactivated once access is no longer required.</p> <p><b>7.a(8).</b> Identifies and controls use of shared accounts.</p>
	✓	<p><b>7.b.</b> The Agency has established and is maintaining an identity and access management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.</p>
<p>If 7.b. is checked above, check areas that need significant improvement:</p>		<p><b>7.b(1).</b> Account management policy is not fully developed (NIST 800-53: AC-1).</p> <p><b>7.b(2).</b> Account management procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1).</p> <p>✓ <b>7.b(3).</b> Account management procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-2).</p> <p><b>7.b(4).</b> Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).</p> <p><b>7.b(5).</b> Accounts are not properly issued to new users (NIST 800-53, AC-2).</p> <p>✓ <b>7.b(6).</b> Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).</p> <p><b>7.b(7).</b> Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).</p> <p><b>7.b(8).</b> Agency has not adequately planned for implementation of personal identity verification for logical access in accordance with government policies (Homeland Security Presidential Directive 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).</p>



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

✓	<b>7.b(9).</b> Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).
	<b>7.b(10).</b> Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).
	<b>7.b(11).</b> Network devices are not properly authenticated (NIST 800-53, IA-3).
	<b>7.b(12).</b> The process for requesting or approving membership in shared privileged accounts is not adequate in accordance to government policies.
	<b>7.b(13).</b> Use of shared privileged accounts is not necessary or justified.
	<b>7.b(14).</b> When shared accounts are used, the Agency does not renew shared account credentials when a member leaves the group.
	<b>7.b(15).</b> Other
	<b>7.b(15ex).</b> Explanation for Other
	<b>7.c.</b> The Agency has not established an identity and access management program.
<p>Comments: In March 2011, the GAO reported<sup>7</sup> that the IRS had newly identified and unresolved weaknesses related to access controls, configuration management, and segregation of duties that continue to jeopardize the confidentiality, integrity, and availability of the financial and sensitive taxpayer information processed by IRS's systems. Considered collectively, these weaknesses were the basis for GAO's determination that the IRS had a material weakness in internal control over its financial reporting related to information security in Fiscal Year 2010. In May 2011, the TIGTA reported<sup>8</sup> access controls had not been implemented or were not operating effectively on an IRS bankruptcy case tracking system, on which many IRS employees had excessive privileges. In addition, the TIGTA reported that user accounts on the bankruptcy case tracking system were not properly terminated when users no longer required access. Our review of the 10 IRS systems selected for the Fiscal Year 2011 FISMA evaluation found that all systems needed improvement in implementing NIST baseline access controls and identity and authentication controls.</p>	

<sup>7</sup> *INFORMATION SECURITY: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data* (GAO-11-308, dated March 2011).

<sup>8</sup> *Access Controls for the Automated Insolvency System Need Improvement* (Reference Number 2011-20-046, dated May 16, 2011).



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

**8: Continuous Monitoring Management**

Status of Continuous Monitoring Program [check one]	<input checked="" type="checkbox"/>	<p><b>8.a.</b> The Agency has 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. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>8.a(1).</b> Documented policies and procedures for continuous monitoring.</p> <p><b>8.a(2).</b> Documented strategy and plans for continuous monitoring.</p> <p><b>8.a(3).</b> Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.</p> <p><b>8.a(4).</b> Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&amp;M additions and updates with the frequency defined in the strategy and/or plans.</p>
		<p><b>8.b.</b> The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.</p>
If 8.b. is checked above, check areas that need significant improvement:		<p><b>8.b(1).</b> Continuous monitoring policy is not fully developed (NIST 800-53: CA-7).</p>
		<p><b>8.b(2).</b> Continuous monitoring procedures are not fully developed (NIST 800-53: CA-7).</p>
		<p><b>8.b(3).</b> Continuous monitoring procedures are not consistently implemented (NIST 800-53: CA-7; 800-37 Rev 1, Appendix G).</p>
		<p><b>8.b(4).</b> Strategy or plan has not been fully developed for enterprise-wide continuous monitoring (NIST 800-37 Rev 1, Appendix G).</p>
		<p><b>8.b(5).</b> Ongoing assessments of security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).</p>
		<p><b>8.b(6).</b> The following were not provided to the authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&amp;Ms (NIST 800-53, NIST 800-53A).</p>
		<p><b>8.b(7).</b> Other</p>
		<p><b>8.b(7ex).</b> Explanation for Other</p>
Comments:		



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

**9: Contingency Planning**

<p>Status of Contingency Planning Program [check one]</p>	<input checked="" type="checkbox"/>	<p><b>9.a.</b> The Agency established and is maintaining an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>9.a(1).</b> Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.</p> <p><b>9.a(2).</b> The agency has performed an overall business impact analysis.</p> <p><b>9.a(3).</b> Development and documentation of division, component, and information technology infrastructure recovery strategies, plans and procedures.</p> <p><b>9.a(4).</b> Testing of system specific contingency plans.</p> <p><b>9.a(5).</b> The documented business continuity and disaster recovery plans are in place and can be implemented when necessary.</p> <p><b>9.a(6).</b> Development of test, training, and exercise programs.</p> <p><b>9.a(7).</b> Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans.</p>
		<p><b>9.b.</b> The Agency has established and is maintaining an enterprise-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.</p>
<p>If 9.b. is checked above, check areas that need significant improvement:</p>		<p><b>9.b(1).</b> Contingency planning policy is not fully developed contingency planning policy is not consistently implemented (NIST 800-53: CP-1).</p> <p><b>9.b(2).</b> Contingency planning procedures are not fully developed (NIST 800-53: CP-1).</p> <p><b>9.b(3).</b> Contingency planning procedures are not consistently implemented (NIST 800-53; 800-34).</p> <p><b>9.b(4).</b> An overall business impact assessment has not been performed (NIST SP 800-34).</p> <p><b>9.b(5).</b> Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).</p> <p><b>9.b(6).</b> A business continuity/disaster recovery plan has not been developed (Federal Continuity Directive 1 (FCD1), NIST SP 800-34).</p> <p><b>9.b(7).</b> A business continuity/disaster recovery plan has been developed but not fully implemented (FCD1, NIST SP 800-34).</p> <p><b>9.b(8).</b> System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).</p> <p><b>9.b(9).</b> System contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53).</p> <p><b>9.b(10).</b> Test, training, and exercise programs have not been developed (FCD1, NIST SP 800-34, NIST 800-53).</p>



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

	<b>9.b(11).</b> Test, training, and exercise programs have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).
	<b>9.b(12).</b> After-action report did not address issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).
	<b>9.b(13).</b> Systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).
	<b>9.b(14).</b> Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).
	<b>9.b(15).</b> Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).
	<b>9.b(16).</b> Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).
	<b>9.b(17).</b> Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).
	<b>9.b(18).</b> Contingency planning does not consider supply chain threats.
	<b>9.b(19).</b> Other
	<b>9.b(19ex).</b> Explanation for Other
	<b>9.c.</b> The Agency has not established a business continuity/disaster recovery program.
Comments:	



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

**10: Contractor Systems**

<p>Status of Agency Program to Oversee Contractor Systems [check one]</p>	<p>✓</p>	<p><b>10.a.</b> The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>10.a(1).</b> Documented policies and procedures for information security oversight of systems operated on the Agency’s behalf by contractors or other entities, including Agency systems and services residing in public cloud.</p> <p><b>10.a(2).</b> The Agency obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and agency guidelines.</p> <p><b>10.a(3).</b> A complete inventory of systems operated on the Agency’s behalf by contractors or other entities, including Agency systems and services residing in public cloud.</p> <p><b>10.a(4).</b> The inventory identifies interfaces between these systems and Agency-operated systems.</p> <p><b>10.a(5).</b> The agency requires appropriate agreements (e.g., Memorandums of Understanding, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.</p> <p><b>10.a(6).</b> The inventory of contractor systems is updated at least annually.</p> <p><b>10.a(7).</b> Systems that are owned or operated by contractors or entities, including Agency systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.</p>
		<p><b>10.b.</b> The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in public cloud. However, the Agency needs to make significant improvements as noted below.</p>
<p>If 10.b. is checked above, check areas that need significant improvement:</p>		<p><b>10.b(1).</b> Policies to oversee systems operated on the Agency’s behalf by contractors or other entities, including Agency systems and services residing in public cloud, are not fully developed.</p> <p><b>10.b(2).</b> Procedures to oversee systems operated on the Agency’s behalf by contractors or other entities, including Agency systems and services residing in public cloud, are not fully developed.</p> <p><b>10.b(3).</b> Procedures to oversee systems operated on the Agency’s behalf by contractors or other entities, including Agency systems and services residing in public cloud are not consistently implemented.</p> <p><b>10.b(4).</b> The inventory of systems owned or operated by contractors or other entities, including Agency systems and services residing in public cloud, is not complete in accordance with government policies (NIST 800-53: PM-5).</p> <p><b>10.b(5).</b> The inventory does not identify interfaces between contractor/entity-operated systems to Agency owned and operated systems.</p>



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

	<b>10.b(6).</b> The inventory of contractor/entity-operated systems, including interfaces, is not updated at least annually.
	<b>10.b(7).</b> Systems owned or operated by contractors and entities are not subject to NIST and OMB’s FISMA requirements (e.g., security requirements).
	<b>10.b(8).</b> Systems owned or operated by contractors and entities do not meet NIST and OMB’s FISMA requirements (e.g., security requirements).
	<b>10.b(9).</b> Interface agreements (e.g., Memorandums of Understanding) are not properly documented, authorized, or maintained.
	<b>10.b(10).</b> Other
	<b>10.b(10ex).</b> Explanation for Other:
	<b>10.c.</b> The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in public cloud.
Comments:	

**11: Security Capital Planning**

Status of Agency Program to Oversee Security Capital Planning [check one]	✓	<p><b>11.a.</b> The Agency has established and maintains a security capital planning and investment program for information security. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p><b>11.a(1).</b> Documented policies and procedures to address information security in the capital planning and investment control process.</p> <p><b>11.a(2).</b> Includes information security requirements as part of the capital planning and investment process.</p> <p><b>11.a(3).</b> Establishes a discrete line item for information security in organizational programming and documentation.</p> <p><b>11.a(4).</b> Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.</p> <p><b>11.a(5).</b> Ensures that information security resources are available for expenditure as planned.</p>
		<p><b>11.b.</b> The Agency has established and maintains a capital planning and investment program. However, the Agency needs to make significant improvements as noted below.</p>
If 11.b. is checked above, check areas that need significant improvement:		<b>11.b(1).</b> Capital planning and investment control information security policy is not fully developed.
		<b>11.b(2).</b> Capital planning and investment control information security procedures are not fully developed.
		<b>11.b(3).</b> Capital planning and investment control information security procedures are not consistently implemented.
		<b>11.b(4).</b> The Agency does not adequately plan for information technology security during the capital planning and investment control process (SP 800-65).



**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

	<b>11.b(5).</b> The Agency does not include a separate line for information security in appropriate documentation (NIST 800-53: SA-2).
	<b>11.b(6).</b> Exhibits 300/53 or business cases do not adequately address or identify information security costs (NIST 800-53: PM-3).
	<b>11.b(7).</b> The Agency does not provide information technology security funding to maintain the security levels identified.
	<b>11.b(8).</b> Other
	<b>11.b(8ex).</b> Explanation for Other
	<b>11.c.</b> The Agency does not have a capital planning and investment program.
Comments:	



---

**Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011**

---

**Appendix I**

**Treasury Inspector General for Tax Administration  
Information Technology Security Reports Issued  
During the Fiscal Year 2011 Evaluation Period**

1. *The Internal Revenue Service Is Improving Management Controls for Information Technology Strategic Planning and Capital Investments* (Reference Number 2010-20-064, dated July 9, 2010).
2. *Additional Actions and Resources Are Needed to Resolve the Audit Trail Portion of the Computer Security Material Weakness* (Reference Number 2010-20-082, dated July 28, 2010).
3. *More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness* (Reference Number 2010-20-084, dated August 26, 2010).
4. *The Federal Student Aid Datashare Application Was Successfully Deployed, but Improvements in Systems Development Disciplines Are Needed* (Reference Number 2010-20-099, dated September 3, 2010).
5. *Treasury Inspector General for Tax Administration Federal Information Security Management Act (Non-Intelligence National Security Systems) Report for Fiscal Year 2010* (Reference Number 2010-20-101, dated September 9, 2010).
6. *Annual Assessment of the Business Systems Modernization Program* (Reference Number 2010-20-094, dated September 23, 2010).
7. *Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2010* (Reference Number 2011-20-003, dated November 10, 2010).
8. *Prototype Process Improvements Will Benefit Efforts to Modernize Taxpayer Account Administration* (Reference Number 2011-20-001, dated November 24, 2010).
9. *The Sustaining Infrastructure Program Is Significantly Improved and a Comprehensive Information Technology Infrastructure Strategy Has Been Developed* (Reference Number 2011-20-006, dated December 30, 2010).
10. *Additional Security Is Needed for the Taxpayer Secure Email Program* (Reference Number 2011-20-012, dated February 4, 2011).



***Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011***

---

11. *The Applications Development Function's Quality Assurance Program Office Can Make Its Processes More Effective* (Reference Number 2011-20-007, dated February 17, 2011).
12. *Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected* (Reference Number 2011-20-044, dated May 4, 2011).
13. *Access Controls for the Automated Insolvency System Need Improvement* (Reference Number 2011-20-046, dated May 16, 2011).
14. *Corrective Actions to Address the Disaster Recovery Material Weakness Are Being Completed* (Reference Number 2011-20-060, dated June 27, 2011).



***Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011***

---

**Appendix II**

***Major Contributors to This Report***

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)  
Kent Sagara, Director  
Jody Kitazono, Audit Manager  
Louis Lee, Lead Auditor  
Charles Ekunwe, Senior Auditor  
Bret Hunter, Senior Auditor  
Esther Wilson, Senior Auditor  
Victor Taylor, Auditor



***Treasury Inspector General for Tax  
Administration – Federal Information Security  
Management Act Report for Fiscal Year 2011***

---

---

**Appendix III**

***Report Distribution List***

Commissioner C  
Office of the Commissioner – Attn: Chief of Staff C  
Deputy Commissioner for Operations Support OS  
Chief Technology Officer OS:CTO  
Chief Counsel CC  
National Taxpayer Advocate TA  
Director, Office of Legislative Affairs CL:LA  
Director, Office of Program Evaluation and Risk Analysis RAS:O  
Office of Internal Control OS:CFO:CPIC:IC  
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM