Audit Report

OIG-13-007

INFORMATION TECHNOLOGY: The Department of the Treasury Federal Information Security Management Act Fiscal Year 2012 Performance Audit

November 9, 2012

Office of
Inspector General

Department of the Treasury

THIS PAGE INTENTIONALLY LEFT BLANK

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

November 9, 2012

MEMORANDUM FOR **NANI COLORETTI**
ACTING ASSISTANT SECRETARY FOR MANAGEMENT

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 – Fiscal Year 2012 Audit of Treasury's Federal Information Security Management Act 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 2012 Performance Audit, November 7, 2012 (Attachment 1)
- Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2012 (Audit No. 2012-20-114), September 28, 2012 (Attachment 2)

The Department of the Treasury Federal Information Security Management Act (FISMA) Fiscal Year 2012 report presents the audit results of Treasury's compliance with FISMA for its unclassified systems. FISMA requires federal agencies, including Treasury, to (1) have an annual independent evaluation performed of their information security programs and practices and (2) report the results of the evaluation to the Office of Management and Budget (OMB). OMB has delegated to the Department of Homeland Security (DHS) the collection of annual FISMA responses. FISMA also 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). As indicated above, TIGTA's audit results are presented in Attachment 2. Appendix IV of Attachment 1 includes our response to DHS's FISMA 2012 Questions for Inspectors General and incorporates the responses from

the TIGTA report as well. 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),[1] we determined that Treasury's information security program for unclassified systems 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 in place or not consistently performed by the Bureau of Public Debt (BPD), the Alcohol and Tobacco Tax and Trade Bureau, Departmental Offices (DO), Office of the Comptroller of the Currency (OCC), and Financial Crimes Enforcement Network (FinCEN).
2. Security incidents were not reported in a timely manner at the Bureau of Engraving and Printing, BPD, and FinCEN.
3. System security plans at OCC and Financial Management Service (FMS) did not fully document all security controls from National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3, and one System Security Plan for FinCEN was not updated to address weaknesses identified in the security assessments.
4. Audit logs were not sufficiently reviewed by FMS and DO in accordance with NIST and Treasury requirements.
5. Plans of Action and Milestones were not tracked in accordance with NIST and Treasury requirements at DO.
6. Vulnerability scanning and remediation was not performed in accordance with Treasury requirements at FMS, United States Mint, DO, BPD, and OCC.
7. Contingency planning and testing controls were not fully implemented or operating as designed at DO and FMS.
8. Backup controls were not in place or were not operating as designed at BPD and Community Development Financial Institution Fund.
9. System configuration settings were not implemented properly at DO and OCC.
10. System baselines were not documented properly at BPD, FMS, and FinCEN.
11. Multifactor authentication was not implemented at FMS.

[1] *FINANCIAL AUDIT: IRS's Fiscal Years 2012 and 2011 Financial Statements* (GAO-13-120, dated November 2012)

KPMG is making 31 recommendations to the responsible officials to address the findings noted above.

TIGTA reported that the IRS's information security program generally complies with FISMA, but improvements are needed as a result of the conditions identified in configuration management, identity and access management, and security training.

In addition, GAO reported IRS's information security over financial reporting systems as a significant deficiency, which was previously reported as a long-standing material weakness.

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 2012 Performance Audit,
November 7, 2012

THIS PAGE INTENTIONALLY LEFT BLANK

The Department of the Treasury
Federal Information Security Management Act
Fiscal Year 2012 Performance Audit

November 7, 2012

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

The Department of the Treasury
Federal Information Security Management Act Fiscal Year 2012 Performance Audit

Table of Contents

FISMA Performance Audit Report

BACKGROUND 4
Federal Information Security Management Act (FISMA) 4
Federal Standards and Guidelines 4
Department of the Treasury Bureaus/Offices (Bureaus) 5
Department of the Treasury Information Security Management Program 6
OVERALL AUDIT RESULTS 9
FINDINGS 12
1. Logical account management activities were not in place or were not consistently performed by the bureaus at BPD, TTB, DO, OCC, and FinCEN 12
2. Security incidents were not reported in a timely manner at BEP, BPD, and FinCEN 13
3. System security plans at OCC and FMS did not fully document all security controls from NIST SP 800-53, Rev. 3, and one SSP for FinCEN was not updated to address weaknesses identified in the security assessments 15
4. Audit logs were not sufficiently reviewed by FMS and DO in accordance with NIST and Department of the Treasury requirements 15
5. POA&Ms were not tracked in accordance with NIST and Department of the Treasury requirements at DO 16
6. Vulnerability scanning and remediation was not performed in accordance with Department of the Treasury requirements at FMS, Mint, DO, BPD, and OCC 17
7. Contingency planning and testing controls were not fully implemented or operating as designed at DO and FMS 18
8. Backup controls were not in place or were not operating as designed at BPD and CDFI Fund 19
9. System configuration settings were not implemented properly at DO and OCC 20
10. System baselines were not documented properly at BPD, FMS, and FinCEN 20
11. Multifactor authentication was not implemented at FMS 21
MANAGEMENT RESPONSE TO THE REPORT 22

Appendices

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY 34
APPENDIX II – STATUS OF PRIOR-YEAR FINDINGS 38
APPENDIX III – THE DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS's FISMA 2012 QUESTIONS FOR INSPECTORS GENERAL 53
APPENDIX IV – APPROACH TO SELECTION OF SUBSET OF SYSTEMS 64
APPENDIX V – SELECTED SECURITY CONTROL CLASSES AND FAMILIES 66
APPENDIX VI – SUMMARY OF OTHER IT FINDINGS FROM TREASURY FINANCIAL STATEMENT AUDITS 70
APPENDIX VII – GLOSSARY OF TERMS 75

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

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

Re: The United States Department of the Treasury Federal Information Security Management Act Fiscal Year 2012 Performance Audit

Dear Mr. Thorson:

This report presents the results of our independent evaluation of the United States 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. DHS has prepared the FISMA 2012 questionnaire to collect these responses. Appendix III, *The Department of the Treasury's Consolidated Response to DHS's FISMA 2012 Questions for Inspectors General,* provides the Treasury's response to the questionnaire. 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. 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The objective for this performance audit was to determine the effectiveness of the Department of the Treasury's information security program and practices for the period July 1, 2011 to June 30, 2012 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-selected Department of the Treasury information systems. The scope of our work did not include the Internal Revenue Service (IRS), as the component was audited by the Department of the Treasury Inspector General for Tax Administration (TIGTA). The TIGTA report will be appended to this report and the findings of that report will be incorporated

within Appendix III, *The Department of the Treasury's Consolidated Response to DHS's FISMA 2012 Questions for Inspectors General*. Additional details regarding the scope of our performance audit are included in the *Objective, Scope & Methodology* section of this report.

Based on our audit work, we concluded that the United States 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 in place or not consistently performed by the Bureau of Public Debt (BPD), the Alcohol and Tobacco Tax and Trade Bureau (TTB), Departmental Offices (DO), Office of the Comptroller of the Currency (OCC), and Financial Crimes Enforcement Network (FinCEN).
2. Security incidents were not reported in a timely manner at the Bureau of Engraving and Printing (BEP), BPD, and FinCEN.
3. System security plans at OCC and Financial Management Service (FMS) did not fully document all security controls from NIST Special Publication (SP) 800-53, Revision (Rev.) 3, and one System Security Plan (SSP) for FinCEN was not updated to address weaknesses identified in the security assessments.
4. Audit logs were not sufficiently reviewed by FMS and DO in accordance with NIST and Department of the Treasury requirements.
5. Plans of Action and Milestones (POA&Ms) were not tracked in accordance with NIST and Department of the Treasury requirements at DO.
6. Vulnerability scanning and remediation was not performed in accordance with Department of the Treasury requirements at FMS, United States Mint (Mint), DO, BPD, and OCC.
7. Contingency planning and testing controls were not fully implemented or operating as designed at DO and FMS.
8. Backup controls were not in place or were not operating as designed at BPD and **Community Development Financial Institution (**CDFI) Fund.
9. System configuration settings were not implemented properly at DO and OCC.
10. System baselines were not documented properly at BPD, FMS, and FinCEN.
11. Multifactor authentication was not implemented at FMS.

We have made 31 recommendations related to these control deficiencies that, if addressed by management, will strengthen the respective bureaus, offices, and the Department of the Treasury's information security program. In a written response, the Treasury Chief Information Officer (CIO) agreed with our findings and recommendations and provided corrective action plans (see *Management Response*). The Department of Treasury's planned corrective actions are responsive to the intent of our recommendations. We tested controls for the period July 1, 2011

to June 30, 2012. 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 describes the FISMA audit's objective, scope, and methodology. Appendix II, *Status of Prior-Year Findings*, summarizes the Department of the Treasury's progress in addressing prior-year recommendations. Appendix III provides *The Department of the Treasury's Consolidated Response to DHS's FISMA 2012 Questions for Inspectors General*. Appendix IV, *Approach to Selection of Subset of Systems*, describes how we selected systems for review. Appendix V, *Selected Security Control Classes and Families*, describes the selected NIST SP 800-53, Rev. 3, security controls reviewed for each of the selected systems. Appendix VI summarizes IT security findings identified from the Department of the Treasury's financial statement audit at non-IRS bureaus that impact FISMA compliance, and Appendix VII contains a glossary of terms used in this report.

Sincerely,

KPMG LLP

November 7, 2012

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 Inspectors General (IGs) in complying with requirements of FISMA. The Act is supported by Office of Management and Budget (OMB), agency security policy, and risk-based standards and guidelines published by National Institute of Standards and Technology (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 the Department of Homeland Security (DHS) in memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*, for the operational aspects of Federal cyber security, 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: Security Control Classes and Families

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

Source: NIST Special Publication 800-53 Revision 3

Department of the Treasury Bureaus/Offices (Bureaus)

The Department of the Treasury consists of 13 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 United States paper currency, 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 United States Department of the 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 information technology (IT) Security Policy.
6. **Financial Crimes Enforcement Network (FinCEN) – S**upports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes. It also provides United States policy makers with strategic analyses of domestic and worldwide trends and patterns.
7. **Financial Management Service (FMS) – R**eceives 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 United States.
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 the Department of the Treasury programs and operations. The OIG also keeps the Secretary and the Congress fully and currently informed about problems, abuses, and deficiencies in the Department of the Treasury programs and operations.
11. **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 United States coins to the Federal Reserve banks as well as maintains physical custody and protection of our nation's silver and gold assets.
12. **Special Inspector General for the Troubled Asset Relief Program (SIGTARP) – H**as 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).
13. **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 our 2012 FISMA audit did not include the IRS, which was audited by TIGTA. The TIGTA report will be appended to this report and the findings of that report will be incorporated within Appendix III, *The Department of the Treasury's Consolidated Response to DHS's FISMA 2012 Questions for Inspectors General*.

Department of the 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 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 the Department of the Treasury's bureaus. The OCIO Cyber Security Program's mission focuses on the following areas:

1. **Cyber Security Policy** – Manages and coordinates the Departmental cyber security policy for sensitive (unclassified) systems throughout the Department of the Treasury, assuring these policies and requirements are updated to address today's threat environment, and conducts program performance, progress monitoring, and analysis.
2. **Performance Monitoring and Reporting** – Implements collection of Federal and Department of the Treasury-specific security measures and reports those to national authorities and in appropriate summary or dashboard form to senior management, IT managers, security officials, and Bureau officials. For example, this includes preparation and submission of the annual FISMA report and more frequent continuous monitoring information through CyberScope.
3. **Cyber Security Reviews** – Conducts technical and program reviews to help strengthen the overall cyber security posture of the Department of the Treasury and meet their oversight responsibilities.
4. **Enterprise-wide Security** – Works with the Bureaus' and the Department of the Treasury's Government Security Operations Center to deploy new Department of the Treasury-wide capabilities or integrate those already in place, as appropriate, to strengthen the overall protection of the Department of the Treasury. Examples include implementation of Domain Name System Security Extensions, an automated asset inventory, and Department of the Treasury-wide security-related audit findings. Includes addressing the Department of the Treasury'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 of the Treasury'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 of the Treasury-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 Computer Security Incident Response Center (CSIRC) within the Department of the Treasury.
7. **National Security Systems** – Manages and coordinates the Department of the Treasury-wide program to address the cyber security requirements of national security systems through the development of policy and program or technical security performance reviews.
8. **Cyber Security Sub-Council (CSS) of the CIO Council** – Operates to serve as the formal means for gaining bureau input and advice as new policies are developed, enterprise-wide activities are considered, and performance measures are developed and implemented; provides a structured means for information-sharing among the bureaus.

The 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 Volume I, *Treasury Information Technology Security Program*, as the Department of the Treasury IT security policy to provide for information security for all information and information systems that support the mission of the Department of the Treasury, including those operated by another Federal agency or contractor on behalf of the Department of the Treasury. In addition, as OMB periodically releases updates/clarifications of FISMA or as NIST releases updates to publications, the ACIOCS and the Cyber Security Program have

responsibility to interpret and release updated policy for the Department of the Treasury. The ACIOCS and the Cyber Security Program are also responsible for promoting and coordinating a Department of the Treasury IT security program, as well as monitoring and evaluating the status of Department of the Treasury's IT security posture and compliance with statutes, regulations, policies, and guidance. Lastly, the ACIOCS has the responsibility of managing Department of the Treasury's IT Critical Infrastructure Protection (CIP) program for Department of the Treasury IT assets.

Bureau CIOs

Organizationally, the Department of the Treasury has established bureau-level and office (bureau) 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.

Department of the Treasury – Bureau OCIO Collaboration

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

OVERALL AUDIT RESULTS

We concluded that the Department of the Treasury's information security program and practices for its non-IRS bureaus' unclassified systems were generally consistent[1] with the FISMA legislation and related information security policies, standards, and guidelines. However, they were not fully effective, resulting in the identification of 11 categories of control weaknesses and 31 recommendations that the bureaus, offices, and the Department of the Treasury should address to strengthen their information security management programs. The *Findings* section of this report presents the detailed findings and associated recommendations. In a written response to this report, the Treasury CIO agreed with our findings and recommendations and provided corrective action plans (see *Management Response*). The Department of Treasury's planned corrective actions are responsive to the intent of our recommendations.

Additionally, we evaluated all prior-year findings from the fiscal year (FY) 2011 FISMA Performance Audit and noted that 20 of 28 findings had been closed by management. For 3 of the 28 findings, we were unable to test the implementation of the findings in time by our end of fieldwork date, June 30, 2012. For these findings, we noted that they are closed but untested and should be evaluated as part of the FY 2013 independent evaluation. See Appendix II, *Status of Prior-Year Findings*, for additional details.

Summaries of the 11 categories of control weaknesses follow:

1. **Logical account management activities were not in place or not consistently performed by BPD, TTB, DO, OCC, and FinCEN.**

   Logical account management activities were not in place or activities, such as disabling accounts of users that no longer need access and documenting of access approvals, were not consistently performed at BPD, TTB, DO, OCC, and FinCEN. By not establishing and consistently performing access management activities, there is an increased risk that potentially unauthorized access, disclosure, and changes could occur within the IT infrastructure.

2. **Security incidents were not reported in a timely manner at BEP, BPD, and FinCEN.**

   There were untimely reporting of incidents at BEP, BPD, and FinCEN. These bureaus had United States Computer Emergency Readiness Team (US-CERT) Category (CAT) 1 security incidents that were reported after the timelines had 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 OCC and FMS did not fully document all security controls from NIST SP 800-53 Rev. 3, and one SSP for FinCEN was not updated to address weaknesses identified in the security assessments.**

   OCC and FMS relied on system security plans (SSP) that did not contain all of the security controls required by NIST SP 800-53, Rev. 3, and FinCEN had not updated an SSP to reflect and address self-identified control weaknesses. NIST SP 800-53, Rev. 3, was issued in August 2009, and agencies were required to implement this guidance one year after issuance. Failing to select the proper baseline of security controls, or failing to document the results of a risk assessment within a system's SSP, impacts subsequent security activities in the NIST

[1] TIGTA will provide a separate report evaluating the IRS's implementation of the Department of the Treasury's information security program.

Risk Management Framework. Therefore, system security controls may not appropriately or sufficiently protect the confidentiality, integrity, and availability of sensitive bureau information.

4. **Audit logs were not sufficiently reviewed by FMS and DO in accordance with NIST and Department of the Treasury requirements.**

   FMS and DO did not fully implement NIST auditing and accountability controls as required by NIST and Treasury guidance. By not identifying and reviewing significant audit events, system owners may be unable to identify and mitigate all significant threats to the information system. This could cause Treasury personnel to remain unaware of security incidents that have already taken place, leaving the system in a compromised state for an extended period.

5. **Plans of Action and Milestones (POA&Ms) were not tracked in accordance with NIST and Department of the Treasury requirements at DO.**

   DO did not fully implement POA&M controls as required by NIST and Treasury guidance. By not timely recording and updating identified security weaknesses in their respective systems, DO 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.

6. **Vulnerability scanning and remediation was not performed in accordance with Treasury requirements at FMS, Mint, DO, BPD, and OCC.**

   FMS, Mint, DO, BPD, and OCC did not fully implement NIST vulnerability scanning and flaw remediation controls as required by NIST and Department of the Treasury guidance. Without knowledge of missing security patches, insecure configurations, or application vulnerabilities, Department of the Treasury bureaus could not take steps to mitigate potential vulnerabilities in their information systems. Additionally, lack of timely remediation of vulnerabilities can result in systems being compromised.

7. **Contingency planning and testing controls were not fully implemented or operating as designed at DO and FMS.**

   DO and FMS did not fully implement contingency planning and testing controls as required by NIST and Department of the Treasury guidance. Disaster failover tests are paramount in assuring that in emergencies, systems can recover with the least amount of down time possible. Failure to appropriately test contingency plans could result in the unavailability of critical Department of the Treasury information and information systems in the event of a disaster.

8. **Backup controls were not in place or were not operating as designed at BPD and CDFI Fund.**

   Backup controls were not in place at BPD and that CDFI Fund did not fully implement backup controls as required by NIST and Department of the 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, or national emergency) were to occur. Data that has not been stored off-site on tape or other media could be lost if a disaster were to occur.

9. System configuration settings were not implemented properly at DO and OCC.

DO and OCC lacked sufficient implemented settings as required by TD P 85-01 Volume I. The bureaus self-identified multiple settings that were not in place and that there was no one specific or one overall trend. By not adequately implementing restrictive configuration settings, Treasury bureaus increase the risk of malicious attacks to their systems.

10. System baselines were not documented properly at BPD, FMS, and FinCEN.

BPD, FMS, and FinCEN lacked sufficient baseline documentation as required by TD P 85-01 Volume I. By not adequately documenting configuration baselines, Department of the Treasury bureaus are susceptible to risks when new security threats emerge or system hardware and software is changed.

11. Multifactor authentication was not implemented at FMS.

A selected FMS system lacked sufficient multifactor authentication as required by NIST guidance. Multifactor authentication provides an additional level of security for accounts to prevent unauthorized access within the IT infrastructure.

FINDINGS

1. Logical account management activities were not in place or were not consistently performed by the bureaus at BPD, TTB, DO, OCC, and FinCEN

We identified an inconsistent implementation of logical access controls at BPD, TTB, DO, OCC, and FinCEN. We noted the following:

1. For the two selected BPD systems, BPD management could not provide sufficient supporting documentation evidencing the users' last log-on date or time. As a result, we were unable to test the operating effectiveness of the controls over whether inactive users are disabled. *(See Recommendations #1 and #2.)*

2. Account management activities were not consistently performed as required by TD P 85-01 Volume I, *Treasury Information Technology Security Program*, and bureau-specific policies at TTB, OCC, FinCEN, and DO.
   - TTB had three active user accounts that should have had access revoked. One account, a test account, had last logged in on March 22, 2012 and the account was not deactivated after 60 days of inactivity. Another account was for an individual who had separated in July 2011 but still had an enabled account. Additionally, there was a separated individual whose account was still active 20 days after her departure. TTB management explained that it did not have an automated mechanism to disable inactive accounts due to a technical limitation; therefore, some user accounts were not properly disabled in a timely manner. Additionally, TTB stated that access removal for separated employees was a manual process by each employee's supervisor and that human error occurred. *(See Recommendations #3 and #4.)*
   - For a selected DO system, DO management did not formally document and maintain access request forms for privileged user accounts. This was self-discovered during the systems continuous monitoring test performed in June 2012. While there was a documented corrective action plan in the continuous monitoring report, there was not an updated POA&M item during the FISMA year. *(See Recommendation #5.)*
   - OCC did not incorporate all general support system user accounts of Office of Thrift Supervision (OTS), the bureau that OCC partially took over last year, as part of its access review process. When OTS migrated to OCC, most of the accounts were changed from OTS accounts to OCC accounts. Fourteen users were not transferred over. OCC noticed this when they did their account review and created a POA&M to remediate it. This was a self-reported finding and documented within OCC's POA&M report in the Trusted Agent FISMA (TAF) system and scheduled to be corrected on July 31, 2012.
   - A selected FinCEN system had a user account on the database that had unnecessary access permissions. We noted this was due to database accounts not being sufficiently reviewed for access privileges. This was a self-identified weakness as a result of FinCEN's security assessment and authorization and scheduled to be corrected on January 14, 2013.

These control deficiencies demonstrate that these bureaus did not appropriately implement policies for reviewing user access, disabling or deleting inappropriate user access, and following NIST's concept of least privilege.

By failing to disable the accounts of separated users or inactive users promptly, and by not implementing a periodic review of all user and administrator accounts for inactivity or permissions,

there is an increased risk that users could gain or retain unauthorized access and/or modify production data on their respective systems or the network

We recommend that BPD management:

1. For both selected systems, develop or acquire additional system capability that generates user lists with last log-on dates so that inactive users are automatically disabled in a timely manner.

2. For both selected systems, in the absence of a long-term system capability solution, perform manual monthly reviews of all system user accounts and disable or delete accounts that no longer need access.

We recommend that TTB management:

3. Implement an automated mechanism, a script, or manual review process to ensure inactive accounts are disabled after 60 days of inactivity.

4. Ensure that supervisors are aware of their responsibilities to remove the access of separated employees.

We recommend that DO management:

5. Include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.

Based on the planned corrective actions for OCC and FinCEN, we are not making additional recommendations.

2. Security incidents were not reported in a timely manner at BEP, BPD, and FinCEN

Department of the Treasury bureaus are required to submit all security incidents to the TCSIRC within specified time frames categorized by incident severity. The audit identified incidents that were reported later than the US-CERT and Department of the Treasury recommended guidelines at BEP, BPD, and FinCEN. We noted that all three bureaus reported CAT 1 security incidents later than the deadlines required by TD P 85-01 Volume I, which takes its guidance from US-CERT. Specifically, we noted the following:

- BEP did not report 3 of the 15 sampled security incidents to TCSIRC within the one-hour time period required for a CAT 1 incident. Specifically, one incident was reported 50 minutes late, one incident was reported 65 minutes late, and another incident was not reported until seven days after identification. BEP Help Desk reports incidents to the designated BEP Incident Coordinator, who then forwards the reported incident to the BEP CSIRC Management Team. This two-step process caused delays with the submission of the security incident to TCSIRC within BEP's documented time frames. Additionally, not all Help Desk members had been fully trained to respond to security incidents and properly report them to the BEP CSIRC Management Team. *(See Recommendations #6 and #7.)*
- BPD did not report one out of three security incidents within the required one-hour time period for a CAT 1 incident (the incident took 14 hours to report). The delay was caused by BPD's reliance on United Parcel Service (UPS) to verify the status of a missing package.

BPD followed UPS's advice and waited until the following day when the next UPS delivery was made to ensure that the package was truly lost. *(See Recommendations #8 and #9.)*

- FinCEN did not report 1 of the 12 incidents to TCSIRC within the required one-hour time period for a CAT 1. Specifically, the incident was reported 69 hours after identification. There was only one person responsible for FinCEN's CSIRC reporting, and the incident occurred when this person was out of the office, which delayed reporting until he returned. At the time, there were no backup CSIRC personnel. *(See Recommendation #10.)*

By not reporting security incidents in a timely manner, these bureaus increase the risk of unauthorized access, or denial of service attacks, posed to their information system while the incident remains unreported. Additionally, by not reporting incidents, the bureaus can impair the TCSIRC's and the US-CERT's ability to track, analyze, and act on aggregated incident data.

We recommend that BEP management:

6. Revise the current Incident Response reporting process and written procedures to have the Help Desk send all incidents to the CSIRC group as opposed to the BEP Incident Coordinator.

7. Provide additional training to the Help Desk team members regarding BEP's incident response policies and procedures to ensure they are consistently implemented. Additional training for Help Desk personnel should include the same curriculum used by BEP CSIRC management team members to allow for better understanding of the incident reporting process.

We recommend that BPD management:

8. Ensure that BPD's CSIRC report all CAT 1 incidents to US-CERT within one hour regardless of any additional procedures (follow- up, confirmation, or additional feedback from third party) performed by CSIRC personnel.

9. Provide additional training to the BPD's CSIRC management team regarding BPD's incident response policies and procedures to ensure that all incidents are reported in time regardless of reliance on third parties to confirm incident.

We recommend that FinCEN management:

10. Evaluate its current CSIRC capability for collecting and submitting incident responses and implement backup CSIRC personnel to ensure that incident response tickets are handled in a timely fashion.

3. System security plans at OCC and FMS did not fully document all security controls from NIST SP 800-53, Rev. 3, and one SSP for FinCEN was not updated to address weaknesses identified in the security assessments

NIST and Department of the Treasury guidance require that Department of the Treasury SSPs remain up-to-date and current with the NIST Risk Management Framework and required NIST SP 800-53, Rev. 3, security controls. Specifically, we noted that:

- The two selected information systems from OCC did not include all required security controls in areas such as access control, audit and accountability, contingency planning, identification and authentication, maintenance, media protection, system and communications protection, and system and information integrity, as specified in NIST SP 800-53, Rev. 3. We noted that the conditions cited above occurred because OCC management did not perform an adequate review of the two selected systems' SSPs and overlooked the lack of these controls and control enhancements when updating the SSPs. *(See Recommendations #11 and #12.)*
- The SSP for a selected FMS system did not reflect the current and primary source of backups for the application. FMS management stated that the error was due to a management oversight when updating the SSP. *(See Recommendation #13.)*
- FinCEN's SSP for the selected system did not reflect the results of their latest Security Assessment and Authorization, which required certain controls to be updated to reflect self-identified weaknesses. It was noted that this was a self-reported finding and was listed as a POA&M with the TAF system with an estimated date of completion of January 14, 2013.

Failing to document an up-to-date baseline of security controls may have a negative effect on subsequent security activities. Specifically, OCC, FinCEN, and FMS may not be able to properly implement, assess, authorize, and monitor the security controls for the selected systems; therefore, the system security controls may not be sufficient to protect the confidentiality, integrity, and availability of sensitive bureau information.

We recommend that OCC management:

11. For both selected systems, update the SSP to address and reference all the NIST SP 800-53, Rev. 3, security controls and control enhancements for a Moderate baseline.

12. For both selected systems, ensure management conducts an adequate review of the SSPs to ensure that it includes applicable NIST SP 800-53, Rev. 3, controls.

We recommend that FMS management:

13. Update the selected system's SSP to reflect the current and primary source of backups for the application.

Based on the planned corrective actions for FinCEN, we are not making a recommendation.

4. Audit logs were not sufficiently reviewed by FMS and DO in accordance with NIST and Department of the Treasury requirements

NIST SP 800-53, Rev. 3, and TD P 85-01 Volume I require that government information systems owners and security managers identify and review 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. We noted the following:

- A selected FMS system's audit capabilities and functions did not adhere to the Fiscal Service Baseline Services Requirements (BLSR) and NIST SP 800-53, Rev. 3, guidance as required for HIGH categorized systems. Specifically, it did not have any automated capabilities or any supporting processes to log and monitor security-relevant events. When designing the system, FMS management did not adequately identify requirements and provide capabilities to log and monitor security-related events. In addition, management did not establish a robust monitoring process to support the review and follow-up of selected auditable events, and management did not document within their system security plan specific security-related events that will be monitored on an ongoing basis. *(See Recommendations #14, #15, and #16.)*
- A selected DO system lacked a process to review audit records. DO management self-identified this weakness during a continuous monitoring assessment in June 2012. While there was a documented corrective action plan in the continuous monitoring report, there was not an updated POA&M item during the FISMA year. *(See Recommendation #17.)*

By not adhering to NIST guidance over audit log review policies, IT security personnel would be unable to identify and mitigate significant threats to the information system. Additionally, this could cause Department of the Treasury personnel to remain unaware of security incidents that have already taken place, leaving the system in a compromised state for an extended period.

We recommend that FMS management:

14. Enhance the selected system audit capabilities to capture security-related events as prescribed by the BLSR and NIST SP 800-53 guidance.

15. Establish a clear oversight process to review the security-related events and ensure appropriate follow-up action is taken as prescribed by the BLSR and NIST SP 800-53.

16. Update the selected system's system security plan to document security-related events that need to be monitored as prescribed by the BLSR.

We recommend that DO management:

17. Include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.

5. POA&Ms were not tracked in accordance with NIST and Department of the Treasury requirements at DO

Department of the Treasury has provided guidance on POA&M creation and tracking through TD P 85-01 Volume I. This policy requires Department of the Treasury bureaus to maintain POA&Ms in order to help remedy 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. We noted that a selected DO system had multiple identified weaknesses identified in the June 2012 continuous monitoring test report that were not documented in the system POA&M. DO bureau policy requires that POA&Ms be inputted 30 days after the

weaknesses are initially identified. The lack of these findings being added to the POA&M was an oversight by DO management when updating the system POA&M. *(See Recommendations #18 and #19.)*

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

We recommend that DO management:

18. Update the selected system POA&M with the findings and recommendations reported in the system continuous monitoring test report.

19. Ensure the continuous monitoring test results and recommendations are captured within the selected system POA&M within the 30-day required period.

6. Vulnerability scanning and remediation was not performed in accordance with Department of the Treasury requirements at FMS, Mint, DO, BPD, and OCC

TD P 85-01 Volume I 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 way are required to be remedied in a timely manner, or, if a vulnerability cannot be remedied in a timely manner, tracked in a POA&M until the remediation actions are complete. We noted that five bureaus did not implement Department of the Treasury policy adequately. Specifically, we noted the following:

- For a selected FMS system, FMS was unable to provide us with supporting documentation confirming that vulnerability scans were being performed over the system's Internet Protocol (IP) addresses. Therefore, we could not determine if vulnerability scans had been performed, if any vulnerabilities were identified, and if any corresponding corrective actions or POA&M had been implemented *(See Recommendations #20 and 21.)*
- For a selected Mint system, the November 2011 vulnerability scan contained vulnerabilities with a high risk rating that were not remedied prior to the March 2012 vulnerability scans. The Mint POA&M report from TAF, generated in June 2012, did not reflect the open vulnerabilities. These vulnerabilities were not properly remedied due to the Mint's management decision to remediate noncritical vulnerabilities using a risk-based approach. This risk-based approach did not address all noncritical vulnerabilities in a timely manner and deviated from the Mint's vulnerability remediation policy, which requires noncritical patches to be applies on a bimonthly basis. *(See Recommendation #22.)*
- For the selected DO system, DO management identified multiple high-risk weaknesses in vulnerability scans and missing scans for database components during DO's continuous monitoring assessment in 2012. While a documented corrective action plan was established in the continuous monitoring report, the weaknesses were not recorded in the POA&M during the FISMA year. *(See Recommendation #23.)*
- For both selected BPD systems, BPD management identified that there were insufficient procedures over vulnerability remediation in place. This was a self-reported finding and

documented within BPD's POA&M report on TAF. The POA&M item is scheduled to be completed on June 30, 2013.

- For both selected OCC systems, OCC management identified multiple high-risk weaknesses in vulnerability scans that were not remediated. This was a self-reported finding and documented within OCC's POA&M report on TAF. The POA&M item is scheduled to be completed on August 15, 2012.

Without knowledge of missing security patches, insecure configurations, or application vulnerabilities, Department of the Treasury bureaus might 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, altered, or deleted.

We recommend that FMS management:

20. Formally document the vulnerability scanning and flaw remediation processes for the Fiscal Services organization and communicate the processes to affected field personnel.

21. Maintain a complete listing of hosts and IP addresses for the selected FMS system production environment and document any changes to this listing, and retain enough supporting documentation to confirm the accuracy of completed vulnerability scans.

We recommend that Mint management:

22. Follow their vulnerability remediation policy for all vulnerabilities, including older, noncritical patches, to ensure that vulnerabilities are not missed in the remediation process.

We recommend that DO management:

23. Include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.

Based upon the planned correction actions for BPD and OCC, we are not making a recommendation.

7. Contingency planning and testing controls were not fully implemented or operating as designed at DO and FMS

Treasury guidance requires its bureaus to protect their information systems in the event of a disaster. Bureaus must create plans for system recovery and test these plans. Two Treasury bureaus did not fully implement contingency planning (planning and testing) controls as required by TD P 85-01 Volume I 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. Specifically, we noted the following:

- Contingency plan documentation for a selected DO system was not updated within the FISMA year. Additionally, contingency plan testing was not performed for the system within the FISMA year. DO management self-identified these weaknesses during a continuous monitoring assessment in June 2012. While there was a documented corrective action plan in the continuous monitoring report, there was not an updated POA&M item during the FISMA year. *(See Recommendation #24.)*

- For one selected FMS system, FMS management identified the contingency plan test was not performed within the FISMA year. This was a self-reported finding and documented within FMS's POA&M report on TAF, with an estimated completion date of August 30, 2012.
- For another selected FMS system, FMS management identified one of three disaster recovery exercise reconstitution test objectives was not completed during contingency plan testing. This was a self-reported finding and documented within FMS's POA&M report on TAF, with an estimated completion date of August 30, 2012.

Contingency plans and contingency plan testing, as required by NIST SP 800-34, are paramount in assuring that Department of the 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 Department of the Treasury information and information systems in the event of a disaster.

We recommend that DO management:

24. Include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.

Based on the planned corrective actions for FMS, we are not making a recommendation.

8. Backup controls were not in place or were not operating as designed at BPD and CDFI Fund

We identified insufficient implementation of backup controls at BPD and CDFI Fund. Specifically, we noted the following:

- BPD management could not provide sufficient supporting documentation evidencing that the backup jobs were run successfully. As a result, we were unable to test the operating effectiveness of the controls over backups. The weekly backup logs did not specify whether the selected backup jobs were successful or had failed. BPD stated that the system was not configured to include the backup status on the logs. *(See Recommendation #25.)*
- Backups of CDFI Fund data for the selected system were not being performed on a regular basis. Upon inspection of all successful backups between December 2011 and April 2012, it was noted that backups of data were occurring, but the frequency ranged from two to seven times a month. This did not comply with the SSP, which indicated that daily incremental backups and a weekly full backups occur. CDFI Fund stated that TTB took over the backup responsibilities in May 2012, and, as a result of the upcoming transition, evidence for successful backups was not maintained. *(See Recommendation #26.)*

Department of the 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. Two Department of the Treasury bureaus did not fully implement backup controls as required by TD P 85-01 Volume I, 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. Lack of frequent, successful backups can have a significant negative effect on Department of the Treasury information systems if a disaster (i.e., hard-drive failure, natural disaster, and national emergency) were to occur. Data can be lost and successful system restoration thwarted if backup are not available.

We recommend that BPD management:

25. Enhance the logging capability of the system's backup process so management can determine whether the backups were successfully completed.

We recommend that CDFI Fund management:

26. Ensure that the system backups are completed successfully per the defined frequency in the SSP, and retain evidence of successful completion for one year.

9. System configuration settings were not implemented properly at DO and OCC

TD P 85-01, Volume I, requires its bureaus to implement restrictive configuration settings levels and to detect and track unauthorized changes to the information system. This is to protect information integrity and confidentiality. By not adequately implementing restrictive system configuration settings, DO and OCC reduce their ability to protect against malicious attacks. We noted the following:

- A selected DO system lacked sufficient mechanisms to track and detect unauthorized changes. DO management self-identified these weaknesses during a continuous monitoring assessment in June 2012. While there was a documented corrective action plan in the continuous monitoring report, there was not an updated POA&M item during the FISMA year. *(See Recommendation #27.)*
- For both selected OCC systems, OCC management identified configuration settings were not set to the most restrictive settings possible. Both systems had multiple weaknesses identified in configuration settings that did not meet the require threshold for restrictive settings as stated by NIST. This was a self-reported finding and documented within OCC's POA&M report on TAF. The POA&M item is scheduled to be completed on December 31, 2013.

We recommend that DO management:

27. Include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.

Based upon the planned correction actions for OCC, we are not making a recommendation.

10. System baselines were not documented properly at BPD, FMS, and FinCEN

TD P 85-01, Volume I, requires that Treasury bureaus document configuration baselines. TD P 85-01, Volume I, uses The Federal Enterprise Architecture Framework, Version 1.1, as guidance to federal bureaus on how to establish enterprise architecture over IT systems. These mechanisms are in place to establish security standards for information systems to protect from threats and vulnerabilities. By not adequately documenting and implementing system baselines, BPD, FMS, and FinCEN increase the risk of vulnerabilities being exposed on the system. We noted the following:

- Both selected BPD systems did not have baseline configurations formally documented. BPD management was aware of the lack of this documentation for both systems; however, management had planned to rely on system backups to restore system information in case of a disaster event. *(See Recommendation #28.)*

- A selected FMS system lacked sufficient system baseline documentation. Specifically, the baseline documentation did not establish operational requirements. Moreover, documentation of the following elements did not exist: mandatory configuration settings for the information system components to reflect the most restrictive mode; list of authorized and unauthorized programs; and mechanisms to verify configuration settings and respond to unauthorized changes. The selected system Configuration Management Plan did not provide a clear distinction between program change control and system configuration management processes identified in the FMS Entity-Wide IT Standards. The lack of clarity and baseline features within the selected system Configuration Management Plan was overlooked by FMS management when establishing the plan. *(See Recommendations #29, #30, and #31.)*
- KPMG confirmed that, for a selected FinCEN system, FinCEN management identified the baseline settings were outdated. This was a self-reported finding and documented within FinCEN's POA&M report on TAF. The POA&M item is scheduled to be completed on January 14, 2013.

We recommend that BPD management:

28. For both selected systems, develop baseline configurations (application build guides) that are consistent with the system's SSP and Federal Enterprise Architecture.

We recommend that FMS management:

29. Clarify the distinction between program change control and system configuration management within the FMS Entity-Wide IT Standards and the selected system Configuration Management Plan by documenting and considering correcting gaps in the current process and work flow to clearly outline work flow, tasks, and management oversight.

30. Update the selected system Configuration Management Plan to establish operational requirements and document the following elements: mandatory security relevant configuration settings, description of the controls to address unauthorized security relevant changes to the configuration of the system, and a list of authorized/unauthorized changes.

31. Document a secure baseline and mandatory configuration settings for the information system components in the selected system Configuration Management Plan to reflect the most restrictive mode in support of the security controls for the system.

Based upon the planned correction actions for FinCEN, we are not making a recommendation.

11. Multifactor authentication was not implemented at FMS

NIST SP 800-53, Rev. 3, guidance requires systems to implement multifactor authentication to local and network access to privileged and nonprivileged accounts. Multifactor authentication provides an additional level of security for accounts to prevent unauthorized access within the IT infrastructure. KPMG confirmed that, for the selected FMS system, FMS management identified it did not implement multifactor authentication for any level of access to the system. This was a self-reported finding and documented within FMS's POA&M report on TAF. The POA&M item is scheduled to be completed on December 31, 2012.

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

MANAGEMENT RESPONSE TO THE REPORT

The following is the OCIO's response, dated October 12, 2012, to the FY 2012 FISMA Performance Audit Report.

October 12, 2012

MEMORANDUM FOR JOEL GROVER
DEPUTY ASSISTANT INSPECTOR GENERAL
FOR FINANCIAL MANAGEMENT AND
INFORMATION TECHNOLOGY AUDIT

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

SUBJECT: Management Response to Draft Audit Report – "FY 2012 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 2012 Audit of Treasury's Federal Information Security Management Act (FISMA) Implementation for Its Unclassified Systems." We are pleased that the report found that our security program is generally consistent with FISMA legislation, OMB information security requirements and related information security standards published by the National Institute of Standards and Technology. We have carefully reviewed the draft and agree with all findings and recommendations. Please refer to the attachment for further details on our planned corrective actions. We appreciate your noting that some of the findings were actually items identified by Bureaus through their security programs.

The Department remains committed to improving its security program. We have made notable progress over the past year. For example we closed all but six of the forty-three recommendations from last year's FISMA audit. Also, as the Department continues to transition to OMB's eventual goal of "real-time" reporting capability, we have accomplished a number of achievements, to include:

- Initiated, and continue to expand the Treasury Continuous Monitoring and Automation (CMA) Program. When fully implemented, CMA will provide a centralized Departmental means for the automated collection, correlation, and analysis of data regarding the IT security posture across Treasury.

- Re-aligned and updated the Department's core cybersecurity policies to be consistent with the latest federal policies and guidelines to protect our information systems from potential adversaries and other threats.

- Received DHS and OMB approval for three new Trusted Internet Connections (TICs) at the IRS and deployed DHS Einstein security sensors at each of these sites. This resulted in an increase of the Department's overall Internet traffic traversing an approved TIC from 4% to over 95%. Information collected via

these sensors is used by DHS to detect and correlate potential cyber security threats throughout the federal government.

- Increased the level of compliance with the OMB policy requirement for Domain Name System Security Extensions (DNSSEC) from 14% in FY 2011 to 65% in FY 2012. This is important to reduce the ability of others to impersonate Treasury websites. This mandate is monitored weekly.

- Addressed a key OMB goal of enhancing automated security data feeds from bureaus to the OMB secure data site. This was raised from 15% in FY 2011 to over 83% in FY 2012. These automated feeds provide both OMB and DHS the ability to conduct continuous monitoring of asset, vulnerability and security configuration management across the government.

We appreciate the audit recommendations because they will help improve our security posture. If you have any questions, please contact Edward Roback, Associate CIO for Cyber Security, at 202-622-2593.

Attachment

cc: Edward A. Roback

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

(U) OIG Finding 1: Logical account management activities were not in place or were not consistently performed by the bureaus at BPD, TTB, DO, OCC and FinCEN

(U) OIG Recommendation 1: For Bureau of the Public Debt (BPD), we recommend that management: For both selected systems, develop or acquire additional system capability that generates user lists with last log-on dates so that inactive are automatically disabled in a timely manner.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. BPD will develop or acquire additional system capability that generates user lists with last logon dates so that inactive users are automatically disabled in a timely manner. Target completion: June 30, 2013
>
> **(U) Responsible Official:** Bureau of Fiscal Service (BFS), Acting Chief Information Security Officer (CISO)

(U) OIG Recommendation 2: For BPD, we recommend that management: For both selected systems, in the absence of a long-term system capability solution, perform manual monthly reviews of all system user accounts and disable or delete accounts that no longer need access.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. In the absence of a long term system capability solution, BPD will perform manual monthly reviews of all user accounts for both selected systems, and disable or delete accounts that no longer need access. Target completion: June 30, 2013
>
> **(U) Responsible Official:** BFS, Acting CISO

(U) OIG Recommendation 3: For Alcohol and Tobacco Tax Bureau (TTB), we recommend that management: Implement an automated mechanism, a script, or manual review process to ensure inactive accounts are disabled after 60 days of inactivity.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. All three noted accounts have been deleted. Based on the findings and recommendations, TTB has already implemented a mechanism to examine and disable inactive accounts. An automated script has been deployed that examines Active Directory accounts and checks various attributes to determine if any of the accounts have been inactive for over 60 days and the password has not been changed in 90 days. If the script finds an account that meets this criterion, the script disables the user account and creates a log fine for system Administration review and action. Completed: August 6, 2012
>
> **(U) Responsible Official:** TTB, Assistant Chief Information Officer (ACIO) for Information Technology (IT) Security, Chief Information Security Office/Information System Security Officer (CISO/ISSO)

(U) OIG Recommendation 4: For TTB, we recommend that management: Ensure that supervisors are aware of their responsibilities to remove the access of separated employees.

(U) Treasury Response: Treasury agrees with the finding and recommendation. TTB has sent out written communications to all supervisors stressing the need to follow the Automated Information System (AIS) Security Program Procedures and to submit timely e7200 user removal requests. Completed: August 20, 2012

(U) Responsible Official: TTB, ACIO for IT CISO/ISSO

(U) OIG Recommendation 5: For Departmental Offices (DO), we recommend that management: Include the corrective action plans from the selected system's continuous monitoring report into a POA&M [Plan of Action and Milestones] item.

(U) Treasury Response: The corrective action plans from the selected DO system continuous monitoring report has been created in Trusted Agent FISMA as a POA&M item. Completed: August 15, 2012

(U) Responsible Official: DO, ISSO for the appropriate system.

(U) OIG: Based on the planned corrective actions for OCC [Office of the Comptroller of the Currency] and FinCEN [Financial Crimes Enforcement Network], we are not making additional recommendations.

(U) OIG Finding 2: Security incidents were not reported in a timely manner at BEP, BPD, and FinCEN

(U) OIG Recommendation 6: For Bureau of Engraving and Printing (BEP), we recommend that management: Revise the current Incident Response reporting process and written procedures to have the helpdesk send all incidents to the CSIRC [Computer Security Incident Response Center] group as opposed to the BEP Incident Coordinator.

(U) Treasury Response: Treasury agrees with the finding and recommendation. BEP will work with Treasury to evaluate and modify as necessary its incident response reporting process and procedures to meet the objective of the recommendation. Additionally, Treasury will review its Department-wide incident response reporting policy, and, if appropriate, coordinate with other agencies with Federal-wide policy setting authority on the lack of identifiable utility of the "one-hour rule" for reporting of fully encrypted devices." Target completion: February 1, 2013

(U) Responsible Official: BEP CIO, BEP CISO, and Treasury CISO

(U) OIG Recommendation 7: For BEP, we recommend that management: Provide additional training to the Help Desk team members regarding BEP's incident response policies and procedures to ensure they are consistently implemented. Additional training for Help Desk personnel should include the same curriculum used by BEP CSIRC management team members to allow for better understanding of the incident reporting process.

(U) Treasury Response: Treasury agrees with the finding and recommendation. BEP will ensure that all its incident response team members (i.e., Help Desk) receive training commensurate with their duties and responsibilities. Target completion: January 31, 2013

(U) Responsible Official: BEP, CIO and BEP CISO

(U) OIG Recommendation 8: For BPD, we recommend that management: Ensure that BPD's CSIRC report all CAT 1 incidents to US-CERT [United State Computer Emergency Readiness Team] within the one (1) hour regardless of any additional procedures (follow up, confirmation or additional feedback from third party) performed by CSIRC personnel.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. Procedures defining CAT I reporting responsibilities are defined in Public Debt's CSIRC Manual. Completed: October 3, 2012
>
> **(U) Responsible Official:** BFS Acting CISO

(U) OIG Recommendation 9: For BPD, we recommend that management: Provide additional training to the BPD's CSIRC management team regarding BPD's incident response policies and procedures to ensure that all incidents are reported in time regardless of reliance on third parties to confirm incident.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. BPD has clarified any perceived ambiguity that existed with regard to reporting CAT I incidents with all applicable employees. Completed: October 3, 2012
>
> **(U) Responsible Official:** BFS, Acting CISO

(U) OIG Recommendation 10: For FinCEN, we recommend that management: Evaluate its current CSIRC capability for collecting and submitting incident responses and implement back-up CSIRC personnel to ensure that incident response tickets are handled in a timely fashion.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. FinCEN's will incorporate an active acknowledgement process via FinCEN CSIRC upon receipt of a security incident and will assign a backup point of contact to ensure that incidents are handled timely. Target completion: December 31, 2012.
>
> **(U) Responsible Official:** FINCEN, CISO

(U) OIG Finding 3: System security plans at OCC and FMS did not fully document all security controls from NIST SP 800-53, Rev. 3, and one SSP [system security plans] for FinCEN was not updated to address weaknesses identified in the security assessments

(U) OIG Recommendation 11: For OCC, we recommend that management: For both selected systems, update the SSP to address and reference all the NIST SP 800-53, Revision 3 security controls and control enhancements for a Moderate baseline.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. OCC has completed updates to the SSPs reviewed by the auditors, verifying that both reference all NIST 800-53, Revision 3 security controls and control enhancements for a Moderate baseline system. Completed: August 23, 2012
>
> **(U) Responsible Official:** OCC, CISO/Chief Privacy Officer (CPO)

(U) OIG Recommendation 12: For OCC, we recommend that management: For both selected systems, ensure management conducts an adequate review of the SSPs [System Security Plan] to ensure that it

includes applicable [National Institute of Standards and Technology Special Publication] NIST SP 800-53, Revision 3 controls.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. OCC is currently in the process of refining its Security Assessment and Authorization (SA&A) document review process to ensure adequate reviews are performed. Target completion: December 16, 2012
>
> **(U) Responsible Official:** OCC, CISO/CPO

(U) OIG Recommendation 13: For Financial Management Service (FMS), we recommend that management: Update the selected system's SSP to reflect the current and primary source of backups for the application.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. FMS will update the SSP to reflect the current and primary source of backups for the application. Target completion:
> June 30, 2013
>
> **(U) Responsible Official:** BFS, Acting CISO

(U) OIG: Based on the planned corrective actions for FinCEN, we are not making a recommendation.

(U) OIG Finding 4: Audit logs were not sufficiently reviewed by FMS and DO in accordance with NIST and Department of the Treasury requirements

(U) OIG Recommendation 14: For FMS, we recommend that management: Enhance the selected system audit capabilities to capture security-related events as prescribed by the [Baseline Services Requirements] BLSR and NIST SP 800-53 guidance.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. FMS will implement the UNIX baseline on the SPS boxes to include auditing capabilities. Target completion: May 31, 2013
>
> **(U) Responsible Official:** BFS, Acting CISO

(U) OIG Recommendation 15: For FMS, we recommend that management: Establish a clear oversight process to review the security-related events and ensure appropriate follow-up action is taken as prescribed by the BLSR and NIST SP 800-53.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. FMS will establish a clear oversight process to review the security-related events and ensure appropriate follow-up action is taken. Target completion: May 31, 2013
>
> **(U) Responsible Official:** BFS, Acting CISO

(U) OIG Recommendation 16: For FMS, we recommend that management: Update the selected system's system security plan to document security-related events that need to be monitored as prescribed by the BLSR.

(U) Treasury Response: Treasury agrees with the finding and recommendation. FMS will update the selected system's security plan to document security-related events that need to be monitored. Target completion: June 15, 2013

(U) Responsible Official: BFS, Acting CISO

(U) OIG Recommendation 17: For DO, we recommend that management: Include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.

(U) Treasury Response: Treasury agrees with the finding and recommendation. The corrective action plans from the selected DO system continuous monitoring report has been created in Trusted Agent FISMA as a POA&M item. Completed: August 15, 2012

(U) Responsible Official: DO, ISSO for the selected system

(U) OIG Finding 5: Plans of Action and Milestones (POA&Ms) were not tracked in accordance with NIST and Department of the Treasury requirements at DO

(U) OIG Recommendation 18: For DO, we recommend that management: Update the selected system POA&M with the findings and recommendations reported in the system continuous monitoring test report.

(U) Treasury Response: Treasury agrees with the finding and recommendation. Departmental Offices respective ISSOs has updated the selected system POA&M in Trusted Agent FISMA with the findings and recommendations reported in the system continuous monitoring test report. Completed: August 15, 2012

(U) Responsible Official: DO, ISSO for the selected system

(U) OIG Recommendation 19: For DO, we recommend that management: Ensure the continuous monitoring test results and recommendations are captured within the selected system POA&M within the 30-day required period.

(U) Treasury Response: Treasury agrees with the finding and recommendation. Departmental Offices respective ISSOs has updated the selected system POA&M in Trusted Agent FISMA with the findings and recommendations reported in the system continuous monitoring test report. Completed: August 15, 2012

(U) Responsible Official: DO, ISSO for the selected system

(U) OIG Finding 6: Vulnerability scanning and remediation was not performed in accordance with Department of the Treasury requirements at FMS, Mint, DO, BPD, and OCC

(U) OIG Recommendation 20: For FMS, we recommend that management: Formally document the vulnerability scanning and flaw remediation processes for the Fiscal Services organization and communicate the processes to affected field-personnel.

(U) Treasury Response: Treasury agrees with the finding and recommendation. FMS will develop and implement an enterprise procedure for vulnerability scanning & remediation. Target completion:
June 30, 2013

(U) Responsible Official: BFS, Acting CISO

(U) OIG Recommendation 21: For FMS, we recommend that management: Maintain a complete listing of hosts and IP addresses for the selected FMS system production environment and document any changes to this listing, and retain enough supporting documentation to confirm the accuracy of completed vulnerability scans.

(U) Treasury Response: Treasury agrees with the finding and recommendation. FMS will ensure that all infrastructure Configuration Items (as defined by Service Asset and Configuration Management Standard) include their FISMA system association as a required element of their CMDB entry. Target completion: May 1, 2013

(U) Responsible Official: BFS, Acting CISO

(U) OIG Recommendation 22: For Mint, we recommend that management: Follow their vulnerability remediation policy for all vulnerabilities, including older, noncritical patches, to ensure that vulnerabilities are not missed in the remediation process.

(U) Treasury Response: Treasury agrees with the finding and recommendation. Mint will institute a new patch remediation procedure that gives patch criticality, instance count, and patch publish date equal weight in the remediation tracking process. This will ensure that all patches are addressed in a timely manner regardless of the instance count in the environment. Target completion: November 30, 2012

(U) Responsible Official: Mint, CISO

(U) OIG Recommendation 23: For DO, we recommend that management: Include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.

(U) Treasury Response: Treasury agrees with the finding and recommendation. The corrective action plans from the selected DO system continuous monitoring report has been created in Trusted Agent FISMA as a POA&M item. Completed: August 15, 2012

(U) Responsible Official: DO, ISSO for the selected system

(U) OIG: Based upon the planned correction actions for BPD and OCC, we are not making a recommendation.

(U) OIG Finding 7: Contingency planning & testing controls were not fully implemented or operating as designed at DO and FMS

(U) OIG Recommendation 24: For DO, we recommend that management: Include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.

(U) Treasury Response: Treasury agrees with the finding and recommendation. The corrective action plans from the selected DO system continuous monitoring report has been created in Trusted Agent FISMA as a POA&M item. Completed: August 15, 2012

(U) Responsible Official: DO, ISSO for the selected system

(U) OIG: Based on the planned corrective actions for FMS, we are not making a recommendation.

(U) OIG Finding 8: Backup controls were not in place or were not operating as designed at BPD and CDFI Fund

(U) OIG Recommendation 25: For BPD, we recommend that management: Enhance the logging capability of the system's backup process so management can determine whether the backups were successfully completed.

(U) Treasury Response: Treasury agrees with the finding and recommendation. BPD will provide detailed logs of selected system's backups and a legend of the current backup logs, which show the volume sets being backed up. Target completion: April 30, 2013

(U) Responsible Official: BFS, Acting CISO

(U) OIG Recommendation 26: For Community Development Financial Institution (CDFI) Fund, we recommend that management: Ensure that the system backups are completed successfully per the defined frequency in the SSP, and retain evidence of successful completion for one year.

(U) Treasury Response: Treasury agrees with the finding and recommendation. The CDFI Fund will ensure that backups are performed successfully per the defined frequency in the SSP, and that TTB retains evidence of successful completion for one year. Target completion: October 31, 2012

(U) Responsible Official: CDFI, CIO

(U) OIG Finding 9: System configuration settings were not implemented properly at DO and OCC

(U) OIG Recommendation 27: For DO, we recommend that management: Include the corrective action plans from the selected system's continuous monitoring report into a POA&M item.

(U) Treasury Response: Treasury agrees with the finding and recommendation. The corrective action plans from the selected DO system continuous monitoring report has been created in Trusted Agent FISMA as a POA&M item. Completed: August 15, 2012

(U) Responsible Official: DO, ISSO for the selected system

(U) OIG: Based upon the planned correction actions for OCC, we are not making a recommendation.

(U) OIG Finding 10: System baselines were not documented properly at BPD, FMS, and FinCEN

(U) OIG Recommendation 28: For BPD, we recommend that management: For both selected systems, develop baseline configurations (applications build guides) that are consistent with the system's SSP and Federal Enterprise Architecture.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. BPD will leverage existing Configuration Management data to ensure all Configuration Items (CIs) necessary to deliver the system are identified. This will include: infrastructure, applications, and supporting services; ensure relationships and dependencies among the identified CIs are documented within the Configuration Management Data Base (CMDB); ensure build guides ("baselines") exist, where appropriate, for all identified CIs; and, ensure a system-level build guide exists, including CI build guides by reference as appropriate. Target completion: June 30, 2013
>
> **(U) Responsible Official:** BFS, Acting CISO

(U) OIG Recommendation 29: For FMS, we recommend that management: Clarify the distinction between program change control and system configuration management within the FMS Entity-Wide IT Standards and the selected system Configuration Management Plan by documenting and considering correcting gaps in the current process and work flow to clearly outline work flow, tasks, and management oversight.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. Due to the fiscal service consolidation, FMS Entity-Wide IT Standards are now obsolete. However, the Fiscal Service will review documentation defining work flow for change control and configuration management, and, if deemed necessary, revise documentation to further clarify workflow, tasks, and management oversight for these two processes. Target completion: March 31, 2013
>
> **(U) Responsible Official:** BFS, Acting CISO

(U) OIG Recommendation 30: For FMS, we recommend that management: Update the selected system Configuration Management Plan to establish operational requirements and document the following elements: mandatory security relevant configuration settings, description of the controls to address unauthorized security relevant changes to the configuration of the system, and a list of authorized/unauthorized changes.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. FMS will review documentation defining work flow for change control and configuration management, and, if deemed necessary, revise documentation to further clarify workflow, tasks, and management oversight for these two processes. Target completion: March 31, 2013
>
> **(U) Responsible Official:** BFS, Acting CISO

(U) OIG Recommendation 31: For FMS, we recommend that management: Document a secure baseline and mandatory configuration settings for the information system components in the selected system Configuration Management Plan to reflect the most restrictive mode in support of the security controls for the system.

> **(U) Treasury Response:** Treasury agrees with the finding and recommendation. FMS will review documentation defining work flow for change control and configuration management,

and, if deemed necessary, revise documentation to further clarify workflow, tasks, and management oversight for these two processes. Target completion: March 31, 2013

(U) Responsible Official: BFS, Acting CISO

(U) OIG: Based upon the planned correction actions for FinCEN, we are not making a recommendation.

(U) OIG Finding 11: Multifactor authentication was not implemented at FMS

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

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY

The objective for this performance audit was to determine the effectiveness of the Department of the Treasury's information security programs and practices for the period July 1, 2011 to June 30, 2012 for its unclassified systems, including and to determine whether non-Internal Revenue Service (IRS) Treasury bureaus had implemented:

- An information security program, consisting of policies, procedures, and security controls consistent with the Federal Information Security Management Act (FISMA) legislation.
- The security controls catalog contained in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 3, *Recommended Security Controls for Federal Information Systems and Organizations*.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS).Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective.

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation, Presidential directives, Department of Homeland Security (DHS) *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics,* dated March 6, 2012, and NIST standards and guidelines as outlined in the *Criteria* section. We reviewed the Department of the Treasury information security program from both the Department-level perspective for Department of the Treasury program-level controls and the Bureau-level implementation perspective. We considered each area above to reach an overall conclusion regarding Department of the Treasury's information security program and practices.

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

PHASE A: Assessment of Department-Level Compliance

To gain an enterprise-level understanding, we assessed management, policies, and guidance for the overall Treasury-wide information security program per requirements defined in FISMA and DHS Federal Information Security Memorandum (FISM) 12-02, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*; NIST SP 800-53, Rev. 3; as well as Department of the Treasury guidelines developed in response to FISMA. This included program controls applicable to information security governance, certification and accreditation, security configuration management (CM), 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 a bureau-level understanding, we assessed the implementation of the guidance for the 12[2] bureau and office wide information security programs according to requirements defined in FISMA and DHS FISM 12-02, NIST SP 800-53, Rev. 3, as well as Department of the Treasury guidelines developed in response to FISMA. This included program controls applicable to information security governance, certification and accreditation (C&A), security configuration management, incident response and reporting, security training, POA&M, remote access, account and identity management, continuous monitoring, contingency planning, and contractor systems.

[2] 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 understanding of how effectively 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 subset of Department of the Treasury information systems (see Appendix V).

Our scope included evaluating the information security practices and policies established by the Treasury Office of the Chief Information Officer (OCIO). In addition, we evaluated the information security practices, policies, and procedures in use across 12 bureaus of the Treasury, excluding the IRS.

We also tested a subset of 15 information systems from a total population of 118 non-IRS major applications and general support systems as of April 3, 2012.[3] We tested the 15 information systems to determine whether bureaus were effective in implementing the Department of the Treasury's security program and meeting the Federal Information Processing Standards (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 10 of 13 Treasury bureaus, excluding IRS, Treasury Inspector General for Tax Administration (TIGTA), and Office of Inspector General (OIG).[4]

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., volatility) 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 non-IRS bureaus. We also evaluated the Department of the Treasury's and bureaus' policies, procedures, and guidelines. Lastly, we evaluated selected security-related documents and records, including C&A packages, configuration assessment results, and training records.

We performed our fieldwork at the Department of the Treasury's headquarters offices in Washington, D.C., and bureau locations in Washington, D.C.; Hyattsville, Maryland; Vienna, Virginia; and Parkersburg, West Virginia, during the period of April 12, 2012 through July 31, 2012. During our performance audit, we met with Department of the Treasury management to discuss our preliminary conclusions.

Criteria

We focused our FISMA performance audit approach on federal information security guidance developed by NIST and Office of Management and Budget (OMB). NIST Special Publications provide guidelines

[3] A subset of information systems refers to our approach of stratifying the population of non-IRS Department of the Treasury information system and selecting an information system from each Department of the Treasury bureau, excluding IRS, TIGTA, and OIG, rather than selecting a random sample of information systems that might exclude a Treasury bureau.

[4] Our rotational system selection strategy precludes selecting systems reviewed within the past two years. In FY 2011, TIGTA was selected, and the OIG was selected in FY 2010. Therefore, each of those bureau's systems were exempt from being reviewed in FY 2012.

that are considered essential to the development and implementation of agencies' security programs.[5] The following is a listing of the criteria used in the performance of the fiscal year (FY) 2012 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 Federal Information 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: A Security Life Cycle Approach*
  - 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, Building Effective Security Assessment Plans*
  - 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, *National Checklist Program for IT Products: Guidelines for Checklist 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*
  - 08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)*

- United States Department of Homeland Security:

[5] Note (per *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*): 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.

- FISM 12-02, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*

- Treasury Guidance:
  - TD P 85-01, Volume I, *Treasury Information Technology Security Program*

APPENDIX II – STATUS OF PRIOR-YEAR FINDINGS

For the following prior year findings, we have evaluated the information systems to determine whether the recommendations have been implemented and the finding is closed. We inquired of Treasury personnel and inspected evidence to determine the status of the findings. If recommendations were determined to be implemented, we closed the findings. If recommendations were determined to be only partially implemented or not implemented at all, we determined the finding to be open. For 3 of the 28 findings, we were unable to test the implementation of the findings in time by our end of fieldwork date, June 30, 2012. For these findings, we noted that they are closed but untested and should be evaluated as part of the FY 2013 independent evaluation.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Finding #1 – Office of Comptroller of Currency (OCC) Logical account management activities were not fully documented or consistently performed	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.	We recommend that OCC management document the process for granting access to the newly hired bank examiners, including the associated user roles and required management approvals.	**Implemented/Closed.** OCC updated policies and procedures to cover process for granting access to newly hired bank examiners.
Finding #1 – Office of Thrift Supervision (OTS) Logical account management activities were not fully documented or consistently performed	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 System Security Plan (SSP) or other application configuration document the required application service accounts for the application to function properly, thus limiting OTS's ability to identify unnecessary service accounts.	We recommend that OCC, in its capacity managing prior OTS systems: 1 Add the review of system administrator and application service accounts for the sampled system to the review of external user accounts. 2 Document the purpose and use of application service accounts in the SSP or other publication.	**Implemented/Closed.** OCC decommissioned the OTS system.
Finding #1 – Treasury Inspector General for Tax Administration (TIGTA)	TIGTA did not fully document account management activities (e.g., review frequency, inactivity limits, use of shared accounts) in their SSPs. TIGTA management	Based on TIGTA's planned corrective actions, we are not making a recommendation.	**Open.** TIGTA has not finished completing its corrective action.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Logical account management activities were not fully documented or consistently performed	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&M with scheduled completion dates of October 2011, April 2012, July 2012, and December 2012. These security weaknesses continued to exist at the time of fiscal year (FY) 2011 FISMA audit.		
Finding #1 – Departmental Offices (DO) Logical account management activities were not fully documented or consistently performed	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.	We recommend that DO management: 1 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. 2 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.	**Implemented/Closed.** DO has created policies and procedures over account approval and performs annual review of user accounts to determine access appropriateness.
Finding #1– Financial Management Service (FMS) Logical account management activities were not fully documented or	For a sampled FMS payment management system, 12 user accounts out of 2,950 inappropriately remained active following 90 days of inactivity. Additionally, 920 user accounts out of 2,950 did not have a last login date recorded, suggesting these accounts may never have been used by the account owner.	We recommend that FMS management: 1 Continue to monitor the automated solution to disable user accounts after 90 days of inactivity in order to confirm the	**Partially Implemented/Open.** We were informed that Recommendation 1 of the FY 2011 finding has been addressed. However, we noted that 268 active user accounts have not logged in greater than 90 days since

Finding #	Prior-Year Condition	Recommendation(s)	Status
consistently performed	We 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.	automated solution is working in all cases. 2 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.	the list was generated (March 20, 2012 or earlier).
Finding #2 – Community Development Financial Institution (CDFI) Fund Security incidents were not reported timely	The CDFI Fund did not report its single security incident to Treasury Computer Security Incident Response Capability (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.	We recommend that the CDFI Fund management: 1 Provide additional incident response training to increase awareness of the CDFI Fund's policies and procedures. 2 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. 3 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	**Implemented/Closed.** CDFI has shifted the responsibility of their incident response program to the Alcohol and Tobacco Tax and Trade Bureau (TTB), which is now responsible for reporting incidents to TCSIRC.

Finding #	Prior-Year Condition	Recommendation(s)	Status
		response e-mail account and/or phone number for reporting purposes.	
Finding #2 – FMS Security incidents were not reported timely	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, we attributed the untimely reporting by FMS employees to a lack of sufficient awareness and training.	We recommend that FMS management: 1 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. 2 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. 3 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. 4 Improve FMS employee awareness to report both confirmed and suspected security incidents to the FMS Service Desk. FMS could create awareness through periodic	**Closed/Untested.** We noted that FMS corrected the design of the Incident Response processes but did not complete all corrective actions until June 2012 and was unable to test the effectiveness. The finding will be tested as part of the FY 2013 FISMA evaluation.

Finding #	Prior-Year Condition	Recommendation(s)	Status
		reminders via e-mail, posting security posters in common employee areas, and through increased emphasis in annual security and awareness training.	
Finding #2 – United States Mint (Mint) Security incidents were not reported timely	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.	We recommend that Mint management: 1 Have all tickets sent to the CSIRC group mailbox as opposed to individual members to ensure that tickets are tracked properly. 2 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.	**Implemented/Closed.** Mint has implemented a backup mechanism, which requires the reporter to contact the incident response team by phone, leave a message, and also send an e-mail to the incident response group e-mail account.
Finding #2 – TIGTA Security incidents were not reported timely	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.	We recommend that TIGTA management: 1 Assign an additional individual as a backup resource to the TIGTA CSIRC for periods of reduced staffing. 2 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	**Implemented/Closed.** TIGTA has updated its incident response policies and procedures to provide additional guidance over how to properly handle security incidents. Additionally, TIGTA has entered into a contract agreement with an external vendor to provide additional coverage over incident response outside normal working hours.

Finding #	Prior-Year Condition	Recommendation(s)	Status
		Response team with another Treasury bureau to provide increased capabilities outside of normal working hours. 3 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.	
Finding #3 – DO SSPs did not fully adopt NIST recommended security controls from NIST Special Publication (SP) 800-53, Rev. 3	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. We noted that one sampled information system from DO 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, *Recommend Security Controls for Federal Information Systems and Organizations*, dated August 2009. We noted that the conditions, cited above for DO had various factors including the bureau and vendor's misunderstanding of contract requirements to maintain compliance with all NIST standards.	We recommend that DO management instruct the vendor to update the SSPs to include NIST SP 800-53, Rev. 3, security controls and associated control enhancements.	**Partially Implemented/Open.** While DO updated the system security plan to reflect NIST SP 800-53, Rev. 3, for some controls, not all controls in the system security plan reflected NIST SP 800-53, Rev. 3, guidance.
Finding #3 – Mint SSPs did not fully adopt NIST recommended security controls from NIST SP 800-53, Rev. 3	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. We noted that one sampled information system from Mint utilized outdated NIST guidance (Rev. 2).	We recommend that Mint management: 1 Update their Information Security Program's policies and procedures to require that all SSPs are updated to include the latest	**Implemented/Closed.** Mint updated the system security plans to reflect NIST SP 800-53, Rev. 3, controls.

Finding #	Prior-Year Condition	Recommendation(s)	Status
	Specifically, the SSPs did not include all required security controls as specified in NIST SP 800-53, Rev. 3, *Recommend Security Controls for Federal Information Systems and Organizations*, dated August 2009. We noted that the conditions, cited above for Mint had various factors including Mint management had an informal policy to only update SSPs during reaccreditation; therefore, the sampled SSPs had not been updated since the next reaccreditation cycle had not begun.	NIST SP 800-53 controls and control enhancements one year after issued. 2 Ensure that all existing SSPs are 800-53, Rev. 3 compliant.	
Finding #3 – FMS SSPs did not fully adopt NIST recommended security controls from NIST SP 800-53, Rev. 3	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.	We recommend that FMS 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.	**Open.** FMS did not fully implement NIST 800-53, Rev. 3, controls for the SSP.
Finding #4 – FMS Insufficient audit log reviews	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	We recommend that FMS management: 1 Identify and document significant audit events that warrant review and further investigation. 2 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. 3 Ensure that sufficient resources are available to implement audit log review procedures.	**Closed/Untested.** We were informed that all recommendations of the FY 2011 finding have been addressed. However, We noted that additional significant audit events were identified and three new reports were created (High Dollar Payee Settlement Report, Payee Settlement with Name Change Report, and 700-Weekly Frontier Security Audit Report). These reports were available in May 2012, making these reports not reviewable from July 1, 2011 until May 2012. The finding will be tested as part of the FY 2013 FISMA evaluation.

Finding #	Prior-Year Condition	Recommendation(s)	Status
	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.		
Finding #5 – Bureau of Public Debt (BPD) Improper media sanitization schedule	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. 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.	We recommend that BPD management: 1 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. 2 Train BPD IT specialists on the BPD media sanitization policies and procedures in order to protect the confidentiality of the bureau's sensitive information.	**Implemented/Closed.** BPD developed Standard Operation Procedure2.2.85 OIT Excess and Media Sanitation Tracking (hard drives, mobile media) to prepare and track media that has been degaussed.
Finding #6 – FMS POA&Ms were not tracked and remediated in accordance with NIST and Department of the Treasury requirements	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	We recommend that FMS management: 1 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	**Closed/Untested.** We noted that FMS corrected the design of the POA&M process but did not complete all corrective actions until the end of the FISMA Year. We also noted specific system POA&M issues that stem from the corrective actions were not being completed until later in the year. The finding will be tested as part of the FY 2013 FISMA evaluation.

Finding #	Prior-Year Condition	Recommendation(s)	Status
	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.	POA&M items. 2 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. 3 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. 4 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.	
Finding #6 – OTS POA&Ms were not tracked and remediated in accordance with NIST and Department of the Treasury	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	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*.	**Implemented/Closed.** The OTS system was decommissioned.

Finding #	Prior-Year Condition	Recommendation(s)	Status
requirements	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.		
Finding #7 – CDFI Fund Vulnerability scanning and remediation was not performed in accordance with Department of the Treasury requirements	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.	We recommend that the CDFI Fund management: 1 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. 2 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.	**Implemented/Closed.** CDFI modified its Interconnection Security Agreement with TTB to clearly assign vulnerability scanning roles and responsibilities.
Finding #7 – DO Vulnerability scanning and remediation was not performed in accordance with Department of the Treasury requirements	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 IT 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.	We recommend that DO management direct personnel charged with remediating vulnerabilities to track open, unresolved vulnerabilities in system POA&Ms when the anticipated remediation will exceed 30 days.	**Implemented/Closed.** DO has directed personnel to follow bureau-level policies and procedures over inputting open vulnerabilities to POA&Ms. DO personnel have updated POA&Ms to include open vulnerabilities. Additionally, DO has updated its vulnerability scan process to include all system devices to identify all flaws.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Finding #7 – OTS Vulnerability scanning and remediation was not performed in accordance with Department of the Treasury requirements	OTS did not consistently scan its application servers on a monthly basis as required by NIST and Department of the Treasury requirements and OTS Continuous Monitoring procedures. OTS personnel verbally outlined to a risk-based set of scanning frequencies that was not documented and not verifiable at the system level. Further, we noted that OTS management was aware of these flaws and indicated that it lacked the resources to scan more frequently	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*.	**Implemented/Closed.** The OTS system was decommissioned.
Finding #8 – DO Contingency planning and testing and backup controls were not fully implemented or operating as designed	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.). We observed that DO management was unaware of this issue. Once informed of this significant security	We recommend that DO management: 1 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. 2 Determine whether an upgraded version of DO's backup solution or a different backup tool will remediate unexpected server shutdowns and restarts. 3 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. 4 Increase backup storage capacity to ensure that archived data is not overwritten prematurely and data retention standards are observed.	**Implemented/Closed.** DO has updated backup process to perform frequent backups on a daily and weekly basis and test backups on a monthly basis. Additionally, DO has increased the backup storage capacity.

Finding #	Prior-Year Condition	Recommendation(s)	Status
	weakness, DO management created a POA&M item to track the issue to closure.		
Finding #8 – FMS Contingency planning and testing and backup controls were not fully implemented or operating as designed	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 . These two systems process approximately all Social Security Administration payments, Medicare and Medicaid payments, IRS tax refunds, Veteran Affairs payments, and other United States government vendor payments. However, these two systems had only undergone a tabletop disaster recovery test during FY 2010 and FY 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 FY 2010 due to operational priorities to relocate and consolidate data centers.	We recommend that FMS 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.	**Open.** FMS did not perform failover testing during the FISMA testing period for the two systems.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Finding #8 – TTB Contingency planning and testing and backup controls were not fully implemented or operating as designed	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.	We recommend that TTB management develop and implement policies and procedures to detect backup failures and remediate unsuccessful backups.	**Implemented/Closed.** TTB has closed this prior-year finding since they now conduct their own system backups, rather than outsource the responsibility. We tested the effectiveness of this control as part of the 2012 FISMA audit by inspecting evidence of the successful completion of backups.
Finding #8 – TIGTA Contingency planning and testing and backup controls were not fully implemented or operating as designed	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.	Based on TIGTA's planned corrective actions, we are not making a recommendation.	**Open.** TIGTA has not finished completing its corrective action.
Finding #9 – OTS Outdated and unsupported software was utilized	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.	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.	**Implemented/Closed.** The OTS system was decommissioned.

Finding #	Prior-Year Condition	Recommendation(s)	Status
Finding #10 – TIGTA Risk management program was not consistent with NIST SP 800-37, Rev. 1	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. We 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.	**Open.** TIGTA has not finished completing its corrective action.
Finding #11 – Financial Crimes Enforcement Network (FinCEN) Improper personnel termination procedures	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.	We recommend that the FinCEN management: 1 Provide training on the requirements of FinCEN's Personnel Separations Process Directive regarding employee separation to all parties involved in the exit process. 2 Maintain the employee exit forms in accordance with Treasury records management requirements.	**Implemented/Closed.** FinCEN revised documentation to require forms to be stored on a central shared drive. Share drive is only accessible to authorized personnel.
Finding #12 – DO	A sampled DO system did not implement	Based on DO's planned corrective	**Implemented/Closed.**

Finding #	Prior-Year Condition	Recommendation(s)	Status
Improper system configuration programs	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.	actions, we are not making a recommendation.	DO enforced baselines for the system through Group Policy Objects. Additionally, DO has maintained an approved Federal Desktop Core Configuration deviation memo.
Finding #12 – TIGTA Improper system configuration programs	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.	Based on TIGTA's planned corrective actions, we are not making a recommendation.	**Open.** TIGTA has not finished completing its corrective action.

APPENDIX III – THE DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO DHS's FISMA 2012 QUESTIONS FOR INSPECTORS GENERAL

The information included in Appendix III represents the Department of the Treasury's consolidated responses to Department of Homeland Security's (DHS) FISMA 2012 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, OIG and TIGTA. TIGTA performed audit procedures over the IRS information systems and provided their answers to the Treasury OIG and KPMG for consolidation. These answers are included within the table below. The information provided by TIGTA has not been subjected to KPMG audit procedures and, accordingly, we express no opinion on it.

1: Continuous Monitoring

Status of Continuous Monitoring Program [check one: Yes or No]	Yes	**1.1.** Has the Organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	Yes	**1.1.1.** Documented policies and procedures for continuous monitoring (NIST 800-53: CA-7).
	Yes	**1.1.2.** Documented strategy and plans for continuous monitoring (NIST 800-37 Rev 1, Appendix G).
	Yes	**1.1.3.** Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST 800-53, NIST 800-53A).
	Yes	**1.1.4.** 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&M additions and updates with the frequency defined in the strategy and/or plans (NIST 800-53, NIST 800-53A).
		1.2. Please provide any additional information on the effectiveness of the Organization's Continuous Monitoring Management Program that was not noted in the questions above. **Comments – Treasury OIG**: FMS did not have sufficient audit logging capability for a selected system. DO did not perform audit log reviews for a selected system. FMS did not perform audit log reviews for a selected system. (See Finding #4)

2: Configuration Management

Status of Configuration Management Program [check one: Yes or No]	Yes	**2.1** Has the Organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	Yes	**2.1.1.** Documented policies and procedures for configuration management.
	No	**2.1.2.** Standard baseline configurations. **Comments – Treasury OIG:** BPD did not document baseline configurations for two selected systems. FMS did not document all required aspects of baseline configuration for a selected system. TIGTA did not identify standard baseline configurations. (See Finding #10 and Prior-Year Finding #12)

No	**2.1.3.** Assessing for compliance with baseline configurations **Comments – Treasury OIG:** FinCEN baseline configurations for a selected system did not meet compliance requirements (See Finding #10) **Comments – TIGTA:** The IRS is still in the process of implementing tools compliant with the Security Content Automation Protocol to perform security configuration assessments for Windows and UNIX systems.
Yes	**2.1.4.** Process for timely, as specified in Organization policy or standards, remediation of scan result deviations.
No	**2.1.5.** For Windows-based components, FDCC/USCGB secure configuration settings fully implemented, and any deviations from FDCC/USCGB baseline settings fully documented. **Comments – Treasury OIG:** OCC did not implement restrictive settings for two selected systems (See Finding #9) **Comments – TIGTA:** The IRS has not yet fully documented Windows 7 FDCC/USGCB deviations.
No	**2.1.6.** Documented proposed or actual changes to the hardware and software configurations **Comments – Treasury OIG:** DO did not track and detect unauthorized changes to a selected system (See Finding #9) **Comments – TIGTA:** The IRS had not yet fully implemented configuration and change management controls to ensure that proposed or actual changes to hardware and software configurations are documented. During FY 2012, the Enterprise Services organization was in the process of implementing the Enterprise Configuration Management System to provide an enterprise solution for configuration and change management.
No	**2.1.7.** Process for the timely and secure installation of software patches. **Comments – TIGTA:** During the FY 2012 FISMA evaluation period, a TIGTA audit to evaluate the IRS's enterprise-wide patch management process identified that critical patches continue to be missing or are installed in an untimely manner on IRS computers.
No	**2.1.8.** Software assessing (scanning) capabilities are fully implemented (NIST 800-53: RA-5, SI-2). **Comments – Treasury OIG:** FMS was unable to provide evidence that scanning was being performed for two selected systems. (See Finding #6 and Financial Statement Finding #3). **Comments – TIGTA:** The IRS's software assessing (scanning) capabilities are not yet fully implemented. The IRS Cybersecurity organization is still in the process of coordinating with information system owners to implement vulnerability scanning enterprise-wide. For vulnerability scans the IRS did conduct, analyses of

	No	**2.1.3.** Assessing for compliance with baseline configurations **Comments – Treasury OIG:** FinCEN baseline configurations for a selected system did not meet compliance requirements (See Finding #10) **Comments – TIGTA:** The IRS is still in the process of implementing tools compliant with the Security Content Automation Protocol to perform security configuration assessments for Windows and UNIX systems.
		the scans were not being performed by the system owners. In addition, the IRS has not yet deployed an automated mechanism to detect the presence of unauthorized software on IRS information systems.
	No	**2.1.9.** Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in Organization policy or standards (NIST 800-53: CM-4, CM-6, RA-5, SI-2). **Comments – Treasury OIG:** Mint, OCC, BPD, and DO did not remediate vulnerabilities in a timely manner (See Finding #6) **Comments – TIGTA:** In June 2012, the TIGTA reported that monthly scanning results were not consistently being used to correct improper settings on Windows servers in a timely manner, but rather, security vulnerabilities of high, medium, and low risk levels were repeatedly reported on Windows Policy Checker reports for two or three consecutive months.
	No	**2.1.10.** Patch management process is fully developed, as specified in Organization policy or standards (NIST 800-53: CM-3, SI-2). **Comments – TIGTA:** Due to the lack of enterprise-level oversight and leadership, the IRS has not yet implemented key elements of its patch management policies and procedures that are needed to ensure all IRS systems are patched timely and operating securely. The IRS's current monitoring processes are not sufficient to ensure that vulnerabilities resulting from unpatched systems are successfully and timely remediated.
		2.2. Please provide any additional information on the effectiveness of the Organization's Configuration Management Program that was not noted in the questions above. **Comments – Treasury OIG:** FMS did not have a management-approved list of all privileged programs that reside on the mainframe. Federal Financing Bank (FFB) had discrepancies in the cash receipt amounts included in the cash receipt report. (See Financial Statement Finding #2 and Financial Statement Finding #7) **Comments – TIGTA:** The IRS should ensure that data collected by its various tools and organizations will be efficiently utilized and that the IRS is not developing duplicative configuration management processes or products. For example, our discussions with the IRS Cybersecurity and Enterprise Services organizations revealed that an approach for integrating the configuration management data collected by both organizations has not yet been formulated.

3: Identity and Access Management

Status of Identity and Access Management Program [check one: Yes or No]	Yes	**3.1** Has the Organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices? If yes, besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes:
	No	**3.1.1.** Documented policies and procedures for account and identity management (NIST 800-53: AC-1) **Comments – Treasury OIG:** TIGTA did not formally document account management activities for a selected system (See Prior-Year Finding #1)
	Yes	**3.1.2.** Identifies all users, including federal employees, contractors, and others who access Organization systems.
	No	**3.1.3.** Identifies when special access requirements (e.g., multi-factor authentication) are necessary. **Comments – Treasury OIG:** FMS did not fully implement multifactor authentication as required by NIST and Treasury guidance (See Finding #11).
	No	**3.1.4.** If multi-factor authentication is in use, it is linked to the Organization's PIV program. **Comments – TIGTA:** The IRS has not deployed multifactor authentication via the use of an HSPD-12 PIV card for all users for network and local access to nonprivileged or privileged accounts as required by Federal mandate.
	No	**3.1.5.** Organization has adequately planned for implementation of PIV for logical access in accordance with Treasury policies **(**HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). **Comments – TIGTA:** The IRS has experienced significant delays in deploying PIV cards for logical access, which reveals the IRS's inadequate planning efforts.
	No	**3.1.6.** Ensures that the users are granted access based on needs and separation of duties principles. **Comments – Treasury OIG:** FinCEN had a user account with access permissions that were not longer necessary. FMS did not document separation of duties principles (See Finding #1 and Financial Statement Finding #1) **Comments – TIGTA:** Two of the three general support systems in our sample of 10 IRS systems did not have the controls in place to ensure users are granted access based on needs or to enforce separation of duties.

	No	**3.1.7.** Identifies devices that are attached to the network and distinguishes these devices from users (for example: IP, phones, faxes, printers, are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that uses accounts). **Comments – TIGTA:** The IRS informed us that Business DNA will be its enterprise asset discovery tool for identifying devices on its network. Business DNA network scans can identify devices with internet protocol addresses that are attached to the network and distinguish these devices from users. However, the full implementation of the Business DNA tool is not expected to be completed until September 2012.
	No	**3.1.8.** Identifies all User and Non-User Accounts (refers to user accounts that are on a system. Examples of non-user accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users). **Comments – TIGTA:** No information was provided to determine how the IRS identifies all user and nonuser accounts.
	No	**3.1.9.** Ensures that accounts are terminated or deactivated once access is no longer required. **Comments – Treasury OIG:** TTB did not properly terminate accounts as required by NIST and Treasury guidance. FMS did not properly terminate inactive accounts. (See Finding #1 and Prior-Year Finding #1) **Comments – TIGTA:** Three systems in our sample of 10 IRS systems (two general support systems and one application) did not have controls in place to ensure accounts are terminated or deactivated once access is no longer needed.
	No	**3.1.10.** Identifies and controls use of shared accounts. **Comments – TIGTA:** One of the general support systems in our sample of 10 IRS systems was not adequately identifying and controlling use of shared accounts. Also, in June 2012, the TIGTA reported that administrative accounts on Windows servers were not being properly safeguarded in accordance with IRS policy. Consequently, individual accountability was lost as to by whom and for what purposes these full-privileged accounts were being accessed.
		3.2. Please provide any additional information on the effectiveness of the Organization's Identity and Access Management that was not noted in the questions above. **Comments – Treasury OIG:** OCC did not incorporate all user accounts into periodic access review. FinCEN did not review access permissions on a annual basis. DO did not formally document all access request forms. BPD was unable to provide evidence of user last log on for testing of inactive users (See Finding #1)

4: Incident Response and Reporting

Status of Incident Response and Reporting Program [check one: Yes or No]	Yes	**4.1** Has the Organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	Yes	**4.1.1.** Documented policies and procedures for detecting, responding, and reporting to incidents (NIST 800-53: IR-1).
	Yes	**4.1.2.** Comprehensive analysis, validation, and documentation of incidents.
	No	**4.1.3.** When applicable, reports to US-CERT within established time frames (NIST 800-53, 800-61, and OMB M-07-16, M-06-19). **Comments – Treasury OIG:** BEP, BPD, and FinCEN did not report incidents within required time frames. FMS did not report incidents within required time frames (See Finding #2 and Prior-Year Finding #2)
	Yes	**4.1.4.** When applicable, reports to law enforcement within established time frames (SP 800-86).
	Yes	**4.1.5.** Responds to and resolves incidents in a timely manner, as specified in Organization policy or standards, to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
	Yes	**4.1.6.** Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.
	Yes	**4.1.7.** Is capable of correlating incidents.
	Yes	**4.1.8.** There is sufficient incident monitoring and detection coverage in accordance with government policy (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
		4.2. Please provide any additional information on the effectiveness of the Organization's Incident Response and Reporting Program that was not noted in the questions above.

5: Risk Management

Status of Risk Management Program [check one: Yes or No]	Yes	**5.1** Has the Organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	Yes	**5.1.1.** Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.
	No	**5.1.2.** Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Revision 1. **Comments – Treasury OIG:** TIGTA did not update risk management program with NIST 800-37 guidance (See Prior-Year Finding #10)
	No	**5.1.3.** Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Revision 1. **Comments – Treasury OIG:** TIGTA did not update risk management program with NIST 800-37 guidance (See Prior-Year Finding #10)
	Yes	**5.1.4.** Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Revision 1.

	Yes	**5.1.5.** Categorizes information systems in accordance with government policies.
	Yes	**5.1.6.** Selects an appropriately tailored set of baseline security controls.
	No	**5.1.7.** Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation. **Comments – Treasury OIG:** OCC, FMS, and DO did not adequately document the implementation of controls as required by NIST and Treasury guidance. (See Finding #3 and Prior-Year Finding #3)
	Yes	**5.1.8.** Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
	Yes	**5.1.9.** Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
	No	**5.1.10.** Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. **Comments – Treasury OIG:** FinCEN did not update documentation with results from security assessment (See Finding #3)
	Yes	**5.1.11.** Information system-specific risks (tactical), mission/business-specific risks and organizational-level (strategic) risks are communicated to appropriate levels of the organization.
	Yes	**5.1.12.** Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO).
	Yes	**5.1.13.** Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.
	Yes	**5.1.14.** Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies (SP 800-18, SP 800-37).
	Yes	**5.1.15.** Security authorization package contains Accreditation boundaries for Organization information systems defined in accordance with government policies.
		5.2. Please provide any additional information on the effectiveness of the Organization's Risk Management Program that was not noted in the questions above.

6: Security Training

Status of Security Training Program [check one: Yes or No]	Yes	**6.1** Has the Organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	Yes	**6.1.1.** Documented policies and procedures for security awareness training (NIST 800-54: AT-1).
	Yes	**6.1.2.** Documented policies and procedures for specialized training for users with significant information security responsibilities.

	Yes	**6.1.3.** Security training content based on the organization and roles, as specified in Organization policy or standards.
	Yes	**6.1.4.** Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other Organization users) with access privileges that require security awareness training.
	No	**6.1.5.** Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other Organization users) with significant information security responsibilities that require specialized training. **Comments – TIGTA:** The IRS has not fully implemented identification and tracking of the status of specialized role-based training for contractors.
	Yes	**6.1.6.** Training material for security awareness training contains appropriate content for the Organization (SP 800-50, SP 800-53).
		6.2. Please provide any additional information on the effectiveness of the Organization's Incident Response and Reporting Program that was not noted in the questions above.

7: POA&M

Status of POA&M Program [check one: Yes or No]	Yes	**7.1** Has the Organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	Yes	**7.1.1.** Documented policies and procedures for managing all known IT security weaknesses discovered during security control assessments and requiring remediation.
	No	**7.1.2.** Tracks, prioritizes, and remediates weaknesses. **Comments – Treasury OIG:** FMS did not transfer POA&Ms to BPD (See Financial Statement Finding #4)
	Yes	**7.1.3.** Ensures remediation plans are effective for correcting weaknesses.
	Yes	**7.1.4.** Establishes and adheres to milestone remediation dates.
	Yes	**7.1.5.** Ensures resources are provided for correcting weaknesses.
	No	**7.1.6.** POA&Ms include security weaknesses discovered during assessments of security controls and requiring remediation (Do not need to include security weakness due to a Risk Based Decision to not implement a security control) (OMB M-04-25). **Comments – Treasury OIG:** DO did not create POA&Ms for security weaknesses discovered during security assessment. FMS did not record POA&Ms for non-remediated vulnerabilities (See Finding #5 and Prior-Year Finding #6)
	Yes	**7.1.7.** Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25).

	Yes	**7.1.8.** Programs officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5 and OMB M-04-25).
		7.2. Please provide any additional information on the effectiveness of the Organization's POA&M Program that was not noted in the questions above.

8: Remote Access Management

Status of Remote Access Management Program [check one: Yes or No]	Yes	**8.1** Has the Organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	Yes	**8.1.1.** Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST 800-53: AC-1, AC-17).
	Yes	**8.1.2.** Protects against unauthorized connections or subversion of authorized connections.
	Yes	**8.1.3.** Users are uniquely identified and authenticated for all access (NIST 800-46, Section 4.2, Section 5.1).
	Yes	**8.1.4.** Telecommuting policy is fully developed (NIST 800-46, Section 5.1).
	Yes	**8.1.5.** If applicable, multifactor authentication is required for remote access (NIST 800-46, Section 2.2, 3.3).
	Yes	**8.1.6.** Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.
	Yes	**8.1.7.** Defines and implements encryption requirements for information transmitted across public networks.
	Yes	**8.1.8.** Remote access sessions, in accordance to OMB M-07-16, are timed-out after a maximum of 30 minutes of inactivity after which reauthentication is required.
	Yes	**8.1.9.** Lost or stolen devices are disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guideline).
	Yes	**8.1.10.** Remote access rules of behavior are adequate in accordance with government policies (NIST 800-53: PL-4).
	Yes	**8.1.11.** Remote access user agreements are adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6).
		8.2. Please provide any additional information on the effectiveness of the Organization's Remote Access Management that was not noted in the questions above.

9: Contingency Planning

Status of Contingency Planning Program [check one: Yes or No]	Yes	**9.1** Has the Organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	Yes	**9.1.1.** Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST 800-53: CP-1).
	Yes	**9.1.2.** The agency has performed an overall Business Impact Analysis (NIST SP 800-34).

	No	**9.1.3.** Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures (NIST SP 800-34). **Comments – Treasury OIG:** DO did not update the contingency plan for a selected system within the FISMA year. TIGTA did not have a new operating system integrated into its contingency plan. (See Finding #7 and Prior-Year Finding #8)
	No	**9.1.4.** Testing of system specific contingency plans. **Comments – Treasury OIG:** FMS and DO did not perform contingency plan testing for selected systems (See Finding #7 and Prior-Year Finding #8)
	Yes	**9.1.5.** The documented business continuity and disaster recovery plans are ready for implementation (FCD1, NIST SP 800-34).
	Yes	**9.1.6.** Development of training, testing, and exercises (TT&E) approaches (FCD1, NIST SP 800-34, NIST 800-53).
	No	**9.1.7.** Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans. **Comments – Treasury OIG:** FMS and DO did not perform contingency plan testing for selected systems (See Finding #7 and Prior-Year Finding #8)
	No	**9.1.8.** After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34). **Comments – Treasury OIG:** FMS and DO did not perform contingency plan testing for selected systems (See Finding #7 and Prior-Year Finding #8)
	Yes	**9.1.9.** Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).
	Yes	**9.1.10.** Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).
	No	**9.1.11.** Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). **Comments – Treasury OIG:** CDFI did not perform consistent backup for a selected system. BPD was unable to provide evidence of backup being performed for a selected system. FMS did not perform testing of backups for a financial system (See Finding #8 and Financial Statement Finding #5)
	No	**9.1.12.** Contingency planning that considers supply chain threats.
		9.2. Please provide any additional information on the effectiveness of the Organization's Contingency Planning that was not noted in the questions above.

10: Contractor Systems

Status of Contractor Systems [check one: Yes or No]	Yes	**10.1** Has the Organization established a program to oversee systems operated on its behalf by contractors or other entities, including Organization systems and services residing in the cloud external to the Organization? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes:

	Yes	**10.1.1.** Documented policies and procedures for information security oversight of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud.
	No	**10.1.2.** The Organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and Organization guidelines. **Comments – Treasury OIG:** FMS did not obtain assurance that IT security controls are in place for service providers over select financial systems (See Financial Statement Finding #6)
	Yes	**10.1.3.** A complete inventory of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud.
	Yes	**10.1.4.** The inventory identifies interfaces between these systems and Organization-operated systems (NIST 800-53: PM-5).
	Yes	**10.1.5.** The Organization requires appropriate agreements (e.g., Memorandum of Understanding, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.
	Yes	**10.1.6.** The inventory of contractor systems is updated at least annually.
	Yes	**10.1.7.** Systems that are owned or operated by contractors or entities, including Organization systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.
		10.2. Please provide any additional information on the effectiveness of the Organization's Contractor Systems that was not noted in the questions above.

11: Security Capital Planning

Status of Security Capital Planning [check one: Yes or No]	Yes	**11.1** Has the Organization established a security capital planning and investment program for information security? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:
	Yes	**11. 1.1.** Documented policies and procedures to address information security in the capital planning and investment control process.
	Yes	**11.1.2.** Includes information security requirements as part of the capital planning and investment process.
	Yes	**11.1.3.** Establishes a discrete line item for information security in organizational programming and documentation (NIST 800-53: SA-2).
	Yes	**11.1.4.** Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST 800-53: PM-3).
	Yes	**11.1.5.** Ensures that information security resources are available for expenditure as planned.
		11.2. Please provide any additional information on the effectiveness of the Organization's Security Capital Planning that was not noted in the questions above.

APPENDIX IV – APPROACH TO SELECTION OF SUBSET OF SYSTEMS

In fiscal year (FY) 2012, a risk-based approach was employed to determine the subset of United States Department of the Treasury (Treasury) information systems for the FISMA Audit. The universe for this subset only included major business applications and general support systems with a security classification of "moderate" or "high." We used the system inventory contained within the Trusted Agent FISMA system (TAF) as the population for this subset.

Based on historical trends in the Treasury systems inventory and past reviews, we used a subset size of 25 from the total population of Treasury major applications and general support systems with a security classification of "Moderate" or "High." Based on their lower risk, we elected not to incorporate any systems with a FIPS 199 System Impact Level of "Low" into the population of applications to be selected. We then applied the weighting of IRS systems to non-IRS bureau systems to the total subset size in order to determine the IRS and non-IRS bureau subset sizes.

To select the subset, we stratified the full population of Treasury major applications and general support systems by bureau and by FIPS 199 system impact level. We used a risk-based approach to select systems out of each stratum. We considered the following factors to select system:

- 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, 2012.
- 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 subset would not exceed the percentage of systems they represent in the Treasury inventory of information systems. We defined financial systems as those information systems that have been 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 April 3, 2012, we noted a total of 191 major applications and general support systems with a security classification of moderate or high are contained within the Treasury-wide inventory. The following table provides our analysis of the composition of the Treasury's inventory of major applications and general support systems.

	Total	**IRS Financial Systems**	**IRS Non-Financial Systems**	**Non-IRS Financial Systems**	**Non-IRS Non-Financial Systems**
Major Applications	134	2	47	36	49
General Support Systems	57	0	24	4	29
Total	191	2	71	40	78

From the analysis above, it was determined that IRS systems make up 39% of the total population of Major Applications and General Support systems and Non-IRS systems make up 61%. When the IRS to Non-IRS weighting is applied to subset size of 25 from the total population, the resulting sizes for the IRS and Non-IRS subsets are 10 and 15, respectively.

We determined that Major Applications account for 72% of the population of the Non-IRS population and General Support Systems account for 28%. We further determined that systems designated as "Financial" and "Mixed Financial" in TAF account for 34% of all Non-IRS Major Applications and General Support Systems. Lastly, we determined that 29% of the Non-IRS Major Applications and General Support Systems are assigned a FIPS 199 System Impact Level of "High," while 71% are assigned a FIPS 199 System Impact Level of "Moderate."

Total Selected	15
Total Major Applications	11
Total General Support Systems	4
Total Systems with a FIPS 199 System Impact Level of "High"	4
Total Systems with a FIPS 199 System Impact Level of "Moderate"	11
Total Systems with a FIPS 199 System Impact Level of "Low"	0
Total Systems Designated as Financial	5

We 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. We used this information as a baseline to determine the total number of systems to select at each bureau or office:

Bureau	Total Systems	Percentage of Total Non-IRS Population	Total Number of Non-IRS Systems to be Select
BEP	7	6%	1
BPD	14	12%	2
CDFI Fund	3	3%	1 (See Note 1)
DO	24	20%	3
FinCEN	7	6%	1
FMS	35	29%	3
Mint	10	8%	1
OCC	7	6%	2 (See Note 2)
OTS	1	1%	0 (See Note 2)
OIG	5	4%	0 (See Note 3)
TIGTA	2	2%	0 (See Note 3)
TTB	3	3%	1 (See Note 1)
Total	118	100%	15

(**Note 1:** Using this methodology initially did not yield a system being selected at these agencies. However, using our risk-based methodology, we elected to select one system for each of these agencies and decrease the number of systems for FMS.)

(**Note 2:** OCC incorporated two of the OTS Systems into their GSS and the rest of the OTS systems are scheduled to be retired. We elected to sample two systems for OCC and none of the retiring systems.)

(**Note 3**: Per instructions from the OIG, we will not sample any systems from OIG or TIGTA, because their systems had been selected in the past two years.)

APPENDIX V – 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. We 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 SP 800-53. We 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.

We 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).

We assessed the following Operational control areas:

- Configuration Management (CM)
- Contingency Planning (CP)
- 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 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
CM-2	Baseline Configuration
CM-6	Configuration Settings

Contingency Planning:

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

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.

We assessed the following Technical control areas:

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)

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-6	Least Privilege

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-6	Audit Review

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-4	Identifier Management

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

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

Finding Number	NIST 800-53 Control Family	Condition	Recommendation
1	Access Control	For the UNIX Mid-Tier environments that host significant financial systems, FMS and BPD management have not identified incompatible duties for sensitive users as required by the FMS Entity-Wide IT Security Standards Manual; therefore, we could not determine if policies were implemented to segregate these duties. Sensitive users include system administrators, database administrators (DBA), developers, change management support, and computer operations personnel.	We recommend that FMS management: 1. Develop a segregation of duties (SOD) matrix that complies with the IT security standards from FMS and NIST for sensitive users across the UNIX Mid-Tier environments and use this matrix when assigning access to groups or creating new groups through the change control process. 2. Analyze existing groups on the UNIX Mid-Tier environments and document the following: a. Description, purpose, and approval of each existing UNIX Mid-Tier group; b. Privileges and actions that each group can perform; c. Job functions and sensitive roles assigned to each group; and d. Process to approve, log, and monitor of groups. 3. Remove any inappropriate access that does not comply with SOD matrix.
2	Configuration Management	(Repeat Condition) FMS did not have a management-approved list of all privileged programs that reside on the mainframe. Additionally, FMS did not implement an automatic tool to alert management when new privileged programs were added to the mainframe to determine if the addition was approved, appropriate, and safe. FMS closed this prior year finding in FY 2012, however, our testing determined the finding had not been resolved and had to be reissued. We repeated the	We recommend that FMS management: 1. Develop a complete authoritative information system inventory of all management-approved privileged programs, and confirm that existing privileged programs are safe and required for successful operation of the mainframe. 2. Develop and implement formal change control procedures to monitor privileged programs to confirm that they were safe, approved by management, and had not been altered without management's approval. 3. Implement an automated mechanism to track the inventory of existing programs and notify appropriate officials when new privileged programs are added or existing privileged programs are modified.

Finding Number	NIST 800-53 Control Family	Condition	Recommendation
		following recommendations made in our FY 2011 report.	
3	Risk Assessment	The FMS Entity-wide IT Standards prescribes that it is management's responsibility to monitor the effectiveness of its security program over the system environment, which includes the UNIX Mid-Tier platform maintained at the BPD; however, we noted a lack of evidence supporting FMS's responsibility of threat management. Moreover, FMS did not document the effectiveness of their monitoring program by not being able to confirm whether: 1. The actual Internet Protocol (IP) addresses in production at the time of the vulnerability scans that were run from October 1, 2011 to June 30, 2012 were valid; 2. Any vulnerabilities were identified; and 3. Any corresponding corrective actions had been implemented.	We recommend that FMS management: 1. Formally document the vulnerability scanning processes for the Fiscal Service organization and communicate the processes to affected field personnel. 2. Maintain a complete listing of hosts and IP addresses for production environment and document any changes to this listing, and retain enough supporting documentation to confirm the accuracy of completed vulnerability scans. 3. Strengthen the threat management process to require the sharing of information obtained from the vulnerability scanning process and security control assessments with designated personnel through the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses).
4	Security Assessment and Authorization	FMS needs to improve its enforcement over coordinating with BPD for the orderly transfer of POA&M items relating to UNIX Mid-Tier platform-specific weaknesses affecting FMS applications, per the FMS Transferring POA&M Items Standard. We noted that several platform-specific weakness that were initially tracked in the POA&Ms	We recommend that FMS management: 1. Strengthen its enforcement over the transfer of POA&M items across the organizations to ensure timely remediation of weaknesses. 2. Enhance the FMS Transferring POA&M Items Standard to require the orderly transfer of POA&Ms items across the organizations within specified time frames.

Finding Number	NIST 800-53 Control Family	Condition	Recommendation
		for FMS applications were not transferred in a timely manner to BPD for inclusion in the UNIX Mid-Tier POA&M, thereby not enabling the monitoring controls necessary to ensure prompt remediation.	
5	Contingency Planning	For a financial system application that resides on the mid-tier Unix environment, FMS management was unable to define formally who was responsible for the backup testing process. FMS management staff informed us that BPD performs backup test procedures for the FMS application. Alternatively, BPD support personnel informed us that BPD does not perform backup tests unless FMS management instructs BPD to do so. We determined that backup tests were not performed consistently by either BPD or FMS management on a semi-annual basis as required by the Fiscal Service Baseline Security Requirements (BLSR) and the Treasury Directive Publication 85-01. In addition, FMS or BPD could only provide to us supporting documentation evidencing backup testing of the application server. No evidence was available to demonstrate backup testing of the database and web servers.	We recommend that FMS management: 1. Update existing application and Mid-Tier UNIX backup procedures and system security plans to clarify roles and responsibilities with regards to the semi-annual testing of the financial system application backups to comply with the Fiscal Services BLSR, Treasury Directive Publication 85-01, and NIST SP 800-53. 2. Communicate the updates to the financial system application and Mid-Tier UNIX backup procedures and SSPs to the financial system application management staff and BPD support personnel. 3. Test backups for the financial system application production servers semi-annually as prescribed the Fiscal Services BLSR and the Treasury Directive Publication 85-01.
6	Contractor Systems	FMS does not monitor IT security control compliance of its service providers and has not addressed the risks or implemented compensating controls.	We recommend that FMS management: 1. Document the following in the FMS system SSPs: (a) the inherited IT security controls that are being performed by the service providers and (b)

Finding Number	NIST 800-53 Control Family	Condition	Recommendation
		Specifically, we noted that FMS has not implemented a process to obtain assurance that inherited IT security controls at the service providers are operating effectively, as prescribed by NIST SP 800-53, Rev. 3. We noted that system security plans (SSPs) or additional FMS procedures do not formally establish the security roles and responsibilities between FMS and its service providers for inherited controls and how FMS should monitor the operating effectiveness of these service providers' controls.	the FMS's monitoring controls to determine that these controls are operating effectively. 2. Develop an enforcement process to obtain assurance that the IT security controls inherited by the service providers are operating effectively.
7	Configuration Management	While performing audit test work over borrowings as of June 30, 2012, we noted discrepancies in the cash receipt amounts included in the cash receipt report. This was determined to be due to a change request to modify the cash receipts report. Specifically, we determined that while FFB management tests and approves change requests prior to implementing system changes, their change management procedures were not comprehensive enough to ensure proper testing occurs prior to and subsequent to development and production. Due to the lack of regression testing, management was unable to detect the effect of the system change in production. Additionally, an FFB IT Staff member	We recommend that Federal Financing Bank (FFB) management strengthen change control procedures for the system and related report modifications. These procedures should conform to existing standards and include the following: 1. Implement policy and procedures to provide adequate supervision, by FFB IT staff, when contracting group develops requirements, testing, acceptance, and subsequent implementation initiatives prior to moving into production. 2. Strengthen change request form to include all requirements, scope of change request including time period of change, life cycle of implementation and end user testing to ensure all change requests are properly tested. 3. Ensure the that the proper level and sufficiency of testing are appropriate to specific change requirements; that change requests are appropriately evaluated, authorized, and monitored to ensure that they achieve the users' requirements and do not negatively impact existing processing.

Finding Number	NIST 800-53 Control Family	Condition	Recommendation
		was not assigned to review in detail the change requests of development or production projects, created by the contracting firm, prior to the accountants performing their tests and approval of the changes.	

APPENDIX VII – GLOSSARY OF TERMS

Acronym	Definition
AC	Access Control
ACIOCS	Associate Chief Information Officer for Cyber Security
AU	Audit and Accountability
BEP	Bureau of Engraving and Printing
BLSR	Fiscal Service Baseline Services Requirements
BPD	Bureau of the Public Debt
CA	Security Assessment and Authorization
CAT	Category
C&A	Certification and Accreditation
CDFI	Community Development Financial Institution
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Planning
CSIRC	Computer Security Incident Response Center
CSS	Cyber Security Sub-Council
DHS	Department of Homeland Security
DO	Departmental Offices
FDCC	Federal Desktop Core Configuration
FFB	Federal Financing Bank
FinCEN	Financial Crimes Enforcement Network
FIPS	Federal Information Processing Standards
FISM	Federal Information Security Memorandum
FISMA	Federal Information Security Management Act
FMS	Financial Management Service
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
IA	Identification and Authentication
IG	Inspector General
IP	Internet Protocol
IRS	Internal Revenue Service
ISSO	Information System Security Officer
IT	Information Technology
KPMG	KPMG LLP
Mint	United States Mint
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency

Acronym	Definition
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OTS	Office of Thrift Supervision
PL	Planning
POA&M	Plan of Action and Milestones
RA	Risk Assessment
Rev.	Revision
SI	System and Information Integrity
SIGTARP	Special Inspector General for the 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 P	Treasury Directive Publication
TIGTA	Treasury Inspector General for Tax Administration
TTB	Alcohol and Tobacco Tax and Trade Bureau
US-CERT	United States Computer Emergency Readiness Team

ATTACHMENT 2

Treasury Inspector General for Tax Administration–Federal Information Security Management Act Report for Fiscal Year 2012, (Audit No. 2012-20-114), September 28, 2012

THIS PAGE INTENTIONALLY LEFT BLANK

Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2012

September 28, 2012

Reference Number: 2012-20-114

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION – FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT FOR FISCAL YEAR 2012

Highlights

Report issued on September 28, 2012

Highlights of Report Number: 2012-20-114 to the Department of the Treasury, Office of the Inspector General, Assistant Inspector General for Audit.

IMPACT ON TAXPAYERS

The 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.

WHY TIGTA DID THE AUDIT

The Federal Information Security Management Act (FISMA) was enacted to strengthen the security of information and systems within Federal agencies. As part of this legislation, the Offices of Inspectors General are required to perform an annual independent evaluation of each Federal agency's information security programs and practices. This report reflects TIGTA's independent evaluation of the status of the IRS's information security program for Fiscal Year 2012.

WHAT TIGTA FOUND

Based on our Fiscal Year 2012 FISMA evaluation, TIGTA found that the IRS's information security program was generally compliant with the FISMA requirements. Specifically, TIGTA determined that the following eight program areas met the level of performance specified by the Department of Homeland Security's *Fiscal Year 2012 Inspector General FISMA Reporting Metrics*:

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

However, TIGTA determined that the following program areas did not meet the level of performance specified by the Department of Homeland Security's *Fiscal Year 2012 Inspector General FISMA Reporting Metrics* as a result of specific program attributes that were missing or other conditions identified that reduced program effectiveness:

- Configuration management.
- Identity and access management.
- Security training.

WHAT TIGTA RECOMMENDED

TIGTA does not include recommendations as part of its annual FISMA evaluation and reports only on the level of performance achieved by the IRS using the guidelines issued by the Department of Homeland Security for the applicable FISMA evaluation period.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 28, 2012

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

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2012 (Audit # 201220001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Management Act[1] evaluation for Fiscal Year 2012. The Act requires the Offices of Inspectors 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 and practices for the period under review.

The report was forwarded to the Treasury Inspector General for consolidation into a report issued to the Department of the Treasury Chief Information Officer. 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.

[1] Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.

Table of Contents

Background ..... Page 1

Results of Review ..... Page 2

The Internal Revenue Service's Information Security Program Generally Complies With the Federal Information Security Management Act, but Improvements Are Needed ..... Page 2

Appendices

Appendix I – Fiscal Year 2012 Reporting Metrics ..... Page 16

Appendix II – Major Contributors to This Report ..... Page 30

Appendix III – Report Distribution List ..... Page 31

Appendix IV – Treasury Inspector General for Tax Administration Information Technology Security-Related Reports Issued During the Fiscal Year 2012 Evaluation Period ..... Page 32

Appendix V – Glossary of Terms ..... Page 33

Abbreviations

AP	Administrative Priority
Base	Baseline Question
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Continuous Monitoring
CMWG	Continuous Monitoring Working Group
DAA	Designated Accrediting Authority
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
ECMS	Enterprise Configuration Management System
FCD1	Federal Continuity Directive 1
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
GSS	General Support System
HSPD-12	Homeland Security Presidential Directive-12
IP	Internet Protocol
IRS	Internal Revenue Service
IT	Information Technology
KFM	Key FISMA Metric
MOU	Memorandum of Understanding

NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SCAP	Security Content Automation Protocol
SP	Special Publication
TIGTA	Treasury Inspector General for Tax Administration
US-CERT	United States Computer Emergency Response Team
USG	U.S. Government
USGCB	United States Government Configuration Baseline

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 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) of 2002[1] 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.[2] 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.

We based our evaluation of the IRS on the Department of Homeland Security's (DHS) *Fiscal Year (FY) 2012 Inspector General FISMA Reporting Metrics* issued on March 6, 2012. These reporting metrics specified the security program areas for the Inspectors General to evaluate and listed specific attributes that each security program area should include, as shown in Appendix I. Major contributors to this report are listed in Appendix II.

[1] Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.
[2] The FISMA evaluation period for the Department of the Treasury is July 1, 2011, through June 30, 2012. All subsequent references to 2012 refer to the FISMA evaluation period.

Results of Review

The Internal Revenue Service's Information Security Program Generally Complies With the Federal Information Security Management Act, but Improvements Are Needed

The DHS *FY 2012 Inspector General FISMA Reporting Metrics* specified 11 information security program areas and a total of 96 attributes within the 11 areas for the Inspectors General to evaluate and determine whether agencies had established and maintained an information security program that was generally consistent with the NIST and OMB's FISMA requirements. The 11 information security program areas are as follows:

- Continuous monitoring management.
- Configuration management.
- Identity and access management.
- Incident response and reporting.
- Risk management.
- Security training.
- Plan of action and milestones.
- Remote access management.
- Contingency planning.
- Contractor systems.
- Security capital planning.

To complete our FISMA evaluation, we reviewed a representative sample of 10 major IRS information systems. 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. In addition, we evaluated the IRS's processes over configuration management, identity and access management, incident response and reporting, security training, remote access management, contractor systems, and security capital planning. During the FY 2012 FISMA evaluation period, we also completed nine audits, as shown in Appendix IV, which evaluated various aspects of information security at the IRS. We considered the results of these audits in our evaluation, as well as results from ongoing audits for which draft reports were issued to the IRS by August 10, 2012.

Based on our FY 2012 FISMA evaluation, we determined that the IRS's information security program was compliant with the FISMA requirements and met the level of performance for eight of the 11 program areas as specified by the DHS's *FY 2012 Inspector General FISMA Reporting Metrics*. However, we also noted that improvements were needed in the remaining three program areas. We determined that these three program areas did not meet the level of performance specified by the DHS's *FY 2012 Inspector General FISMA Reporting Metrics* as a result of specific program attributes that were missing or other conditions that we identified which reduced program effectiveness. The three areas needing improvement are as follows:

- Configuration management.
- Identity and access management.
- Security training.

Configuration Management

Configuration management comprises a collection of activities focused on establishing and maintaining the integrity of products and systems through control of the processes for initializing, changing, and monitoring the configurations of those products and systems. Security-focused configuration management is the management and control of secure configurations for an information system to enable security and facilitate the management of risk. Effective configuration management of information systems requires the integration of the management of secure configurations into the organizational configuration management process or processes.

In order to secure both software and hardware, agencies must develop and implement standard configuration baselines that prevent or minimize exploitable system vulnerabilities. The OMB requires all Windows 7, XP, and Vista workstations to conform to the U.S. Government Configuration Baseline. Furthermore, the NIST has created a repository of secure baselines for a wide variety of operating systems and devices. Agencies must also develop and implement sufficient patch management processes, which is a component of configuration management. Any significant delays in patching software with critical vulnerabilities provide ample opportunity for persistent attackers to gain control over the vulnerable computers and get access to the sensitive data they may contain.

The IRS has not fully implemented the following seven configuration management attributes specified by the DHS metrics:

2.1.3. Assessing for compliance with baseline configurations.

2.1.5. For Windows-based components, Federal Desktop Core Configuration (FDCC)/U.S. Government Configuration Baseline (USGCB) secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.

2.1.6. Documented proposed or actual changes to hardware and software configurations.

2.1.7. Process for timely and secure installation of software patches.

2.1.8. Software assessing (scanning) capabilities are fully implemented.

2.1.9. Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards.

2.1.10. Patch management process is fully developed, as specified in organization policy or standards.

2.1.3. Assessing for compliance with baseline configurations.

The IRS is still in the process of implementing tools compliant with the Security Content Automation Protocol (SCAP)[3] to perform security configuration assessments for Windows and UNIX systems. Agencies are required to use SCAP-validated tools, as specified by the NIST, to continuously monitor the security configurations of their information technology assets as part of compliance with the FISMA.

In April 2008, the IRS formally kicked off an initiative to implement the Security Compliance Posture Monitoring and Reporting tool, an enterprise tool that would utilize the NIST-defined protocol. When in production, the Security Compliance Posture Monitoring and Reporting tool would provide the IRS with the ability to monitor, measure, and manage FISMA security compliance of its Windows and UNIX servers enterprise-wide. Also, it would allow the IRS to retire the Windows and UNIX policy checker programs, which are not SCAP-compliant. However, the IRS has not yet rolled out the Security Compliance Posture Monitoring and Reporting tool.

Also, in September 2011, the Treasury Inspector General for Tax Administration (TIGTA) reported[4] that automated security configuration scans of IRS mainframe databases were not conducted. The Internal Revenue Manual required monthly automated security configuration scans of all operating and database systems. However, the mainframe policy checker does not test configuration compliance for databases that reside on mainframes. The IRS agreed to implement automated security configuration scanning on mainframe databases by March 1, 2013.

[3] The SCAP is a suite of specifications that standardize the format and nomenclature by which security software products communicate software flaw and security configuration information. SCAP is designed to organize, express, and measure security-related information in standardized ways, as well as related reference data, such as identifiers for post-compilation software flaws and security configuration issues. SCAP can be used to maintain the security of enterprise systems, such as automatically verifying the installation of patches, checking system security configuration settings, and examining systems for signs of compromise.

[4] TIGTA Ref. No. 2011-20-099, *The Mainframe Databases Reviewed Met Security Requirements; However, Automated Security Scans Were Not Performed* (Sept. 2011).

The IRS has deployed a SCAP-compliant tool (called the SCAP Compliance Checker) for monitoring Federal Desktop Core Configuration compliance on workstations. However, since February 2010, the IRS has been in the process of implementing additional tools for monitoring workstation compliance, called the Treasury Enhanced Security Initiative. The IRS believes the Treasury Enhanced Security Initiative is needed because of the features it has that the SCAP Compliance Checker does not have, including its ability to:

- Discover all assets on the IRS network.
- Identify rogue computers.
- Monitor administrative access privileges.
- Identify noncompliant security configurations for specific workstations.
- Prioritize highest risk systems for timely remediation.
- Automate remediation of some misconfigurations.

However, the Treasury Enhanced Security Initiative has experienced several delays due to the need for infrastructure upgrades and additional server resources, the IRS placing higher priorities on development of other systems, and filing season moratoriums.

2.1.5. For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.

The IRS has not yet fully documented Windows 7 FDCC/USGCB deviations. The User and Network Services organization indicated that it is currently working with stakeholders to identify and document all Windows 7 settings that do not comply with the Internal Revenue Manual or USGCB.

2.1.6. Documented proposed or actual changes to hardware and software configurations.

The IRS had not yet fully implemented configuration and change management controls to ensure that proposed or actual changes to hardware and software configurations are documented. During FY 2012, the Enterprise Services organization was in the process of implementing the Enterprise Configuration Management System (ECMS) to provide an enterprise solution for configuration and change management. The goal of the ECMS is to provide the IRS the capability to automate the configuration management process, enhance and improve the current change management process, provide a platform for the consolidation of change boards, provide a detailed change analysis capability, and support the adoption of robust configuration management and validation.

The ECMS briefing from the Enterprise Services Configuration and Change Management office cites a number of issues with IRS configuration and change management processes, including:

- A number of organizational change management processes are in place, without a clear understanding on how they link back to the "umbrella" configuration and change management standards.
    - Duplicative steps exist in many of the change management processes.
    - Inconsistent integration/coordination exists across processes.
- There is limited enforcement of configuration and change management standards to date.
- Multiple configuration control boards are in place, without a clear definition of what the hand-offs are between them.
- Configuration items do not always have an owner.
- No clear process hand-offs are defined between configuration management, change management, release management, and other service management processes.
- Organizations do not always have a clear understanding of Configuration and Change Management office staff roles.
- Many organizations do not have a clear understanding of what configuration and change management are and what steps they should be following to perform the related processes.
- Configuration and change management standards applied to organizationally owned tools are sometimes "lost in translation."
- The level of effort required across varied tools and procedures involved in performing configuration management activities is not clear, making it difficult to assign resources.

In July 2012, the Enterprise Services organization deployed the initial release of the ECMS. The ECMS includes a configuration item discovery tool, called the Discovery and Dependency Mapping Advanced tool, for the purpose of establishing a central repository of configuration items for which changes to configuration settings will need to be managed. The Enterprise Services organization plans for the full implementation of the ECMS to occur in FY 2014.

2.1.7. Process for timely and secure installation of software patches.

During the FY 2012 FISMA evaluation period, the TIGTA concluded fieldwork on an audit to evaluate the IRS's enterprise-wide patch management process.[5] The TIGTA identified that critical patches continue to be missing or are installed in an untimely manner. The IRS's own patch monitoring reports continue to report unpatched or untimely patched computers. For example, an IRS-wide patch monitoring report for Windows servers, called the Associate Chief

[5] TIGTA, Ref. No. 2012-20-012, *An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers* (Sep. 2012).

Information Officer Monthly Critical Patch Report, showed the IRS's overall patch compliance rate for critical patches averaged 88 percent in March 2012, ranging from a low of 63 percent to a high of 88 percent for the six-month period of October 2011 to March 2012. The March 2012 report showed that 7,329 potential vulnerabilities remain on IRS servers because 23 critical patches had not been installed on servers that need them; some of these patches had been released as far back as April 2011. These vulnerabilities could potentially be exploited to gain unauthorized access to information, disrupt operations, or launch attacks against other systems.

In addition, the IRS informed us that patching is still manual for the majority of its UNIX operating systems and is not in accordance with patch frequencies required by the Internal Revenue Manual. The Enterprise Operations organization is currently testing a process for automating patching on its UNIX servers.

IRS patch management policy did not provide clear expectations for when patches must be installed. In addition, the IRS has no mechanism to enforce timely patching or to hold system owners accountable for ensuring that their systems are timely patched or that they formally accept the risk of not patching systems timely. By not installing security patches in a timely fashion, the IRS increases the risk that known vulnerabilities in its systems may be exploited.

In March 2012, the Government Accountability Office (GAO) also reported[6] that the IRS did not always apply critical patches or ensure versions of its operating system were still supported by the vendor.

2.1.8. Software assessing (scanning) capabilities are fully implemented.

The IRS's software assessing (scanning) capabilities are not yet fully implemented. The IRS Organizational Common Controls Security Plan, Version 1, dated June 28, 2012, stated that the required vulnerability scanning control was not in place at the IRS organizational level and that the IRS Cybersecurity organization is still in the process of coordinating with information system owners to implement vulnerability scanning enterprise-wide. It also stated that, for vulnerability scans the IRS did conduct, analysis of the scans were not being performed by the system owners. In addition, it stated that the IRS has not yet deployed an automated mechanism to detect the presence of unauthorized software on IRS information systems.

In June 2012, the TIGTA reported[7] that the IRS had not implemented or enforced enterprise-wide procedures for monitoring and remediating weaknesses reported by nCircle scans. These scans help to identify what details about the information system are discoverable by adversaries and provide an associated risk level/score. During FY 2012, the IRS Cybersecurity organization was in the process of developing enterprise-wide standard operating

[6] GAO, GAO-12-393, *IRS Needs to Further Enhance Internal Control Over Financial Reporting and Taxpayer Data* (Mar. 2012).
[7] TIGTA, Ref. No. 2012-20-063, *Enterprise-Level Oversight Is Needed to Ensure Adherence to Windows Server Security Policies* (June 2012).

procedures for reviewing and analyzing the results of vulnerability scans and educating system owners on how to prioritize and resolve the identified weaknesses.

In September 2011, the TIGTA reported[8] that four individuals had installed and used personal unauthorized wireless devices on their laptops to connect to the IRS network. The TIGTA recommended that the IRS implement automated nationwide network scans for unauthorized wireless activity, devices, and software and improve processes to handle incidents of noncompliance with IRS security policy so that when unauthorized wireless activity is identified, subsequent investigations and disciplinary actions are effective. The IRS plans to complete the corrective action by September 28, 2012.

Additionally, our review of 10 sample systems' System Security Plans revealed that vulnerability scans were not being conducted in accordance with the IRS's defined frequency and process for the three General Support System's (GSS) in our sample.

2.1.9. Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards.

In June 2012, the TIGTA reported[9] that monthly scanning results were not consistently being used to correct improper settings on Windows servers in a timely manner; rather, security vulnerabilities of high, medium, and low risk levels were repeatedly reported on Windows Policy Checker reports for two or three consecutive months. During FY 2012, the Cybersecurity organization issued standard operating procedures for the monitoring and remediation of weaknesses reported by the Windows server configuration scans to all IRS staff administering Windows servers. The document stated that the Cybersecurity organization staff will work with the system administrators, application owners, and project offices to maintain a 100-percent compliance level on all Windows servers across all IRS organizations.

2.1.10. Patch management process is fully developed, as specified in organization policy or standards.

During the FY 2012 FISMA evaluation period, the TIGTA concluded fieldwork on an audit to evaluate the IRS's enterprise-wide patch management process.[10] The TIGTA identified that, although IRS policy requires the IRS to establish an enterprise-level group with responsibility for patch management, no enterprise-level group exists. Due to the lack of enterprise-level oversight and leadership, the IRS has not yet implemented key elements of its patch management policies and procedures that are needed to ensure all IRS systems are patched timely and operating

[8] TIGTA, Ref. No. 2011-20-101, *Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security* (Sept. 2011).
[9] TIGTA, Ref. No. 2012-20-063, *Enterprise-Level Oversight Is Needed to Ensure Adherence to Windows Server Security Policies* (June 2012).
[10] TIGTA, Ref. No. 2012-20-012, *An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers* (Sep. 2012).

securely. Specifically, the IRS has not:

- Completed the implementation of an accurate and complete inventory of its information technology assets, which is critical for ensuring that patches are identified and applied timely for all types of operating systems and software used within its environment.
- Implemented patch policy and monitoring processes to ensure patches are applied timely enterprise-wide.
- Implemented controls to ensure that unsupported operating systems are not putting the IRS at risk.

IRS processes to monitor the installation of required patches need improvement. The IRS's current monitoring processes are not sufficient to ensure that vulnerabilities resulting from unpatched systems are successfully and timely remediated. The IRS depends on the various IRS organizations that manage their own computers to frequently self-report patching data from their organization-level patch monitoring reports. This effort is labor intensive and results in incomplete and unverified patch data. For example, in March 2012, the IRS Information Technology organization reported that it had not received percentage data for 14 consecutive months from non-Information Technology managed Windows workstations needing critical patches, which it needed to track patch metrics in its Information Technology Internal Dashboard. Further, the IRS had not established patch performance metrics in terms of setting compliance rate goals and measuring them on a monthly basis to ensure IRS organizations are complying with security patch policy.

2.2. Please provide any additional information on the effectiveness of the organization's configuration management program that was not noted in the questions above.

To achieve FISMA-compliant configuration management, the IRS is in the process of implementing a number of tools to automate tasks, that when done manually, are extremely time-consuming and error-prone. However, we are concerned the IRS is not ensuring that it is avoiding tool redundancy and, therefore, excess cost or that it will be making the most efficient use of the data collections.

Tools or initiatives that the IRS already implemented or are in progress to improve its security posture include Business DNA (asset discovery), nCircle (vulnerability scanning), Security Compliance Posture Monitoring and Reporting (server configuration management), Treasury Enhanced Security Initiative (workstation configuration management), Altiris (Windows server patching), Guardium (database scanning), Knowledge Incident/Problem Service Asset Management (asset inventory), CiscoWorks (network management), Tivoli (older asset management tool), and a central repository for warehousing and integrating the collected data. The Cybersecurity organization has prepared an Information Technology Security Controls Tools Strategy for planning how all of this data will be organized and combined to provide near-real-time enterprise security intelligence for decision making.

As mentioned above, the Enterprise Services organization is also implementing a configuration and change management tool, called the ECMS. This solution is comprised of a number of commercial off-the-shelf products that include a configuration item discovery tool (the Discovery and Dependency Mapping Advanced tool), a central repository of configuration items and related components, change management analysis, and other tools for monitoring and maintaining configuration compliance. The Enterprise Services organization stated that until the ECMS is implemented, the IRS will continue to lack the capability to effectively implement configuration and change management.

We believe the IRS should ensure that data collected by its various tools and organizations will be efficiently utilized and that the IRS is not developing duplicative configuration management processes or products. For example, our discussions with the Cybersecurity and Enterprise Services organizations revealed that an approach for integrating the configuration management data collected by both organizations has not yet been formulated.

Identity and Access Management

Proper identity and access management ensures that users and devices are properly authorized to access information or information systems. Users and devices must be authenticated to ensure that they are who they identify themselves to be. In most systems, a user name and password serve as the primary means of authentication, while the system enforces authorized access rules established by the system administrator. To ensure that only authorized users and devices have access to a system, policy and procedures must be in place for the creation, distribution, maintenance, and eventual termination of accounts. The use of Personal Identity Verification (PIV) cards by all agencies, required by Homeland Security Presidential Directive-12 (HSPD-12),[11] is a major component of a secure, Government-wide account and identity management system.

The IRS has not fully implemented the following seven identity and access management attributes specified by the DHS metrics:

3.1.4. If multifactor authentication is in use, it is linked to the organization's PIV program, where appropriate.

3.1.5. Organization has adequately planned for implementation of PIV for logical access in accordance with government policies.

[11] On August 27, 2004, President Bush signed HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*. This directive established a new standard for issuing and maintaining identification badges for Federal employees and contractors entering Government facilities and accessing computer systems. The intent was to improve security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Agencies are required to use PIV badges (also referred to as SmartID cards) to access computer systems (logical access).

3.1.6. Ensures that the users are granted access based on needs and separation of duties principles.

3.1.7. Identifies devices with Internet Protocol addresses that are attached to the network and distinguishes these devices from users.

3.1.8. Identifies all user and nonuser accounts (refers to user accounts that are on a system.)

3.1.9. Ensures that accounts are terminated or deactivated once access is no longer required.

3.1.10. Identifies and controls use of shared accounts.

3.1.4. If multifactor authentication is in use, it is linked to the organization's PIV program, where appropriate.

During the FY 2012 FISMA evaluation period, the TIGTA concluded fieldwork on an audit to evaluate the implementation and security of the IRS's two-factor authentication for logical (system) access.[12] The IRS has not deployed multifactor authentication via the use of an HSPD-12 PIV card for all users for network and local access to nonprivileged or privileged accounts as required by Federal mandate. Therefore, the IRS's multifactor authentication is not yet linked to its PIV program.

3.1.5. Organization has adequately planned for implementation of PIV for logical access in accordance with Government policies.

The IRS has experienced significant delays in deploying PIV cards for logical access, which reveals the IRS's inadequate planning efforts. The Federal Government mandated that agencies implement PIV cards to access computer systems in August 2004. The IRS originally planned to complete the deployment by September 2011. The deployment is now planned to be completed by July 2013, but various issues threaten further delays, including:

- The inability of the IRS to require its employees to use their PIV cards for logical access to the network because it did not negotiate mandatory use of the cards with the National Treasury Employees Union.
- Resolving PIV card deployment for system administrators, who currently require separate identities to perform administrator services on computer systems.
- The large number (1,888) of IRS applications that are not yet PIV card-enabled and the lack of resources to change these existing applications.

[12] TIGTA, Ref. No. 2012-20-115, *Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected* (Sept. 2012).

3.1.6. Ensures that the users are granted access based on needs and separation of duties principles.

Two of the three GSSs in our sample did not have the controls in place to ensure users are granted access based on needs or to enforce separation of duties. Applications residing on GSSs often rely on the GSS to implement these controls; therefore, the applications residing on these GSSs would also inherit these weaknesses.

The most recent security control assessment for one of the two GSSs that did not have these controls in place stated that accounts are not managed, enforced, separated, or deployed with least privilege in accordance with IRS policy requirements for all GSS components. Also, the most recent security control assessment for the other GSS found controls for granting access based on needs and for separation of duties were not implemented. For example, the operating system administrator could perform database administrator functions.

In addition, the GAO reported in March 2012[13] that IRS authorization controls were not always functioning as intended and access authorization policies were not effectively implemented. For example, systems used to process tax and financial information did not fully prevent access by unauthorized users or excessive levels of access for authorized users. In addition, the IRS's compliance checks revealed unauthorized access to another system. During its monthly compliance check in August 2011, the IRS identified 16 users who had been granted access to the procurement system without receiving approval from the IRS's authorization system. Also, the data in a shared work area used to support accounting operations were fully accessible by network administration staff although they did not need such access.

3.1.7. Identifies devices with Internet Protocol addresses that are attached to the network and distinguishes these devices from users.

The IRS informed us that Business DNA will be its enterprise asset discovery tool for identifying devices on its network. Business DNA network scans can identify devices with Internet Protocol addresses that are attached to the network and distinguish these devices from users. However, the full implementation of the Business DNA tool is not expected to be completed until September 2012. Therefore, the IRS has not yet fully implemented this attribute.

We also found that one of our three sample GSSs did not have device identification and authentication in place. It did not uniquely identify and authenticate devices or users before establishing a connection. Also, its firewalls did not use the Terminal Access Controller Access Control System[14] to authenticate organization users or devices. Rather, these firewalls were accessed via a shared administrator account.

---

[13] GAO, GAO-12-393, *IRS Needs to Further Enhance Internal Control Over Financial Reporting and Taxpayer Data* (Mar. 2012).

[14] An enterprise access control security system that provides device/network access authentication, authorization, and accounting.

3.1.8. Identifies all user and nonuser accounts.

No information was provided to determine how the IRS identifies all user and nonuser accounts.

3.1.9. Ensures that accounts are terminated or deactivated once access is no longer required.

Three of our 10 sample systems (two GSSs and one application) did not have controls in place to ensure accounts are terminated or deactivated once access is no longer needed. The most recent security control assessment for one GSS found:

- The system did not disable inactive accounts after 120 days of inactivity and did not employ automated mechanisms to audit account creation, modification, disabling, and termination actions.
- Evidence was not provided to ensure system accounts are reviewed at least annually.
- The system was not configured to notify appropriate individuals when accounts were modified.
- Evidence was not provided to ensure system accounts were reviewed at least annually and automated mechanisms were employed to support system account management functions.
- No automated mechanisms existed to support information system account management functions.
- Inactive accounts were not automatically disabled.

For the other GSS, the most recent security control assessment found:

- Accounts were not automatically disabled.
- The log files did not contain any evidence of logging the account creation, modification, disabling, and termination actions of a user account.

For the one application, its most recent security control assessment found that it did not disable accounts after 45 days or remove accounts after 90 days of inactivity.

Further, the GAO reported in March 2012[15] that the IRS had not taken actions to remove active application accounts in a timely manner for employees who had separated or no longer needed access.

[15] GAO, GAO-12-393, *IRS Needs to Further Enhance Internal Control Over Financial Reporting and Taxpayer Data* (Mar. 2012).

3.1.10. Identifies and controls use of shared accounts.

One of the GSSs in our sample was not adequately identifying and controlling use of shared accounts. The most recent security control assessment found that the administrative account for this GSS was shared. For example, the operating system administrator had the ability to "switch user" into Oracle using the "root" password. This login process is not uniquely linked to any one individual. Rather, this access is "shared" among the operating system administrators. Sharing this account in this manner allows fully privileged actions to be taken on the system without any accountability. In addition, passwords were stored and transmitted in plaintext.

Also, in June 2012, the TIGTA reported[16] that administrative accounts on Windows servers were not being properly safeguarded in accordance with IRS policy. Specifically, administrators in two IRS organizations were using the built-in system administrator accounts to perform normal administrative duties rather than only in emergencies as required by IRS policy. Seven administrators in one organization and 14 administrators in the other were sharing the password to the built-in accounts and were using these accounts for administrative tasks rather than using their unique role-based administrator accounts. Consequently, individual accountability was lost as to by whom and for what purposes these full-privileged accounts were being accessed.

Security Training

The FISMA requires all Government personnel and contractors to complete annual security awareness training that provides instruction on threats to data security and responsibilities for information protection. It also requires specialized training for personnel and contractors with significant security responsibilities. Without adequate security training programs, agencies cannot provide appropriate training or ensure that all personnel receive the required training.

The IRS had not fully implemented the following security training attribute specified by the DHS metrics: 6.1.5. Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.

6.1.5. Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.

The DHS provided clarification for this attribute as it relates to contractors, stating that agencies should be providing and tracking completion of specialized training for contractors just as they would for Federal employees. The specialized training requirement is based on the role of the contractor, not just on contractor status. Whoever holds a significant security role needs to receive specialized role-based training.

[16] TIGTA, Ref. No. 2012-20-063, *Enterprise-Level Oversight Is Needed to Ensure Adherence to Windows Server Security Policies* (June 2012).

The IRS has not fully implemented identification and tracking of the status of specialized role-based training for contractors. However, the IRS stated it is making plans to implement such tracking by October 15, 2012. The Contractor Security Management office in the Agency-Wide Shared Services organization is currently leading efforts to modify its contractor tracking system to allow the identification of those contractors with significant security responsibilities, with subsequent plans to implement a process to monitor and track completion of contractor specialized training. Once identified, the IRS would rely on the contractors to provide and self-report the completion of their required specialized training hours. Preliminary IRS results indicated that 919 such contractors were employed during the FISMA FY 2012 reporting period, with only 99 of those having confirmed that they completed the required training.

The IRS did not agree that it should provide specialized training for contractors and supported its position by citing the U.S. Office of Personnel Management's Training Policy Handbook, which states:

> *Since contractors are selected for their expertise in a subject area, contractors may only be trained in skills they are not required to bring to the job. Contractors may be trained in rules, practices, procedures, and/or systems that are unique to the employing agency and essential to the performance of the contractor's assigned duties, such as agency computer security procedures. However, the authority for training of contractors is not in training law. It is in the authority to administer contracts. Training of contractors is subject to the decision of the chief contracting official.*

The IRS stated that to require it to provide, track, and report specialized training completions for contractors would present significant challenges, including requiring thousands of contract language modifications before it could enforce this requirement for contract employees.

Appendix I

Fiscal Year 2012 Reporting Metrics

Presented below is the list of reporting metrics questions and information as detailed in the *Fiscal Year 2012 Inspector General Federal Information Security Management Act (FISMA) Reporting Metrics.*[1] The list is presented in its entirety, along with the accompanying Purpose and Use information. Following each metric is a notation identifying each individual question as an Administration Priority (AP), a Key FISMA Metric (KFM), or a Baseline Question (Base). Many abbreviations in this list are used as presented in the original document and are not defined therein. However, we have provided the definitions in the Abbreviations page after the Table of Contents of this report.

1. CONTINUOUS MONITORING MANAGEMENT

1.1. Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

1.1.1. Documented policies and procedures for continuous monitoring (NIST 800-53: CA-7). (AP)

1.1.2. Documented strategy and plans for continuous monitoring (NIST 800-37 Rev. 1, Appendix G). (AP)

1.1.3. Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST 800-53, NIST 800-53A). (AP)

1.1.4. 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&M additions and updates, with the frequency defined in the strategy and/or plans (NIST 800-53, NIST 800-53A). (AP)

[1] U.S. Department of Homeland Security, National Cyber Security Division, *Fiscal Year 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, pp. 6–17 (Mar. 2012). The FISMA is encoded in Title III of the E-Government Act of 2002; Pub. L. No. 107-374, 116 Stat. 2899.

1.2. Please provide any additional information on the effectiveness of the organization's continuous monitoring management program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- The Federal Continuous Monitoring Working Group (CMWG) has determined that continuous monitoring (CM) of configurations is one of the first areas where CM capabilities need to be developed. This applies to both operating systems and widely used applications.
- Even with a completely hardened system, exploitation may still occur due to zero-day vulnerabilities. However, this forces attackers to elevate their sophistication for successful attacks.
- Rather, a robust continuous monitoring solution will be able to provide additional visibility for organizations to identify signs of compromise, though no single indicator may identify a definitive incident.

2. CONFIGURATION MANAGEMENT

2.1. Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

2.1.1. Documented policies and procedures for configuration management. (Base)

2.1.2. Standard baseline configurations defined. (Base)

2.1.3. Assessing for compliance with baseline configurations. (Base)

2.1.4. Process for timely, as specified in organization policy or standards, remediation of scan result deviations. (Base)

2.1.5. For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented. (Base)

2.1.6. Documented proposed or actual changes to hardware and software configurations. (Base)

2.1.7. Process for timely and secure installation of software patches. (Base)

2.1.8. Software assessing (scanning) capabilities are fully implemented (NIST 800-53: RA-5, SI-2). (Base)

2.1.9. Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2). (Base)

2.1.10. Patch management process is fully developed, as specified in organization policy or standards. (NIST 800-53: CM-3, SI-2). (Base)

2.2. Please provide any additional information on the effectiveness of the organization's configuration management program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- A key goal of configuration management is to make assets harder to exploit through better configuration.
- A key assumption is that configuration management covers the universe of assets to which other controls need to be applied (controls that are defined under asset management).
- To have a capable configuration management program, the configuration management capability needs to be:
  - Relatively complete, covering enough of the software base to significantly increase the effort required for a successful attack.
  - Relatively timely, being able to find and fix configuration deviations faster than they can be exploited.

3. IDENTITY AND ACCESS MANAGEMENT

3.1. Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices? If yes, besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes:

3.1.1. Documented policies and procedures for account and identity management (NIST 800-53: AC-1). (Base)

3.1.2. Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST 800-53, AC-2). (Base)

3.1.3. Identifies when special access requirements (*e.g.*, multifactor authentication) are necessary. (Base)

3.1.4. If multifactor authentication is in use, it is linked to the organization's PIV program, where appropriate (NIST 800-53, IA-2). (KFM)

3.1.5. Organization has adequately planned for implementation of PIV for logical access in accordance with Government policies (HSPD-12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). (AP)

3.1.6. Ensures that the users are granted access based on needs and separation of duties principles. (Base)

3.1.7. Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts.) (Base)

3.1.8. Identifies all user and nonuser accounts (refers to user accounts that are on a system. Examples of nonuser accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users.) (Base)

3.1.9. Ensures that accounts are terminated or deactivated once access is no longer required. (Base)

3.1.10. Identifies and controls use of shared accounts. (Base)

3.2. Please provide any additional information on the effectiveness of the organization's identity and access management program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- OMB and DHS have determined that Federal identity management (HSPD-12) is among the areas where additional controls need to be developed. See also OMB M-04-04 for web-based systems.
- Strong information system authentication requires multiple factors to securely authenticate a user. Secure authentication requires something you have, something you are, and something you know. A single-factor authentication mechanism, such as a username and password, is insufficient to block even basic attackers.
- The USG will first move to a two-factor authentication using PIV cards, though a stronger authentication solution would include all three factors.
- Enhanced identity management solutions also support the adoption of additional nonsecurity benefits, such as single sign-on, more useable systems, and enhanced identity capabilities for legal and nonrepudiation needs.

- A key goal of identity and access management is to make sure that access rights are only given to the intended individuals and/or processes.[2]
- To have a capable identity management program, this capability needs to be:
  - Relatively complete, covering all accounts.
  - Relatively timely, being able to find and remove stale or compromised accounts faster than they can be exploited.

4. INCIDENT RESPONSE AND REPORTING

4.1. Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

4.1.1. Documented policies and procedures for detecting, responding to, and reporting incidents (NIST 800-53: IR-1). (Base)

4.1.2. Comprehensive analysis, validation, and documentation of incidents. (KFM)

4.1.3. When applicable, reports to US-CERT within established time frames (NIST 800-53, 800-61, and OMB M-07-16, M-06-19). (KFM)

4.1.4. When applicable, reports to law enforcement within established time frames (SP 800-86). (KFM)

4.1.5. Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19). (KFM)

4.1.6. Is capable of tracking and managing risks in a virtual/cloud environment, if applicable. (Base)

4.1.7. Is capable of correlating incidents. (Base)

4.1.8. There is sufficient incident monitoring and detection coverage in accordance with Government policies (NIST 800-53, 800-61, and OMB M-07-16, M-06-19). (Base)

4.2. Please provide any additional information on the effectiveness of the organization's incident management program that was not noted in the questions above.

[2] This is done, of course, by establishing a process to assign attributes to a digital identity and by connecting an individual to that identity. However, this would be pointless without subsequently using it to control access.

Purpose and Use

These questions are being asked for the following reasons:

- Given real world realities, it is reasonable to expect that some attacks will succeed. Organizations need to be able to detect those attacks. Ideally, organizations would defend against those attacks in real time; but at a minimum, organizations are expected to determine the kinds of attacks that are most successful.
- This allows the organization to use this information about successful attacks and their impact to make informed risk-based decisions about where it is most cost effective and essential to focus security resources.

5. RISK MANAGEMENT

5.1. Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

5.1.1. Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process. (Base)

5.1.2. Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev. 1. (Base)

5.1.3. Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev. 1. (Base)

5.1.4. Addresses risk from an information system 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. (Base)

5.1.5. Categorizes information systems in accordance with Government policies. (Base)

5.1.6. Selects an appropriately tailored set of baseline security controls. (Base)

5.1.7. Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation. (Base)

5.1.8. Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly,

operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (Base)

5.1.9. Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable. (Base)

5.1.10. Ensures information security controls are monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. (Base)

5.1.11. Information system specific risks (tactical), mission/business specific risks, and organizational level (strategic) risks are communicated to appropriate levels of the organization. (Base)

5.1.12. Senior officials are briefed on threat activity on a regular basis by appropriate personnel (*e.g.*, CISO). (Base)

5.1.13. Prescribes the active involvement of information system owners and common control providers, Chief Information Officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks. (Base)

5.1.14. Security authorization package contains system security plan, security assessment report, and POA&M in accordance with Government policies (NIST SP 800-18, SP 800-37). (Base)

5.1.15. Security authorization package contains accreditation boundaries for organization information systems defined in accordance with Government policies. (Base)

5.2. Please provide any additional information on the effectiveness of the organization's risk management program that was not noted in the questions above.

Purpose and Use:

These questions are being asked for the following reasons:

- One goal in issuing these FISMA questions is to further empower OIGs to focus on how agencies are evaluating risk and prioritizing security issues.
- OIGs are encouraged to use a type of risk analysis as specified in NIST 800-39 to evaluate findings and compare those to (1) existing organization priorities and (2) Administration

priorities and key FISMA metrics identified in the CIO metrics to determine areas of weakness and highlight the significance of security issues.

6. SECURITY TRAINING

6.1. Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

6.1.1. Documented policies and procedures for security awareness training (NIST 800-53: AT-1). (Base)

6.1.2. Documented policies and procedures for specialized training for users with significant information security responsibilities. (Base)

6.1.3. Security training content based on the organization and roles, as specified in organization policy or standards. (Base)

6.1.4. Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training. (KFM)

6.1.5. Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training. (KFM)

6.1.6. Training material for security awareness training does not contain appropriate content for the organization (NIST SP 800-50, SP 800-53). (Base)

6.2. Please provide any additional information on the effectiveness of the organization's security training program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- Some of the most effective attacks on cyber-networks world-wide currently are directed at exploiting user behavior. These include phishing attacks, social engineering to obtain passwords, and introduction of malware via removable media.
- These threats are especially effective when directed at those with elevated network privileges and/or other elevated cyber responsibilities.
- DHS has determined that some metrics in this section are prioritized as Key FISMA Metrics.
- Some questions in this section also contain baseline information to be used to assess future improvement in performance.

- The metrics will be used to assess the extent to which organizations are providing adequate training to address these attacks and threats.

7. PLAN OF ACTION & MILESTONES (POA&M)

7.1. Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

7.1.1. Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation. (Base)

7.1.2. Tracks, prioritizes, and remediates weaknesses. (Base)

7.1.3. Ensures remediation plans are effective for correcting weaknesses. (Base)

7.1.4. Establishes and adheres to milestone remediation dates. (Base)

7.1.5. Ensures resources are provided for correcting weaknesses. (Base)

7.1.6. POA&Ms include security weaknesses discovered during assessments of security controls and requiring remediation. (Do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25). (Base)

7.1.7. Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25). (Base)

7.1.8. Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25). (Base)

7.2. Please provide any additional information on the effectiveness of the organization's POA&M program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- POA&M processes are important as part of the risk management process to track problems and to decide which ones to address.

8. REMOTE ACCESS MANAGEMENT

8.1. Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

8.1.1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST 800-53: AC-1, AC-17). (Base)

8.1.2. Protects against unauthorized connections or subversion of authorized connections. (Base)

8.1.3. Users are uniquely identified and authenticated for all access (NIST 800-46, Section 4.2, Section 5.1). (Base)

8.1.4. Telecommuting policy is fully developed (NIST 800-46, Section 5.1). (Base)

8.1.5. If applicable, multifactor authentication is required for remote access (NIST 800-46, Section 2.2, Section 3.3). (KFM)

8.1.6. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms. (Base)

8.1.7. Defines and implements encryption requirements for information transmitted across public networks. (KFM)

8.1.8. Remote access sessions, in accordance to OMB M-07-16, are timed out after 30 minutes of inactivity, after which reauthentication is required. (Base)

8.1.9. Lost or stolen devices are disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines). (Base)

8.1.10. Remote access rules of behavior are adequate in accordance with Government policies (NIST 800-53, PL-4). (Base)

8.1.11. Remote access user agreements are adequate in accordance with Government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6). (Base)

8.2. Please provide any additional information on the effectiveness of the organization's remote access management that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- Adequate control of remote connections is a critical part of boundary protection.

- Attackers exploit boundary systems on Internet-accessible DMZ networks (and on internal network boundaries) and then pivot to gain deeper access on internal networks. Responses to the above questions will help agencies deter, detect, and defend against unauthorized network connections/access to internal and external networks.
- Remote connections allow users to access the network without gaining physical access to organization space and the computers hosted there. Moreover, the connections over the Internet provide opportunities for compromise of information in transit. Because these connections are beyond physical security controls, they need compensating controls to ensure that only properly identified and authenticated users gain access and that the connections prevent hijacking by others.

9. CONTINGENCY PLANNING

9.1. Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

9.1.1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST 800-53: CP-1). (Base)

9.1.2. The organization has performed an overall Business Impact Analysis (BIA) (NIST SP 800-34). (Base)

9.1.3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34). (Base)

9.1.4. Testing of system-specific contingency plans. (Base)

9.1.5. The documented business continuity and disaster recovery plans are in place and can be implemented when necessary (FCD1, NIST SP 800-34). (Base)

9.1.6. Development and fully implementable of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST 800-53). (Base)

9.1.7. Performance of regular ongoing testing or exercising of business continuity/ disaster recovery plans to determine effectiveness and to maintain current plans. (Base)

9.1.8. After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34). (Base)

9.1.9. Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)

9.1.10. Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).

9.1.11. Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)

9.1.12. Contingency planning that considers supply chain threats. (Base)

9.2. Please provide any additional information on the effectiveness of the organization's contingency planning program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- Contingency planning deals with risks which occur rarely. As such, there is a temptation to ignore these risks.
- The purpose of this section is to determine if the organization is giving adequate attention to the rare events which have such significant consequences that they become first-priority risks.

10. CONTRACTOR SYSTEMS

10.1. Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes:

10.1.1. Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in public cloud. (Base)

10.1.2. The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines. (Base)

10.1.3. A complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in public cloud. (Base)

10.1.4. The inventory identifies interfaces between these systems and organization-operated systems (NIST 800-53: PM-5). (Base)

10.1.5. The organization requires appropriate agreements (*e.g.*, MOUs, Interconnection Security Agreements, contracts, *etc.*) for interfaces between these systems and those that it owns and operates. (Base)

10.1.6. The inventory of contractor systems is updated at least annually. (Base)

10.1.7. Systems that are owned or operated by contractors or entities, including organization systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines. (Base)

10.2. Please provide any additional information on the effectiveness of the organization's contractor systems program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- These questions are being asked because in the past some Federal agencies tended to assume that they were not responsible for managing the risk of contractor systems.
- The key question is "Are these contractor-operated systems being managed to ensure that they have adequate security and can the DAA make an informed decision about whether or not to accept any residual risk?"

11. SECURITY CAPITAL PLANNING

11.1. Has the organization established a security capital planning and investment program for information security? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

11.1.1. Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process. (Base)

11.1.2. Includes information security requirements as part of the capital planning and investment process. (Base)

11.1.3. Establishes a discrete line item for information security in organizational programming and documentation (NIST 800-53: SA-2). (Base)

11.1.4. Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST 800-53: PM-3). (Base)

11.1.5. Ensures that information security resources are available for expenditure as planned. (Base)

11.2. Please provide any additional information on the effectiveness of the organization's security capital planning program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- One key area of capital investment in the next few years will be investments in the tools and other infrastructure needed for adequate continuous monitoring. Fortunately, most of these tools also support (and are needed for) good network and system operations. Thus, many of these tools may already be in place.
- This section might equally consider operational budgeting. Clearly, good security requires a wise investment of operational resources, not just capital ones.

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
Bret Hunter, Senior Auditor
Mary Jankowski, Senior Auditor
Louis Lee, Senior Auditor
Midori Ohno, Senior Auditor
Esther Wilson, Senior Auditor
Linda Nethery, Information Technology Specialist

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

Appendix IV

Treasury Inspector General for Tax Administration Information Technology Security-Related Reports Issued During the Fiscal Year 2012 Evaluation Period

1. Treasury Inspector General for Tax Administration (TIGTA), Ref. No. 2011-20-076, *The IRS2GO Smartphone Application Is Secure, but Development Process Improvements Are Needed* (Aug. 2011).
2. TIGTA, Ref. No. 2011-20-088, *The Modernized e-File Release 6.2 Included Enhancements, but Improvements Are Needed for Tracking Performance Issues and Security Weaknesses* (Sept. 2011).
3. TIGTA, Ref. No. 2011-20-116, *Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2011* (Sept. 2011).
4. TIGTA, Ref. No. 2011-20-111, *Continued Centralization of the Windows Environment Would Improve Administration and Security Efficiencies* (Sept. 2011).
5. TIGTA, Ref. No. 2011-20-101, *Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security* (Sept. 2011).
6. TIGTA, Ref. No. 2011-20-099, *The Mainframe Databases Reviewed Met Security Requirements; However, Automated Security Scans Were Not Performed* (Sept. 2011).
7. TIGTA, Ref. No. 2012-20-019, *The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed* (Mar. 2012).
8. TIGTA, Ref. No. 2012-20-041, *Disaster Recovery Testing Is Being Adequately Performed, but Problem Reporting and Tracking Can Be Improved* (May 2012).
9. TIGTA, Ref. No. 2012-20-063, *Enterprise-Level Oversight Is Needed to Ensure Adherence to Windows Server Security Policies* (June 2012).

Appendix V

Glossary of Terms

Term	Definition
Accreditation (or Authorization) Boundary	Includes all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems to which the information system is connected.
Administrative Account	A user account with full privileges on a computer.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication through the use of boundary protection devices.
Boundary System	Physical or logical perimeter of a system.
Cloud (Computing) Environment	The use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams.
Configuration Baseline	A set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and that can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
Configuration Items	Assets, service components, or other items that are (or will be) controlled by configuration management.

Term	Definition
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of products and systems through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Demilitarized Zone	A network segment inserted as a "neutral zone" between an organization's private network and the Internet.
Device Identification and Authentication	The information system uniquely identifies and authenticates before establishing a connection. See Authentication.
Federal Desktop Core Configuration	OMB-mandated set of security configurations for all Federal workstation and laptop devices that run either Windows XP or Vista.
Firewall	A gateway that limits access between networks in accordance with local security policy.
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Identity and Access Management	Addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements.
Internal Revenue Manual	The IRS publication of its information security policies, guidelines, standards, and procedures in order for IRS divisions and offices to carry out their respective responsibilities in information security.
Internet Protocol	Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
Least Privilege	The security objective of granting users only those accesses they need to perform their official duties.

Term	Definition
Logical Access	Controls used to determine the electronic information and systems that users and other systems may access and the actions that may be performed to the information accessed.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the computer's data, applications, or operating system.
Milestone	The "go/no-go" decision point in a project; it is sometimes associated with funding approval to proceed.
Multifactor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (1) something you know (*e.g.*, password/PIN); (2) something you have (*e.g.*, cryptographic identification device, token); or (3) something you are (*e.g.*, physical characteristic).
nCircle	An automated tool that scans computers for vulnerabilities related to network exploits and renders a report of findings.
Operating System	A set of software that manages computer hardware resources and provides common services for computer programs. The operating system is a vital component of the system software in a computer system. Application programs require an operating system to function.
Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.
Phishing (Attack)	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.
Plaintext	Intelligible data that has meaning and can be understood without the application of decryption.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Term	Definition
Policy Checker	An automated tool that reads the security settings of computers and logs any noncompliant setting to text files.
Privileged Account	Individuals who have access to set "access rights" for users on a given system. Sometimes referred to as system or network administrative accounts.
Remote Access	Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (*e.g.*, the Internet).
Rogue Computer	An unauthorized computer on a network.
Security Capital Planning	The integration of information technology security and capital planning processes to ensure that agency resources are protected and risk is effectively managed.
Separation of Duties	As a security principle, its primary objective is the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users.
Single-factor Authentication	Authentication using one factor (*e.g.*, a username or password) to achieve authentication. See Authentication.
Single Sign-On	Provides the capability to authenticate once and be subsequently and automatically authenticated when accessing various target systems. It eliminates the need to separately authenticate and sign on to individual applications and systems, essentially serving as a user surrogate between client workstations and target systems.
Social Engineering	An attempt to trick someone into revealing information (*e.g.*, a password) that can be used to attack systems or networks.
Two-factor Authentication	Authentication using two factors to achieve authentication. See Multifactor Authentication.
US-CERT	A partnership between the Department of Homeland Security and the public and private sectors established to protect the Nation's Internet infrastructure. US-CERT coordinates defense against and responses to cyberattacks across the Nation.

Term	Definition
Virtual Environment	The physical system running a host operating system and hypervisor (*i.e.*, software that allows a single host to run one or more guest operating systems).
Vulnerability Scanning (*i.e.*, Software Assessing)	Scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms.
Zero-Day Vulnerability	An exploit that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known. There are zero days between the time the vulnerability is discovered and the first attack. Given time, the software company can fix the code and distribute a patch or software update.