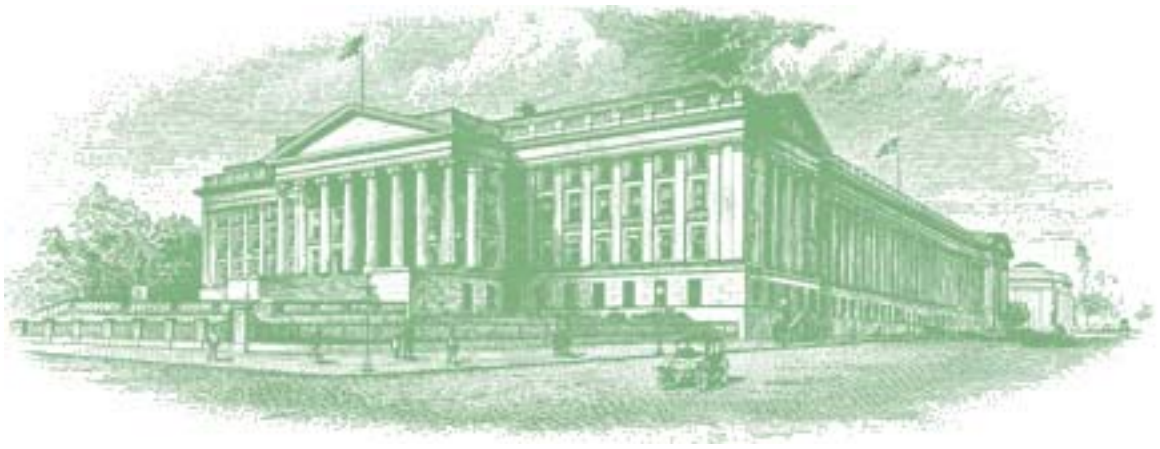
Audit Report



OIG-11-023

INFORMATION TECHNOLOGY: The Department of the Treasury Federal Information Security Management Act Fiscal Year 2010 Audit

November 12, 2010

Office of Inspector General

Department of the Treasury

This report has been reissued to correct the report number on the cover page from OIG-10-023 to OIG-11-023. Additionally, at the request of the Treasury Inspector General for Tax Administration, certain information on page 16 of their report is redacted pursuant to 5 U.S.C. §552(b)(2).

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

November 12, 2010

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

DIANE LITMAN
ACTING DEPUTY ASSISTANT SECRETARY OF INFORMATION SYSTEMS AND CHIEF INFORMATION OFFICER

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

SUBJECT: The Department of the Treasury Federal Information Security Management Act Fiscal Year 2010 Audit

We are pleased to transmit the following reports:

- The Department of the Treasury Federal Information Security Management Act Fiscal Year 2010 Performance Audit, November 10, 2010
- Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2010 (Audit # 2011-20-003), November 10, 2010

The Federal Information Security Management Act (FISMA)[1] requires an annual independent evaluation of the Department of the Treasury's information security program and practices. To meet FISMA requirements, we contracted with KPMG LLP, an independent certified public accounting firm, to perform the FISMA evaluation of Treasury's non-Internal Revenue Service (IRS) unclassified systems. KPMG's work was largely driven by the Office of Management and Budget's (OMB) FISMA 2010 Reporting Guidelines. Attachment 1 contains KPMG's report and *The Department of the Treasury's Consolidated Response to OMB's FISMA 2010 Questions for Inspectors General* (Appendix II of KPMG's report). The response incorporates our response as well as that of the Treasury Inspector General

[1] 44 U.S.C. §§ 3541–3549.

for Tax Administration (TIGTA). Attachment 2 contains TIGTA's stand alone evaluation of FISMA compliance for IRS systems.[2]

Based on the results of KPMG's audit, those reported by TIGTA, and a related report by the Government Accountability Office (GAO),[3] we determined that Treasury's information security program is in place and generally consistent with FISMA, but improvements are needed.

The KPMG audit of Treasury's unclassified systems (except for those of IRS) indicated that additional steps are required to ensure that Treasury's information security risk management program and practices fully comply with applicable National Institute of Standards and Technology standards and guidelines and FISMA requirements. Specifically, KPMG reported that:

1. Logical and physical account management activities were not consistently performed
2. Outsourcing the information system security officer role created an information technology governance concern at Financial Management System
3. Plan of actions and milestones were not updated timely and maintained at Financial Management System and Office of the Comptroller of the Currency
4. Security incidents were not reported timely at Bureau of the Public Debt and Alcohol and Tobacco Tax and Trade Bureau
5. Reviews of audit logs were not documented at Bureau of Engraving and Printing
6. Electronic media destruction process at Financial Crimes Enforcement Network was not fully compliant with its internal policies
7. Password settings were not properly configured to lockout for a Bureau of the Public Debt system

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

---

[2] We did not review the work performed by TIGTA to evaluate the information security program and practices of IRS. Our overall conclusions, insofar as they relate to IRS, are based solely on TIGTA's report (attachment 2). We did, however, coordinate with TIGTA on the scope and methodology, including sample selection, of our respective engagements.

[3] *FINANCIAL AUDIT: IRS's Fiscal Years 2010 and 2009 Financial Statements* (GAO-11-142, dated November 2010)

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

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

ATTACHMENT 1

The Department of the Treasury
Federal Information Security Management Act
Fiscal Year 2010 Performance Audit,
November 10, 2010

The Department of the Treasury
Federal Information Security Management Act
Fiscal Year 2010 Performance Audit

November 10, 2010

KPMG LLP
2001 M Street, NW
Washington, DC 20036

The Department of the Treasury
Federal Information Security Management Act Fiscal Year 2010 Performance Audit

Table of Contents

FISMA Performance Audit Report

Appendices

KPMG LLP
2001 M Street, NW
Washington, DC 20036-3389

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

Re: The Department of the Treasury Federal Information Security Management Act Fiscal Year 2010 Performance Audit

Dear Mr. Thorson:

This report presents the results of our independent evaluation of the 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). FISMA requires that the independent evaluation be performed by the agency Inspector General (IG) or an independent external auditor as determined by the IG. The Department of the Treasury Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct this independent evaluation (referred to herein as a "performance audit").

We conducted our performance audit in accordance with generally accepted government auditing standards (GAGAS) issued by the Comptroller General of the United States (U.S.). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The objective of the performance audit was to determine the effectiveness of the Department of the Treasury's information security program and practices for its unclassified systems, including the Department of the Treasury's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We based our work, in part, on an assessment of fifteen (15) information systems across thirteen (13) Treasury components. The scope of our work did not include the Internal Revenue Service (IRS), as the component was audited by the Treasury Inspector General for Tax Administration (TIGTA). Additional details regarding the scope of our performance audit are included in the *Objective, Scope, and Methodology* section of this report.

Based on our audit work, we concluded that the U.S. Department of the Treasury's information security program for its non-IRS bureaus was 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 and Physical Account Management Activities Were Not Consistently Performed
2. Outsourcing the Information System Security Officer (ISSO) Role Created an Information Technology (IT) Governance Concern at Financial Management System (FMS)
3. Plan of Action and Milestones (POA&Ms) Were Not Updated Timely and Maintained at FMS and Office of the Comptroller of the Currency (OCC)
4. Security Incidents Were Not Reported Timely at Bureau of the Public Debt (BPD) and Alcohol and Tobacco Tax and Trade Bureau (TTB)
5. Reviews of Audit Logs Were Not Documented at Bureau of Engraving and Printing (BEP)
6. Electronic Media Destruction Process at Financial Crimes Enforcement Network (FinCEN) Was Not Fully Compliant with Its Internal Policies
7. Password Settings Were Not Properly Configured to Lockout for a BPD System

We have made 29 recommendations related to these control deficiencies that, if addressed by management, will strengthen the respective bureaus, offices, and the Department's information security program.

This performance audit did not constitute an audit of financial statements in accordance with GAGAS. We were not engaged to, and did not, render an opinion on the Department of the Treasury's internal controls over financial reporting or over financial management systems (for purposes of OMB Circular No. A-127, *Financial Management Systems–Revised*, dated January 9, 2009). We tested controls that were implemented as of June 30, 2010. 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 conditions or because compliance with controls may deteriorate.

Appendix I, *Status of Prior Year Findings,* summarizes the U.S. Department of the Treasury's progress in addressing prior year recommendations. Appendix II, provides *The Department of the Treasury's Consolidated Response to OMB's FISMA 2010 Questions for Inspectors General.* Appendix III, *Approach to Selection of Subset of Systems,* describes how we selected systems for review. Appendix IV, *Selected Security Control Classes and Families,* describes the selected NIST Special Publication 800-53 security controls reviewed for each of the selected systems, and Appendix V contains a list of acronyms used in this report.

Sincerely,

KPMG LLP

November 10, 2010

BACKGROUND

Federal Information Security Management Act (FISMA)

Title III of the E-Government Act of 2002 (the Act), commonly referred to as the Federal Information Security Management Act (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, the Comptroller General, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation of their information security programs and practices 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 to an information system. This rating is assigned to an information system based on the agency's assessment of the system's confidentiality, integrity, and availability. NIST FIPS Publication 199 and NIST Special Publication 800-60 Revision 1, *Guide to Mapping Types of Information and Information Systems to Security Categories (2 Volumes)*, outline a framework that requires agencies to evaluate and categorize the potential magnitude of harm that a breach of security associated with specific information and information systems could have on agency operations and assets. The framework provides agencies with standards and guidance on how agencies should group information for evaluation, evaluate and categorize information and information systems, and document the process.

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. FIPS Publication 200 specifies seventeen (17) controls families that must be addressed when implementing security controls to adequately mitigate risk to an acceptable level.

NIST Special Publication 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*, further defines the seventeen (17) controls families outlined in FIPS Publication 200 by defining

the minimum set of security controls for non-national security systems of all Federal agencies within each of the controls families. NIST Special Publication 800-53 Revision 2 groups the seventeen (17) controls families into three (3) control classes (management, operational, and technical security controls). Management controls are the safeguards or countermeasures, related to an information system, that focus on the management of risk and system security. Operational controls are the safeguards and countermeasures for an information system that are primarily implemented and executed by individuals (as opposed to information systems). Technical controls are the safeguards or countermeasures for an information system that are primarily implemented and executed by the system through mechanisms contained in the hardware, software, or firmware components of the system. Table 1 details the security control classes and families.

Table 1: Selected Security Control Classes and Families

Security Control Class	Security Control Family
Management	Risk Assessment
	Planning
	System and Services Acquisition
	Certification, Accreditation, and Security Assessments
Operational	Physical and Environmental Protection
	Contingency Planning
	Configuration Management
	Maintenance
	Media Protection
	Identification and Authentication
Technical	Access Control
	Audit and Accountability
	System and Communications Protection

Source: NIST Security Standards (see Appendix IV)

Treasury Bureaus/Offices (Bureaus)

Treasury is comprised of fourteen (14) operating bureaus, 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 (U.S.) currency (paper), securities, and other official certificates and awards.
3. **Bureau of the Public Debt (BPD) –** Borrows the money needed to operate the Federal government. It administers the public debt by issuing and servicing U.S. Treasury marketable, savings, and special securities.
4. **Community Development Financial Institution (CDFI) Fund –** Created to expand the availability of credit, investment capital, and financial services in distressed urban and rural communities.
5. **Departmental Offices (DO) –** Primarily responsible for policy formulation. The DO is composed of divisions headed by Assistant Secretaries, some of whom report to Under Secretaries.

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

The scope of KPMG's 2010 FISMA audit did not include the IRS.

Treasury Information Security Management Program

Treasury Office of the Chief Information Officer (OCIO)

The Treasury Chief Information Officer (TCIO) is responsible for providing Treasury-wide leadership and direction for all areas of information and technology management, as well as the oversight of a number of information technology (IT) programs. Among these programs is Cyber Security, which has responsibility for the implementation and management of Treasury-wide IT security programs and practices. Through its mission, the Treasury Office of the Chief Information Officer (OCIO) Cyber Security Program develops and implements IT security policies and provides policy compliance oversight for both unclassified and classified systems managed by each of Treasury's bureaus. The OCIO, Cyber Security Program's mission focuses on the following areas:

1. **Cyber Security Policy and Program Performance Measurement** – Manages and coordinates the Departmental cyber security policy for sensitive (unclassified) systems throughout the Department, assuring these policies and requirements are updated to address today's threat environment, and conducts program performance, progress monitoring and analysis.

2. **Cyber Security FISMA Performance and Technical Review** – Provides assistance, conducts reviews, and tracks metrics to enhance security performance, thereby strengthening the overall cyber security posture of the Department.
3. **Vulnerability Analysis, Configuration, and Planning** – Analyzes current and emerging technologies and directs the Department's strategies and plans to mitigate cyber security risks from configuration and other vulnerabilities.
4. **Cyber Critical Infrastructure Protection (CIP)** – Implements cyber-related requirements of Homeland Security Presidential Directive No. 7, *Critical Infrastructure Identification, Prioritization, and Protection*, focusing on the protection of Department-owned cyber assets.
5. **Treasury Computer Security Incident Response Capability (TCSIRC)** – Leads the TCSIRC and provides Department-wide policy to the operation of each bureau's Computer Security Incident Response Center (CSIRCs). It also facilitates incident reporting with external reporting entities and conducts performance monitoring of CSIRCs within the Department.
6. **National Security Systems** – Manages and coordinates the Department-wide program to address the cyber security requirements of national security systems through the development of policy and program or technical security performance reviews.
7. **Cyber Security Sub-Council (CSS) of the TCIO Council** – Serves 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.

The TCIO has tasked the Associate Chief Information Officer for Cyber Security (ACIOCS) with the responsibility of managing and directing the OCIO's Cyber Security program, as well as ensuring compliance with statutes, regulations, policies, and guidance. The ACIOCS and the Cyber Security Program have established Treasury Directive Publication (TD P) 85-01, *Treasury Information Technology Security Program*, as the Treasury-wide IT security policy to provide for information security for all information and information systems that support the mission of the Treasury, including those operated by another Federal agency or contractor on behalf of Treasury. In addition, as OMB periodically releases updates/clarifications of FISMA or as NIST releases updates to publications, the ACIOCS and the Cyber Security Program have responsibility to interpret and release updated policy for Treasury. The ACIOCS and the Cyber Security Program are also responsible for promoting and coordinating a Treasury-wide IT security program, as well as monitoring and evaluating the status of Treasury's IT security posture and compliance with statutes, regulations, policies, and guidance. Lastly, the ACIOCS has the responsibility of managing Treasury's IT CIP program for Treasury information technology assets.

Bureau Chief Information Officers (CIOs)

Organizationally, the Treasury has established bureau-level and office Chief Information Officers (CIOs) under the OCIO. The CIOs are responsible for managing the IT security program for their bureau, as well as advising the bureau head on significant issues related to the bureau IT security program. The CIOs also have the responsibility for overseeing the development of procedures that comply with Treasury OCIO policy and guidance and federal statutes, regulations, policy, and guidance. The bureau Chief Information Security Officers (CISO) are tasked by their respective CIOs to serve as the central point of contact for the bureau's IT security program, as well as to develop and oversee the bureau's IT security program. This includes the development of policies, procedures, and guidance required to implement and monitor the bureau IT security program.

Treasury – Bureau OCIO Collaboration

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

OBJECTIVE, SCOPE, & METHODOLOGY

The objectives for this performance audit were to determine the effectiveness of Treasury's information security programs and practices as of June 30, 2010, and to determine whether non-IRS Treasury bureaus had implemented:

- An information security program, consisting of policies, procedures, and security controls consistent with the FISMA legislation
- The security controls catalog contained in NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*.

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

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation, Presidential directives, OMB Memorandum 10-15, *FY 2010 Reporting Instructions for Federal Information Security Management Act and Agency Privacy Management*, and NIST standards and guidelines as outlined in the *Criteria* section. We reviewed the Treasury information security program from both the Department-level perspective for Treasury-wide program level controls and the Bureau-level implementation perspective. We considered each area above to reach an overall conclusion regarding Treasury's information security program and practices.

KPMG took a phased approach to satisfy the audit's objective. Specifically, the following three phases were employed:

I. Assessment of Department-Level Compliance

To gain an overall enterprise-level understanding, we assessed management, policies, and guidance for the overall Treasury-wide information security program per requirements defined in FISMA and OMB Memorandum 10-15, NIST Special Publication 800-53, as well as Treasury guidelines developed in response to FISMA. This included program controls applicable to information security governance, certification and accreditation, security configuration management, incident response and reporting, security training, plan of action and milestones (POA&M), remote access, account and identity management, continuous monitoring, contingency planning, and contractor systems.

II. Assessment of Bureau-Level Compliance

To gain an overall bureau-level understanding, we assessed the implementation of the guidance for the 13 bureau and office-wide information security programs per requirements defined in FISMA and OMB Memorandum 10-15, NIST Special Publication 800-53, as well as Treasury guidelines developed in response to FISMA. This included program controls applicable to information security governance, certification and accreditation, security configuration management, incident response and reporting, security training, POA&M, remote access, account and identity management, continuous monitoring, contingency planning, and contractor systems.

III. Assessment of the Implementation of Select Security Controls from the NIST SP 800-53 Revision 2

To gain an overall understanding of how effective the bureaus implemented information security programs at the system level, we assessed the implementation of a selection of security controls from the NIST SP 800-53 Revision 2 for a representative subset of Treasury information systems (*see Appendix IV*).

To conclude on the audit's objectives, our scope included evaluating the information security practices and policies established by the Treasury OCIO. In addition, we evaluated the information security practices, policies, and procedures in use across the thirteen (13) bureaus of the Treasury, excluding the IRS.

We also tested a representative subset of fifteen (15) information systems from a total population of 112 non-IRS major applications and general support systems as of April 14, 2010.[1] We tested the fifteen (15) information systems to determine whether bureaus were effective in implementing Treasury's security program and meeting the FIPS 200 minimum security standards to protect information and information systems. Appendix III, *Approach to Selection of Subset of Systems*, provides additional details regarding our system selection. The subset of systems encompassed systems managed and operated by twelve (12) of 14 Treasury bureaus, excluding IRS and TIGTA[2].

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

- Controls that were shared across a number of information systems, such as common controls.
- Controls that were likely to change over time (i.e. volatile) and require human intervention.
- 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 thirteen (13) non-IRS bureaus. We also evaluated Treasury and bureaus' policies, procedures, and guidelines. Lastly, we evaluated selected security-related documents and records, including certification and accreditation packages, configuration assessment results, and training records.

We performed our fieldwork at Treasury's headquarters offices in Washington, D.C., and bureau locations in Washington, D.C.; Hyattsville, Maryland; McLean, Virginia; Parkersburg, West Virginia; and Newark, Delaware during the period of April 26, 2010 through September 30, 2010. During our performance audit, we met with Treasury management to discuss our preliminary conclusions.

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

[2] A decision was made to inspect only one (1) OIG system every year.

Criteria

Our approach to this FISMA performance audit was based on federal information security guidance developed by NIST and OMB. NIST Special Publications provide guidelines that are considered essential to the development and implementation of agencies' security programs.[3] The following is a listing of the criteria used in the performance of the Fiscal Year (FY) 2010 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 Revision 1, *Guide for Developing Security Plans for Information Technology Systems*
  - 800-30, *Risk Management Guide for Information Technology Systems*
  - 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
  - 800-39, *Managing Risk from Information Systems: An Organizational Perspective*
  - 800-34, *Contingency Planning Guide for Information Technology Systems*
  - 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*
  - 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*
  - 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*
  - 800-61, *Computer Security Incident Handling Guide*
  - 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*

- OMB Memoranda
  - 04-04, *E-Authentication Guidance for Federal Agencies*
  - 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*
  - 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*
  - 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
  - 07-18, *Ensuring New Acquisitions Include Common Security Configurations*
  - 08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)*
  - 10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*

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

[3] Note (per OMB instructions): 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.

OVERALL AUDIT RESULTS

We concluded that the Department's information security program for its non-IRS bureaus was generally consistent[4] with the FISMA legislation and related information security policies, standards, and guidelines. However, the program was not fully effective, resulting in the identification of the following control deficiencies:

1. Logical and Physical Account Management Activities Were Not Consistently Performed
2. Outsourcing the Information System Security Officer (ISSO) Role Created an Information Technology (IT) Governance Concern at Financial Management System (FMS)
3. Plan of Action and Milestones (POA&Ms) Were Not Updated Timely and Maintained at FMS and Office of the Comptroller of the Currency (OCC)
4. Security Incidents Were Not Reported Timely at Bureau of the Public Debt (BPD) and Alcohol and Tobacco Tax and Trade Bureau (TTB)
5. Reviews of Audit Logs Were Not Documented at Bureau of Engraving and Printing (BEP)
6. Electronic Media Destruction Process at Financial Crimes Enforcement Network (FinCEN) Was Not Fully Compliant with Its Internal Policies
7. Password Settings Were Not Properly Configured to Lockout for a BPD System

We have made 29 recommendations that, if addressed, will strengthen the bureaus, offices, and the Department's information security program.

1. Logical and Physical Account Management Activities Were Not Consistently Performed

We found access control review issues with certain bureaus and determined the need for additional attention department-wide. We identified control deficiencies in account management, specifically, the review of user access on an annual basis and the timely disabling of inactive user accounts. In addition, we noted deficiencies related to the review and configuration of physical access. When controls are ineffective, data and the operational status of the impacted systems could have an adverse impact on the mission, operations, and data of the bureau.

2. Outsourcing the Information System Security Officer (ISSO) Role Created an IT Governance Concern at FMS

FMS outsourced the ISSO position to a financial agent without first providing the ISSO the network connectivity to access Trusted Agent FISMA (TAF) and the bureau's Intranet site containing security policy and security templates. Without the network connectivity, the individual could not perform all the required ISSO duties outlined in their ISSO appointment letter. In addition, the transfer of the ISSO function from an FMS employee to an employee of the financial agent created an additional concern regarding the reporting relationship of the ISSO to his supervisor, the financial agent's operations manager. This reporting relationship may limit FMS's ability to receive objective, independent reporting and may prevent the ISSO from fulfilling his duties.

3. POA&Ms Were Not Updated Timely and Maintained at FMS and OCC

We noted FMS and OCC did not include all vulnerabilities or timely submit and effectively track items on their POA&Ms. Without a centralized list of all known security weaknesses, OCIO may not

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

be able to identify reoccurring security issues across multiple systems that could be remediated by a department-wide strategic corrective action plan.

4. Security Incidents Were Not Reported Timely at BPD and TTB

We noted an Incident Response and Reporting deficiency at BPD and TTB that did not timely report incidents to the TCSIRC. When security incidents are not reported timely, there is an increased risk that sensitive information, including personally identifiable information, could be divulged and a loss of public trust could occur.

5. Reviews of Audit Logs Were Not Documented at BEP

We noted a Continuous Monitoring deficiency at BEP because the bureau did not document reviews of audit logs. When this activity is performed, there is less risk that unauthorized activity and access can go undetected. At the close of our audit, we noted that the bureau was developing standard operating procedures to review audit logs on a routine basis.

6. Electronic Media Destruction Process at FinCEN Was Not Fully Compliant with Its Internal Policies

FinCEN was not fully compliant with its media sanitization process by leaving boxes containing old computer hard drives in an area outside the authorized custodian's cubicle within the secured facility and not maintaining an inventory of these devices to ensure they were destroyed.

7. Password Settings Were Not Properly Configured to Lockout for a BPD System

BPD had invalid password lockout configuration settings on a network device. Upon notification by KPMG auditors, the settings were immediately corrected.

Our performance audit of the Department's information security program identified 29 recommendations that the bureaus, offices, and the Department should address to strengthen their information security management programs. The *Findings* section of this report presents the detailed findings and associated recommendations. In addition, we evaluated all prior year findings from the FY 2009 FISMA Evaluation and determined that the bureaus implemented all recommendations, with the exception of Prior Year Finding #5 for POA&Ms, which was reissued as FY 2010 Finding #3. See Appendix I, *Status of Prior Year Findings,* for additional details.

FINDINGS

1. Logical and Physical Account Management Activities Were Not Consistently Performed

The audit identified an inconsistent implementation of account management and physical access security controls at six (6) bureaus including the BEP, DO, FinCEN, OCC, OIG, and the OTS. This finding indicated that the Treasury OCIO had not provided sufficient oversight to enforce and monitor compliance with Treasury and NIST identity and access management standards and guidelines. KPMG noted the following:

1. Account Management activities were not consistently performed as required by the TD P 85-01, *Treasury Information Technology Security Program*, and bureau-specific policies at five (5) bureaus
   - BEP did not document its review of user accounts for the selected system in accordance with their system security plan.
   - The DO system had user and administrator accounts that had been inactive for over ninety (90) days and had not been disabled. These accounts are created and maintained by the OCIO, who uses the system for performance of their Treasury-wide FISMA oversight role.
   - The OCC system did not have an automated control in place to automatically deactivate users' accounts after the bureau-defined period of inactivity.
   - The OIG systems had user and administrator accounts that had been inactive for over ninety (90) days and had not been disabled.
   - The periodic review of the OTS application users' access did not include reviewing users' privileges within the application in order to determine if they were appropriate based on users' roles at the OTS. The review of access only had accessed whether users were active employees at the organization.
2. Physical Access to restricted areas was not properly reviewed and administered as required by the TD P 85-01, *Treasury Information Technology Security Program*, and bureau-specific policies at two (2) bureaus
   - Physical access to the FinCEN data center was not reviewed annually and access approval forms were not maintained.
   - The OIG Local Area Network (LAN) room's access list was not reviewed annually and users, who no longer need access, were not removed in a timely manner.

The above control deficiencies shared a common cause that the respective bureau or office did not appropriately review user access and disable or delete unnecessary access. By not providing sufficient oversight to ensure that all bureaus have followed Treasury and NIST requirements for the design, implementation, and testing of security controls, the Treasury OCIO may not be able to fulfill its oversight responsibilities in accordance with TD P 85-01. This could lead to potential weaknesses of logical and physical access of information systems across the entire Department. By not implementing a periodic review of all user and administrator accounts' inactivity and disabling the accounts according to policy, there is an increased risk that users could gain or retain unauthorized access and/or perform unauthorized transactions within their respective systems. By not implementing the periodic review of all users' physical access to their bureaus' IT facilities, there is an increased risk that unauthorized users could obtain physical access to secure areas they were not authorized to access.

We recommend that OCIO management:

1. Provide sufficient oversight[5] by the Treasury OCIO Cyber Security Program over the NIST Special Publication 800-53 security controls around Account Management, Physical Access Authorization, and Physical Access Control to ensure that the bureaus implement these controls. This can be accomplished by reviewing the implementation of these controls during the next OCIO review at each bureau.
2. Ensure administrators for the reviewed DO system review user accounts and disable inactive accounts in accordance with TD P 85-01 (as a minimum) and any applicable bureau policy.
3. Review administrator accounts for inactivity on a quarterly basis and disable accounts per the TD P 85-01 for the reviewed DO system.
4. Train the reviewed DO system's administrators on how to review the accounts of the users assigned to their respective bureaus on a quarterly basis and disable the accounts that exceed ninety (90) days of inactivity.

We recommend that the BEP management:

5. Perform and document user access reviews for their system in accordance with their system security plan.

We recommend that FinCEN management:

6. Perform review and validation of physical access to restricted areas, annually.
7. Document and approve all employees' physical access requirements.
8. Document and approve the door "zone" configuration of the physical access control system.
9. Develop a documented procedure for the approval, administration, review, and validation of access to restricted areas.

We recommend that OCC management:

10. Develop and implement an automated means to disable inactive user accounts from the reviewed system after sixty (60) days for Federal employees and thirty (30) days for contractors.

We recommend that OIG management:

11. Ensure domain user accounts are reviewed for inactivity on an annual basis and domain administrator accounts are reviewed for inactivity on a semiannual basis, and any accounts that exceed ninety (90) days of inactivity are disabled.
12. Develop policies and procedures and document them in the system security plan for the annual review of OIG LAN room access.
13. Conduct a review of users' access to the OIG LAN room annually and remove access privileges for those individuals that do not need access.

[5] The OCIO does not provide oversight over the OIG or TIGTA to preserve the independence of the offices.

We recommend that OTS management:

14. Develop and implement a training program that outlines how the six-month user privileges review should be performed.

15. Develop and implement a mechanism to track completion of the six-month user privileges review.

2. Outsourcing the ISSO Role Created an IT Governance Concern at FMS

FMS transferred the ISSO role from a government employee to a bank employee for an outsourced information system in March 2010 by utilizing an existing financial agent agreement with a large national bank. The outsourcing of the ISSO role created two (2) IT governance concerns.

First, KPMG noted that the appointed ISSO, a bank employee, could not fully perform his assigned information security duties such as:

- Implementing changes to FMS IT security policies;
- Updating the POA&Ms for the outsourced information system; and
- Maintaining and uploading, when appropriate, the system security plan, the Contingency Plan, and Configuration Management Plan to the TAF tool.

The bank employee could not perform these duties, as the national bank and FMS had not established a network communication link or other remote access solution prior to outsourcing the ISSO role. Additionally, FMS had not included the bank employee on all FMS ISSO e-mail distribution lists to ensure the bank employee received timely notification of revisions and updates to FMS policy and procedures. As a result, the ISSO was uninformed of changes to FMS policies and FMS security templates such as the system security plan. FMS management reported that action was taken to remediate the control deficiency by including the bank employee on all ISSO e-mail distribution lists and requesting remote access to FMS's network for the bank employee.

Second, the transfer of the ISSO role from a FMS employee to a bank employee created additional concerns regarding IT governance. Specifically, the new ISSO, a bank employee, reported to the Operations Manager for the outsourced information system. The Operations Manager's primary responsibility is to ensure the availability of the information system and efficiency of operations. Private industry and government best practice suggest that the IT functions of computer operations should be separate from information security within IT departments to appropriately separate duties and balance the conflicting objectives of availability and operational efficiency (i.e. Operations) against the desire for greater control and limited access (i.e. Security). The reporting relationship of the ISSO to the Operations Manager may limit FMS's ability to receive objective, independent, and complete reporting of security matters and events.

In 2009, FMS changed its internal policies, permitting the ISSO position to be outsourced. Other factors contributed to the decision such as budgeted staff reductions and a belief that an ISSO role could be more effective when located at the bank's development center. Unfortunately, when the policy decision changed and FMS elected to outsource the ISSO role, FMS did not develop additional guidance for information system owners to mitigate potential conflicts and separation of duties concerns. Specific to the communication needs of an outsourced ISSO, FMS did not confirm that communication needs were satisfied prior to transferring the ISSO position to a bank employee.

We recommend that FMS Management:

16. Provide the ISSO with the network connectivity that will allow the bank employee access to FMS internal resources such as Treasury's FISMA collection and reporting tool, current FMS IT security policy and security templates, and ability to receive FMS email alerts regarding changes to FMS IT security policy and security templates.

17. Create FMS official guidance covering the appointment of the ISSO position at external providers. In such circumstances, FMS should confirm that communication requirements and needs are satisfied prior to outsourcing the ISSO position. Additionally, the guidance should address reporting relationships that might impact the ISSO's objectivity and clearly identify monitoring activities and assignment of responsibility to an FMS employee to mitigate potential conflicts.

18. Evaluate solutions to mitigate concerns over ISSO-management reporting relationships, which could include, for example, establishing or modifying internal controls, implementing monitoring tools, re-aligning the ISSO position under the bank's Information Security team or elsewhere within the bank, contracting for ISSO services through a different provider such as independent verification and validation contractor, or reassigning ISSO responsibilities back to an FMS employee.

3. POA&Ms Were Not Updated Timely and Maintained at FMS and OCC

OMB required that all federal agencies implement a POA&M process to identify tasks that are necessary to remediate identified security weaknesses. The POA&M should detail resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. The OCIO has established policies and procedures governing the development and maintenance of POA&Ms for Department information systems and has specified the TAF tool as the central repository for POA&Ms. In addition, the bureaus also developed policies and procedures to implement Departmental guidance. However, the management of POA&Ms at FMS and OCC were not conducted in accordance with the guidance provided. Specifically, KPMG noted the following:

- For two (2) of the three (3) FMS systems reviewed, previously identified security weaknesses and associated remediation plans were not added timely (i.e., within 30 days[6]) to the POA&Ms of record as required by OMB M-10-15, Treasury policy, and FMS policy.
- For one (1) OCC system, previously identified security weaknesses and associated remediation plans were not added timely to the POA&M as required by OMB M-10-15, Treasury policy, and bureau standards. Specifically, OCC did not update, submit, and include all necessary POA&M elements for an information system.

By not maintaining updated POA&Ms, including all identified security weakness and associated information in TAF, the OCIO's ability to monitor aggregated risks to its systems as well as prioritize limited IT resources to address known security weaknesses may be hindered. Additionally, without a centralized list of all known security weaknesses, OCIO may not be able to identify reoccurring security issues across multiple systems that could be remediated by a department-wide strategic corrective action plan. Further, by not consistently recording identified security weaknesses in TAF, the summary-level security metrics reported to OMB will under-report the true number of known security weaknesses associated with the Department's information systems.

[6] FMS policy requires that POA&M items are entered within 30 days for information systems with a FIPS 199 High impact classification.

We recommend that FMS management:

19. Direct ISSOs to develop and record POA&M items in TAF within the designated time period when security vulnerabilities are identified.
20. Provide additional oversight across all FMS systems to ensure that the POA&M process is managed in accordance with FMS, Treasury, and OMB policy and guidance.

We recommend that OCC management:

21. Populate the information system's POA&M to include vulnerabilities found in all applicable IT security reviews and audits, including vulnerabilities identified from annual assessments, audit reports, Treasury ACIOCS reviews, or internal bureau evaluations.
22. Populate the information system's POA&M with the information required by Treasury and OCC.
23. Develop and implement a training program for all individuals tasked with implementing the OCC POA&M process.

4. Security Incidents Were Not Reported Timely at BPD and TTB

BPD and TTB did not consistently report security incidents in a timely manner in accordance with NIST Special Publication 800-53, OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, and Treasury and bureau policy.

- Of thirteen (13) incidents documented by BPD during the reporting period, KPMG determined that four (4) of the incidents were not reported to TCSIRC within the required time period.
- Of fifteen (15) incidents documented by TTB during the reporting period, KPMG determined that two (2) of the incidents were not reported to TCSIRC within the required time period.

By not reporting incidents or potential incidents to TCSIRC in a timely manner, there is a risk that the incident will not be responded to properly. This may result in an increased risk that sensitive information, including personally identifiable information, could be divulged and a loss of public trust could occur.

We recommend that BPD management:

24. Ensure that all potential and actual security incidents are reported to TCSIRC within the required time period.

We recommend that TTB management:

25. Ensure that all potential and actual security incidents are reported to TCSIRC within the required time period.

5. Reviews of Audit Logs Were Not Documented at BEP

BEP did not document reviews of audit logs for the system we reviewed in accordance with NIST Special Publication 800-53 and Treasury policy. The lack of monitoring and regular review of audit logs can increase the risk that unauthorized access to the information system may go undetected.

We recommend that BEP management:

26. Develop and implement a process to review audit log information on a monthly basis for the information system that includes a requirement to document the reviews performed.

6. Electronic Media Destruction Process at FinCEN Was Not Fully Compliant with Its Internal Policies

In order to prevent unauthorized access to Treasury information, electronic media that is no longer in use must be securely stored and appropriately tracked until destroyed. FinCEN did not adequately follow their information systems security program for media sanitization, which requires media to be physically secured when both stored and transported, and that appropriate audit trail records be maintained. KPMG observed nine (9) cardboard boxes containing over 300 hard drives that were stored in an area outside the authorized custodian's cubicle within the FinCEN secured facility. Lists containing the serial numbers of the hardware in the boxes, which would allow for tracking, were not included with the hardware. In addition, serial numbers of hardware and electronic recording media, that were destroyed, were not reconciled against the inventory lists to verify that all equipment and media were appropriately destroyed. By not securing the electronic media in a manner that restricts access to only the authorized custodian, and then not reconciling the serial numbers of destroyed electronic media against the known inventory listing, it is impossible to determine if all electronic media, initially identified as requiring destruction, were actually destroyed.

We recommend that FinCEN management:

27. Secure and restrict access to media scheduled to be destroyed in accordance with their media sanitization policies.
28. Maintain a list identifying the device, serial number, and physical location of media that is scheduled to be destroyed.
29. Reconcile the destroyed hardware and electronic recording media with the list of items to be destroyed.

7. Password Settings Were Not Properly Configured to Lockout for a BPD System

Administrative accounts on a BPD information system were not locked after a defined number of invalid login attempts in accordance with NIST Special Publication 800-53 and system documentation. The system KPMG tested contained a technical error that did not enforce account lockouts after the defined number of invalid login attempts. After this control deficiency was identified, BPD management updated the system configuration settings to ensure that accounts and passwords were locked appropriately. By not enforcing effective lockout controls over administrative accounts to the information system, the potential for a malicious party to compromise user account passwords increased.

Since BPD management updated the system configurations to remediate this finding, no recommendations were necessary.

MANAGEMENT RESPONSE TO DRAFT REPORT

The following is the OCIO's response, dated October 29, 2010, to the draft FY 2010 FISMA Performance Audit Report.

October 29, 2010

MEMORANDUM FOR MARLA A. FREEDMAN
ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: Diane C. Litman /s/
Acting Deputy Assistant Secretary for Information Systems and Chief Information Officer

SUBJECT: Management Response to Draft Audit Report - FY 2010 Audit of Treasury's FISMA Implementation for Its Unclassified Systems

Thank you for the opportunity to comment on the draft audit report entitled, "FY 2010 Audit of Treasury's Federal Information Security Management Act (FISMA) Implementation for Its Unclassified Systems." The audit focuses on the adequacy of the Department's information security program and practices for its unclassified systems. We appreciate your acknowledgement that our security program is in place and is generally consistent with FISMA. We have carefully reviewed the draft and are in agreement with all findings and recommendations. Please refer to the attachment for further details on our planned corrective actions.

The Department is committed to continual improvement of its security program and meeting requirements of FISMA. We have made notable progress over the past year. For example, we closed all but one recommendation from last year's FISMA audit. Additionally, we have focused on the new White House security priorities, including automated reporting, as well as creative use of social media and cloud technologies. Our cloud-hosted security dashboard has improved the efficiency and reduced data collection costs while enabling the Department to monitor security performance at anytime from anywhere. Refining and collecting our measures in a collaborative, modern environment enabled steady security improvement and our ability to make risk-based decisions based upon real-time, accurate information.

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

Attachment

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

Management Response to OIG Recommendations

Note: The Department agrees with all findings and recommendations.

(U) OIG Finding 1: Logical and Physical Account Management Activities Were Not Consistently Performed

(U) OIG Recommendation 1: For Office of the Chief Information Officer (OCIO), we recommend that management: Provide sufficient oversight[7] by the Treasury OCIO Cyber Security Program over the National Institute of Standards and Technology (NIST) Special Publication 800-53 security controls around Account Management, Physical Access Authorization, and Physical Access Control to ensure that the bureaus implement these controls. This can be accomplished by reviewing the implementation of these controls during the next OCIO review at each bureau.

> **(U) Treasury Response: Treasury agrees with this recommendation**. Treasury OCIO will enhance its Cyber Security Program by placing additional emphasis on the oversight of NIST Special Publication 800-53 security controls families pertaining to access and physical controls. Target completion date is June 30, 2011.
>
> **(U) Responsible Official:** Edward Roback, Associate Chief Information Officer for Cyber Security (ACIO CS) and Chief Information Security Officer (CISO), Treasury

(U) OIG Recommendation 2: For OCIO, we recommend that management: Ensure administrators for the reviewed (Departmental Offices) DO system review user accounts and disable inactive accounts in accordance with (Treasury Directive Publication) TD P 85-01 (as a minimum) and any applicable bureau policy.

> **(U) Treasury Response: Treasury agrees with this recommendation.** Treasury OCIO will develop processes and procedures to ensure that administrators of the reviewed DO system review user accounts and disable inactive accounts in accordance with both Treasury and applicable bureau policies. Target completion date is June 30, 2011.
>
> **(U) Responsible Official:** Edward Roback, ACIO CS and CISO, Treasury

(U) OIG Recommendation 3: For OCIO, we recommend that management: Review administrator accounts for inactivity on a quarterly basis and disable accounts per the TD P 85-01 for the reviewed DO system.

> **(U) Treasury Response: Treasury agrees with this recommendation.** Treasury OCIO will ensure that administrator accounts are reviewed for inactivity

[7] The OCIO does not provide oversight over the OIG or TIGTA to preserve the independence of the offices.

on a quarterly basis and disable accounts per the TD P 85-01 for the reviewed DO system. Target completion date is December 30, 2010.

(U) Responsible Official: Edward Roback, ACIO CS and CISO, Treasury

(U) OIG Recommendation 4: For OCIO, we recommend that management: Train the reviewed DO system's administrators on how to review the accounts of the users assigned to their respective bureaus on a quarterly basis and disable the accounts that exceed ninety (90) days of inactivity.

(U) Treasury Response: Treasury agrees with this recommendation. Treasury OCIO will ensure that administrators of the reviewed DO system are trained on bureau level user account management to ensure compliance with Treasury's account inactivity policy. Target completion date is June 30, 2011.

(U) Responsible Official: Edward Roback, ACIO CS and CISO, Treasury

(U) OIG Recommendation 5: For (Bureau of Engraving and Printing) BEP, we recommend that management: Perform and document user access reviews for their system in accordance with their system security plan.

(U) Treasury Response: Treasury agrees with this recommendation. BEP will establish a repository to archive user access reviews within 30 days. Target completion date is November 30, 2010.

(U) Responsible Official: Harinder Singh, CISO, BEP

(U) OIG Recommendation 6: For (Financial Crime Enforcement Network) FinCEN, we recommend that management: Perform review and validation of physical access to restricted areas, annually.

(U) Treasury Response: Treasury agrees with this recommendation. The FinCEN will ensure that access to restricted physical access areas are reviewed and validated annually; all employees' physical access requirements are documented and approved to the restricted areas; document and approve the zone configurations of the restricted areas; and develop a documented procedure for approval, administration, and revalidation of access to restricted areas. Target completion date is January 31, 2011.

(U) Responsible Official: Gregory Sohn, CISO, FinCEN

(U) OIG Recommendation 7: For FinCEN, we recommend that management: Document and approve all employees' physical access requirements.

(U) Treasury Response: Treasury agrees with this recommendation. The FinCEN will ensure that access to restricted physical access areas are reviewed

and validated annually; all employees' physical access requirements are documented and approved to the restricted areas; document and approve the zone configurations of the restricted areas; and develop a documented procedure for approval, administration, and revalidation of access to restricted areas. Target completion date is January 31, 2011.

(U) Responsible Official: Gregory Sohn, CISO, FinCEN

(U) OIG Recommendation 8: For FinCEN, we recommend that management: Document and approve the door "zone" configuration of the physical access control system.

(U) Treasury Response: Treasury agrees with this recommendation. The FinCEN will ensure that access to restricted physical access areas are reviewed and validated annually; all employees' physical access requirements are documented and approved to the restricted areas; document and approve the zone configurations of the restricted areas; and develop a documented procedure for approval, administration, and revalidation of access to restricted areas. Target completion date is January 31, 2011.

(U) Responsible Official: Gregory Sohn, CISO, FinCEN

(U) OIG Recommendation 9: For FinCEN, we recommend that management: Develop a documented procedure for the approval, administration, and review and validation of access to restricted areas.

(U) Treasury Response: Treasury agrees with this recommendation. The FinCEN will ensure that access to restricted physical access areas are reviewed and validated annually; all employees' physical access requirements are documented and approved to the restricted areas; document and approve the zone configurations of the restricted areas; and develop a documented procedure for approval, administration, and revalidation of access to restricted areas. Target completion date is January 31, 2011.

(U) Responsible Official: Gregory Sohn, CISO, FinCEN

(U) OIG Recommendation 10: For (Office of the Comptroller of the Currency) OCC, we recommend that management: Develop and implement an automated means to disable inactive user accounts from the reviewed system after sixty (60) days for Federal employees and thirty (30) days for contractors.

(U) Treasury Response: Treasury agrees with this recommendation. Recognizing room for improvement in the account management controls currently in place, the OCC has enlisted contractor support in evaluating the current account management program. This effort includes developing requirements and working with stakeholders to determine the viability of implementing an

automated tool that integrates with Microsoft Active Directory. This remediation is ongoing, with a planned remediation date of June 30, 2011.

(U) Responsible Official: Roger Mahach, CISO and Chief Privacy Officer (CPO), OCC

(U) OIG Recommendation 11: For OIG, we recommend that management: Ensure domain user accounts are reviewed for inactivity on an annual basis and domain administrator accounts are reviewed for inactivity on a semiannual basis, and any accounts that exceed ninety (90) days of inactivity are disabled.

(U) OIG Response: Treasury agrees with this recommendation. OIG Planned Corrective Action: Disable unused accounts after 90 days. Target completion date is September 23, 2010.

(U) Responsible Official: Dee Thompson, Director of Information Technology, OIG

(U) OIG Recommendation 12: For OIG, we recommend that management: Develop policies and procedures and document them in the system security plan for the annual review of OIG LAN room access.

(U) OIG Response: Treasury agrees with this recommendation. OIG Planned Corrective Action: Review LAN room's access list annually and remove users who no longer need access. Target completion date is December 31, 2010.

(U) Responsible Official: Dee Thompson, Director of Information Technologies, OIG

(U) OIG Recommendation 13: For OIG, we recommend that management: Conduct a review of users' access to the OIG LAN room annually and remove access privileges for those individuals that do not need access.

(U) OIG Response: Treasury agrees with this recommendation. OIG Planned Corrective Action: Update Operational, Technical, and Management Controls in the OIG system security plan. Target completion date is December 31, 2010

(U) Responsible Official: Dee Thompson, Director of Information Technologies, OIG

(U) OIG Recommendation 14: For (Office of Thrift Supervision) OTS, we recommend that management: Develop and implement a training program that outlines how the six-month user privileges review should be performed.

(U) Treasury Response: Treasury agrees with this recommendation. OTS will ensure that a training program is developed and implemented that outlines

how six-month user privileges reviews should be performed. OTS has already conducted a briefing for responsible officials detailing the additional measures that must be taken during the account review and the frequency of which these reviews must occur. Target completion date is June 30, 2011.

(U) Responsible Official: Andrew Krug, CISO, OTS

(U) OIG Recommendation 15: For OTS, we recommend that management: Develop and implement a mechanism to track completion of the six-month user privileges review.

(U) Treasury Response: Treasury agrees with this recommendation. OTS will ensure that mechanisms are developed and implemented which track the completion of the six-month user privileges review process. OTS is in the process of amending its Enterprise Continuous Monitoring process to include account reviews/audits of application user bases consistent with internal policies. Target completion date is January 30, 2011.

(U) Responsible Official: Andrew Krug, CISO, OTS

(U) OIG Finding 2: Outsourcing the ISSO Role Created an IT Governance Concern at FMS

(U) OIG Recommendation 16: For (Financial Management Service) FMS, we recommend that management: Provide the (Information System Security Officer) ISSO with the network connectivity that will allow the bank employee access to FMS internal resources such as Treasury's FISMA collection and reporting tool, current FMS (Information Technology) IT security policy and security templates, and ability to receive FMS email alerts regarding changes to FMS IT security policy and security templates.

(U) Treasury Response: Treasury agrees with this recommendation.
1) FMS will provide the network connectivity that will allow access to FMS internal resources such as Trusted Agent FISMA (TAF), IT security policy updates, and updates to IT security templates by June 30, 2011; 2) FMS will review the ISSO duties to determine any gaps in capabilities by February 11, 2011; and 3) FMS will take appropriate actions against identified gaps by June 30, 2011. Target completion date is June 30, 2011.

(U) Responsible Official: David Ambrose, CISO, Director, Security & Audit Directorate, FMS

(U) OIG Recommendation 17: For FMS, we recommend that management: Create FMS official guidance covering the appointment of the ISSO position at external providers. In such circumstances, FMS should confirm that communication requirements and needs are satisfied prior to outsourcing the ISSO position. Additionally, the guidance should address reporting relationships that might impact the ISSO's objectivity and clearly

identify monitoring activities and assignment of responsibility to an FMS employee to mitigate potential conflicts.

> **(U) Treasury Response: Treasury agrees with this recommendation.** FMS Mission Assurance will develop and issue guidance concerning the appointment of the ISSO position at external providers. Target completion date is June 30, 2011.
>
> **(U) Responsible Official:** David Ambrose, CISO, Director, Security & Audit Directorate, FMS

(U) OIG Recommendation 18: For FMS, we recommend that management: Evaluate solutions to mitigate concerns over ISSO-management reporting relationships, which could include, for example, establishing or modifying internal controls, implementing monitoring tools, re-aligning the ISSO position under the bank's Information Security team or elsewhere within the bank, contracting for ISSO services through a different provider such as an Independent Verification and Validation contractors, or reassigning ISSO responsibilities back to an FMS employee.

> **(U) Treasury Response: Treasury agrees with this recommendation.** The Authorizing Official and System Owner will review the ISSO reporting relationship and determine what if any changes need to be made. Target completion date is June 30, 2011.
>
> **(U) Responsible Official:** David Ambrose, CISO, Director, Security & Audit Directorate, FMS

(U) OIG Finding 3: POA&Ms Were Not Updated Timely and Maintained at FMS and OCC

(U) OIG Recommendation 19: For FMS, we recommend that management: Direct ISSOs to develop and record POA&M items in TAF within the designated time period when security vulnerabilities are identified.

> **(U) Treasury Response: Treasury agrees with this recommendation.** The FMS CISO will issue a memo to all ISSO's directing them to develop and record POA&M items in TAF within the designated time-period according to FMS policy when security vulnerabilities are identified. Target completion date is June 30, 2011.
>
> **(U) Responsible Official:** David Ambrose, CISO, Director, Security & Audit Directorate, FMS

(U) OIG Recommendation 20: For FMS, we recommend that management: Provide additional oversight across all FMS systems to ensure that the POA&M process is managed in accordance with FMS, Treasury, and OMB policy and guidance.

(U) Treasury Response: Treasury agrees with this recommendation. FMS Mission Assurance will implement a tracking mechanism for all security reviews and inform ISSOs of the date those reviews must be in TAF. Target completion date is June 30, 2011.

(U) Responsible Official: David Ambrose, CISO, Director, Security & Audit Directorate, FMS

(U) OIG Recommendation 21: For OCC, we recommend that management: Populate the information system's POA&M to include vulnerabilities found in all applicable IT security reviews and audits, including vulnerabilities identified from annual assessments, audit reports, Treasury ACIOCS reviews, or internal bureau evaluations.

(U) Treasury Response: Treasury agrees with this recommendation. To address a gap in the management of remediation activities, and the allocation of resources associated with the remediation of vulnerabilities across systems, the OCC Information Risk Management (IRM) office has begun to implement a program to issue a Notice of Potential Finding and Recommendation (NPFR). Utilizing the NPFR as a vehicle by which IRM is able to elevate findings to senior management and communicate ownership to stakeholders, IRM aims to receive increased commitment to the Plan of Action and Milestones process from vulnerability owners. This remediation is ongoing, with a planned completion date of June 30, 2011.

(U) Responsible Official: Roger Mahach, CISO and CPO, OCC

(U) OIG Recommendation 22: For OCC, we recommend that management: Populate the information system's POA&M with the information required by Treasury and OCC.

(U) Treasury Response: Treasury agrees with this recommendation. To address a gap in the management of remediation activities, and the allocation of resources associated with the remediation of vulnerabilities across systems, the OCC Information Risk Management (IRM) office has begun to implement a program to issue a Notice of Potential Finding and Recommendation (NPFR). Utilizing the NPFR as a vehicle by which IRM is able to elevate findings to senior management and communicate ownership to stakeholders, IRM aims to receive increased commitment to the Plan of Action and Milestones process from vulnerability owners. This remediation is ongoing, with a planned completion date of June 30, 2011.

(U) Responsible Official: Roger Mahach, CISO and CPO, OCC

(U) OIG Recommendation 23: For OCC, we recommend that management: Develop and implement a training program for all individuals tasked with implementing the OCC POA&M process.

(U) Treasury Response: Treasury agrees with this recommendation. To address a gap in the management of remediation activities, and the allocation of resources associated with the remediation of vulnerabilities across systems, the OCC Information Risk Management (IRM) office has begun to implement a program to issue a Notice of Potential Finding and Recommendation (NPFR). Utilizing the NPFR as a vehicle by which IRM is able to elevate findings to senior management and communicate ownership to stakeholders, IRM aims to receive increased commitment to the Plan of Action and Milestones process from vulnerability owners. This remediation is ongoing, with a planned completion date of June 30, 2011.

(U) Responsible Official: Roger Mahach, CISO and CPO, OCC

(U) OIG Finding 4: Security Incidents Were Not Reported Timely at BPD and TTB

(U) OIG Recommendation 24: For (Bureau of the Public Debt) BPD, we recommend that management: Ensure that all potential and actual security incidents are reported to (Treasury Computer Security Incident Response Center) TCSIRC within the required time period.

(U) Treasury Response: Treasury agrees with this recommendation. The BPD will review and revise incident response procedures to ensure that incidents are reported to TCSIRC in accordance with Treasury defined time requirements. Target completion date is February 2, 2011**.**

(U) Responsible Official: Jim McLaughlin, CISO and Privacy Act Officer (PAO), BPD

(U) OIG Recommendation 25: For (The Alcohol and Tobacco Tax and Trade Bureau) TTB, we recommend that management: Ensure that all potential and actual security incidents are reported to TCSIRC within the required time period.

(U) Treasury Response: Treasury agrees with this recommendation. The current TTB incident response procedures ensure that incidents are reported to TCSIRC in accordance with Treasury defined time requirements. Additionally, all Incident Response personnel are trained in the new procedure to ensure that all security incidents are reported to TCSIRC within the required time period. The completion date was June 30, 2010. **Status:** Closed

(U) Responsible Official: Jackie Washington, ACIO - IT Security, TTB

(U) OIG Finding 5: Reviews of Audit Logs Were Not Documented at BEP

(U) OIG Recommendation 26: For BEP, we recommend that management: Develop and implement a process to review audit log information on a monthly basis for the information system that includes a requirement to document the reviews performed.

> **(U) Treasury Response: Treasury agrees with this recommendation.** BEP will establish a repository to archive audit log reviews within 30 days. Target completion date is November 30, 2010.
>
> **(U) Responsible Official:** Harinder Singh, CISO, BEP

(U) OIG Finding 6: Electronic Media Destruction Process at FinCEN Was Not Fully Compliant with Its Internal Policies

(U) OIG Recommendation 27: For FinCEN, we recommend that management: Secure and restrict access to media scheduled to be destroyed in accordance with their media sanitization policies.

> **(U) Treasury Response: Treasury agrees with this recommendation.** The FinCEN CIO will ensure that media scheduled to be destroyed is properly secured and access restricted; a media destruction list is maintained that identifies the device, serial number, and physical location of the media to be destroyed; and will reconcile the destroyed hardware and media against the list of items to be destroyed. Target completion date is January 31, 2011.
>
> **(U) Responsible Official:** Gregory Sohn, CISO, FinCEN

(U) OIG Recommendation 28: For FinCEN, we recommend that management: Maintain a list identifying the device, serial number, and physical location of media that is scheduled to be destroyed.

> **(U) Treasury Response: Treasury agrees with this recommendation.** The FinCEN CIO will ensure that media scheduled to be destroyed is properly secured and access restricted; a media destruction list is maintained that identifies the device, serial number, and physical location of the media to be destroyed; and will reconcile the destroyed hardware and media against the list of items to be destroyed. Target completion date is January 31, 2011.
>
> **(U) Responsible Official:** Gregory Sohn, CISO, FinCEN

(U) OIG Recommendation 29: For FinCEN, we recommend that management: Reconcile the destroyed hardware and electronic recording media with the list of items to be destroyed.

(U) Treasury Response: Treasury agrees with this recommendation. The FinCEN CIO will ensure that media scheduled to be destroyed is properly secured and access restricted; a media destruction list is maintained that identifies the device, serial number, and physical location of the media to be destroyed; and will reconcile the destroyed hardware and media against the list of items to be destroyed. Target completion date is January 31, 2011.

(U) Responsible Official: Gregory Sohn, CISO, FinCEN

(U) OIG Finding 7: Password Settings Were Not Properly Configured to Lockout for a BPD System

(U) OIG Recommendation: For BPD: Since BPD management updated the system configurations to remediate this finding, no recommendations were necessary.

(U) Treasury Response: This finding has been remediated by BPD management. **Status:** Closed

(U) Responsible Official: Jim McLaughlin, CISO and PAO, BPD

APPENDIX I – STATUS OF PRIOR YEAR FINDINGS

Finding #	Prior Year Condition	Recommendation(s)/ Prior Year Management Response	Status
Finding #1 – Financial Management Service (FMS) NIST Federal Information Processing Standard (FIPS) 200 Minimum Security Control Baselines Were Not Sufficiently Tested or Implemented.	During Fiscal Year (FY) 2009, FMS issued a full Authority to Operate (ATO) for two (2) systems reviewed. However, a full risk assessment was not performed, and the security test and evaluation only included an assessment of the technical security control families of the National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems.*	We recommend that FMS management: 1. Complete the full certification and accreditation of the first FMS system identified above by the estimated completion date tracked in the Plan of Actions & Milestones (POA&M). 2. Finalize the security assessment reporting process and reissue the full ATO for the second FMS system identified above.	**Implemented/Closed** Both systems were certified and accredited in accordance with the NIST Special Publication 800-37.
Finding #1 – Office of Thrift Supervision (OTS) NIST FIPS 200 Minimum Security Control Baselines Were Not Sufficiently Tested or Implemented (Repeated)	As of June 30, 2009, the two (2) systems were not fully accredited systems.	We recommend that OTS management continue with plans to resolve the security weakness identified during the certification and accreditation process for all OTS systems by the end of the interim authorization period, September 25, 2009 and continue with plans to grant a full authority to operate during the FY 2010 Federal Information Security Management Act (FISMA) reporting period.	**Implemented/Closed** Both systems were certified and accredited in accordance with the NIST Special Publication 800-37.
Finding #2 Policies Required by Office of Management and Budget (OMB) Memorandum 07-16 have not been Finalized and Issued (Repeat Finding)	At the conclusion of the FY 2008 FISMA audit, two (2) Treasury Directives and Publications related to the collection, use, sharing, disclosure, transfer, and storage of personally identifiable information (PII) were not finalized. During the 2009 FISMA reporting cycle, the Office of Privacy and Treasury Records (OPTR) finalized Treasury Directive Publication (TD P) 25-07, *Privacy Impact Assessment Manual*; however, at the conclusion of the FY 2009 FISMA Evaluation, Treasury Directive (TD) 25-08, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, was still in draft.	We recommend that OPTR management finalize all of the directives and policies related to the collection, use, sharing, disclosure, transfer, and storage of PII identified above. (Repeat Recommendation)	**Implemented/Closed** OPTR provided the signed TD 25-08, dated December 22, 2009.

Finding #	Prior Year Condition	Recommendation(s)/ Prior Year Management Response	Status
Finding #3 The Departmental Offices (DO) Federal Desktop Core Configuration (FDCC) Image is Not Fully Implemented (Repeat Findings)	At the conclusion of the FY 2008 FISMA audit, the DO had not implemented the FDCC secure configuration baseline on all headquarters workstations. As of the conclusion of the FY 2009 FISMA evaluation, we again noted that DO still had not implemented the FDCC secure configuration baseline on all workstations.	We recommend that DO information technology (IT) management fully implement the FDCC secure baseline configurations on all headquarters end-user workstations by the November 15, 2009 due date outlined in the POA&M weakness.	**Implemented/Closed** All FDCC security configurations were applied to all headquarters end-user workstations.
Finding #4 The Bureau of Public Debt (BPD) is Not Using a Security Content Automation Protocol (SCAP)	At the close of the 2009 FISMA reporting cycle, BPD was not using a SCAP validated tool to scan the BPD FDCC secure configuration baseline.	We recommend that BPD management: 1. Continue with efforts to implement a SCAP-validated tool. 2. Utilize a SCAP-validated tool to monitor the BPD FDCC secure configuration baseline image.	**Implemented/Closed** FDCC baseline settings indicated a SCAP-validated tool was in use.
Finding #5 FMS POA&M Estimate to Completion Dates Were Not Consistently Updated in Accordance with FMS Policy.	FMS was not consistently managing POA&M's Estimate to Complete dates and Milestones for two (2) of the five (5) systems selected in our representative subset of FMS major applications and general support systems.	We recommend that FMS management: 1. Update the estimate to complete dates and milestones for each of the identified weaknesses to reflect current status. 2. Provide additional oversight across all FMS systems to ensure that the POA&M process is managed in accordance with FMS, Treasury, and OMB policy and guidance.	**Partially Implemented/Open** Both systems' POA&Ms were completed or updated to accurately reflect "Estimate to Completion" and "Milestone" dates. However, we identified additional POA&M weakness at FMS. See FY 2010 Finding #3.

Finding #	Prior Year Condition	Recommendation(s)/ Prior Year Management Response	Status
Finding #6 Frequency of Vulnerability Assessment Scanning at BPD Was Not in Line with Bureau and Treasury Policy	The frequency of vulnerability scanning over one (1) of BPD's systems was not in line with Treasury-wide policy and the control requirements outlined in the system's security plan. Currently, the system was being scanned annually, while the minimum required frequency of vulnerability scanning specified by Treasury policy and the control requirements outlined in the system's security plan is at least quarterly.	We recommend that BPD Office of the Information Technology (OIT) management: 1. Continue follow-up efforts to resolve or dispose of all potential vulnerabilities identified during the recent vulnerability assessment. 2. Review and update internal BPD bureau-wide IT policies as appropriate. 3. Conduct vulnerability scans on at least a quarterly basis as required by TD P 85-01	**Implemented/Closed** BPD closed one of the vulnerabilities identified in FY 2009 and the other vulnerability has a corrective action plan in place. In addition, BPD developed a bureau-wide IT policy, which addresses vulnerability scanning. Lastly, vulnerability scans were performed on a monthly basis starting March 2010.
Finding #7 E-Authentication Risk Assessment Was Not Performed at the Financial Crimes Enforcement Network (FinCEN)	FinCEN had not performed an E-Authentication Risk Assessment for the one (1) reviewed system selected.	We recommend that FinCEN management perform an E-Authentication Risk Assessment for the one (1) system selected at FinCEN for the FY 2009 FISMA Evaluation.	**Implemented/Closed** The E-Authentication Risk Assessment was conducted for the system.

APPENDIX II – THE DEPARTMENT OF THE TREASURY'S CONSOLIDATED RESPONSE TO OMB'S FISMA 2010 QUESTIONS FOR INSPECTORS GENERAL

The information included in Appendix II represents the Department of the Treasury's consolidated responses to OMB's FISMA 2010 questions for Inspectors Generals. KPMG prepared responses to OMB questions based on an assessment of 15 information systems across 13 Treasury components, excluding the IRS and TIGTA. A decision was made to inspect only one (1) OIG system every year. TIGTA performed audit procedures over the IRS and its information systems and provided their answers to the Treasury OIG and KPMG for consolidation. The information provided by TIGTA has not been subjected to KPMG audit procedures and, accordingly, we express no opinion on it.

S1: Certification and Accreditation

Status of Certification and Accreditation Program [check one]	✓	a. The Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures describing the roles and responsibilities of participants in the certification and accreditation process. 2. Establishment of accreditation boundaries for agency information systems. 3. Categorizes information systems. 4. Applies applicable minimum baseline security controls. 5. Assesses risks and tailors security control baseline for each system. 6. Assessment of the management, operational, and technical security controls in the information system. 7. Risks to Agency operations, assets, or individuals analyzed and documented in the system security plan, risk assessment, or an equivalent document. 8. The accreditation official is provided (i) the security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective actions; (ii) the plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and (iii) the updated system security plan with the latest copy of the risk assessment.
		b. The Agency has established and is maintaining a certification and accreditation program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a certification and accreditation program.
1a. If b. checked above, check areas that need significant improvement:		1a(1) Certification and accreditation policy is not fully developed.
		1a(2) Certification and accreditation procedures are not fully developed, sufficiently detailed or consistently implemented.
		1a(3) Information systems are not properly categorized (FIPS 199/SP 800-60).
		1a(4) Accreditation boundaries for agency information systems are not adequately defined.

		1a(5) Minimum baseline security controls are not adequately applied to information systems (FIPS 200/SP 800-53).
		1a(6) Risk assessments are not adequately conducted (SP 800-30).
		1a(7) Security control baselines are not adequately tailored to individual information systems (SP 800-30).
		1a(8) Security plans do not adequately identify security requirements (SP 800-18).
		1a(9) Inadequate process to assess security control effectiveness (SP 800-53A).
		1a(10) Inadequate process to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate (SP 800-37).
		1a(11) Inadequate process to continuously track changes to information systems that may necessitate reassessment of control effectiveness (SP 800-37).
		1a(12) Other
		Explanation for Other:
Comments:		

S2: Configuration Management

Status of Security Configuration Management Program [check one]		a. The Agency has established and is maintaining a security configuration management program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for configuration management. 2. Standard baseline configurations. 3. Scanning for compliance and vulnerabilities with baseline configurations. 4. FDCC baseline settings fully implemented and/or any deviations from FDCC baseline settings fully documented. 5. Documented proposed or actual changes to the configuration settings. 6. Process for the timely and secure installation of software patches.
	✓	b. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a security configuration management program.
2a. If b. checked above, check areas that need significant improvement:		2a(1) Configuration management policy is not fully developed.
	✓	2a(2) Configuration management procedures are not fully developed or consistently implemented.
		2a(3) Software inventory is not complete (NIST 800-53: CM-8).
		2a(4) Standard baseline configurations are not identified for all software components (NIST 800-53: CM-8).
		2a(5) Hardware inventory is not complete (NIST 800-53 CM-8).
		2a(6) Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).
		2a(7) Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).
		2a(8) FDCC is not fully implemented (OMB) and/or all deviations are not fully documented.

		2a(9) Software scanning capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).
	✓	2a(10) Configuration-related vulnerabilities have not been remediated in a timely manner (NIST 800-53: CM-4, CM-6, RA-5, SI-2).
	✓	2a(11) Patch management process is not fully developed (NIST 800-53: CM-3, SI-2).
		2a(12) Other
		Explanation for Other:
Comments: **TIGTA:** The IRS has not completed corrective actions to resolve the software configuration management component of the IRS computer security material weakness. Until the IRS has implemented adequate configuration management controls Agencywide, it cannot ensure the security and integrity of system programs, files, and data. In March 2010, TIGTA reported that the IRS was not timely addressing high- and medium-risk system vulnerabilities that it identified on Automated Collection System servers. In addition, during the 2010 FISMA evaluation period, the TIGTA concluded fieldwork on an audit to evaluate IRS email servers and found that the IRS is not taking timely actions to correct medium-risk security vulnerabilities identified through monthly scans on its email servers. The IRS computer security material weakness relating to configuration management includes unresolved weaknesses in the IRS patch management process. The IRS's corrective action plan for resolving the patch management weaknesses indicates that corrective actions are still ongoing.		
2b. Identify baselines reviewed:		
2b(1) Software Name	None	
2b(2) Software Version	None	

S3: Incident Response and Reporting

Status of Incident Response & Reporting Program [check one]	✓	a. The Agency has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for responding and reporting to incidents. 2. Comprehensive analysis, validation, and documentation of incidents. 3. When applicable, reports to US-CERT within established timeframes. 4. When applicable, reports to law enforcement within established timeframes. 5. Responds to and resolves incidents in a timely manner to minimize further damage.
		b. The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established an incident response and reporting program.
3a. If b. checked above, check areas that need significant improvement:		3a(1) Incident response and reporting policy is not fully developed.
		3a(2) Incident response and reporting procedures are not fully developed, sufficiently detailed or consistently implemented.
		3a(3) Incidents were not identified in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
		3a(4) Incidents were not reported to US-CERT as required (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).

		3a(5) Incidents were not reported to law enforcement as required.
		3a(6) Incidents were not resolved in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
		3a(7) Incidents were not resolved to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
		3a(8) There is insufficient incident monitoring and detection coverage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
		3a(9) Other
		Explanation for Other:
Comments: **Treasury OIG:** BPD did not report 4 of 13 incidents in the required timeframe. TTB did not report 2 of 14 in the required timeframe.		

S4: Security Training

Status of Security Training Program [check one]		a. The Agency has established and is maintaining a security training program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for security awareness training. 2. Documented policies and procedures for specialized training for users with significant information security responsibilities. 3. Appropriate training content based on the organization and roles. 4. Identification and tracking of all employees with login privileges that need security awareness training. 5. Identification and tracking of employees without login privileges that require security awareness training. 6. Identification and tracking of all employees with significant information security responsibilities that require specialized training.
	✓	b. The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a security training program.
4a. If b. checked above, check areas that need significant improvement:		4a(1) Security awareness training policy is not fully developed.
		4a(2) Security awareness training procedures are not fully developed, sufficiently detailed or consistently implemented.
		4a(3) Specialized security training policy is not fully developed.
		4a(4) Specialized security awareness training procedures are not fully developed or sufficiently detailed (SP 800-50, SP 800-53).
		4a(5) Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).
		4a(6) Identification and tracking of employees with login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).
		4a(7) Identification and tracking of employees without login privileges that require security awareness training is

		not adequate (SP 800-50, SP 800-53).
		4a(8) Identification and tracking of employees with significant security information security responsibilities is not adequate (SP 800-50, SP 800-53).
		4a(9) Training content for individuals with significant information security responsibilities is not adequate (SP 800-53, SP 800-16).
		4a(10) Less than 90 percent of employees with login privileges attended security awareness training in the past year.
		4a(11) Less than 90 percent of employees with significant security responsibilities attended security awareness training in the past year.
	✓	4a(12) Other: **TIGTA:** (1) Not all contractors with staff-like access at the IRS were provided with security awareness training. (2) The IRS needs to improve identification and tracking of employees and contractors with significant security responsibilities.
		Explanation for Other: **TIGTA:** (1) In June 2010, the GAO reported that the IRS did not provide security awareness training for all IRS contractors who are provided unescorted physical access to its facilities containing taxpayer receipts and information. Based on the GAO's finding, the IRS stated it updated its policy as of September 7, 2010, to require all contractors to take security awareness training suitable to their type of access, and modified its contractor tracking system to track the completion of the required training modules for each contractor during the Fiscal Year 2011 FISMA evaluation period. (2) The TIGTA was unable to definitively determine the percentage of IRS employees and contractors with significant security responsibilities that completed specialized security training in the past year. Until the IRS completes several actions, the TIGTA cannot verify the population of IRS employees and contractors that require specialized training or the numbers of those that completed their required training.
Comments:		

S5: POA&M

Status of Plan of Action & Milestones (POA&M) Program [check one]		a. The Agency has established and is maintaining a POA&M program that is generally consistent with NIST's and OMB's FISMA requirements and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for managing all known IT security weaknesses. 2. Tracks, prioritizes, and remediates weaknesses. 3. Ensures remediation plans are effective for correcting weaknesses. 4. Establishes and adheres to reasonable remediation dates. 5. Ensures adequate resources are provided for correcting weaknesses. 6. 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 POAM activities at least quarterly.
	✓	b. The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a POA&M program.
5a. If b. checked above, check areas that need significant improvement:		5a(1) POA&M policy is not fully developed.
		5a(2) POA&M procedures are not fully developed, sufficiently detailed or consistently implemented.
	✓	5a(3) POA&Ms do not include all known security weaknesses (OMB M-04-25).
	✓	5a(4) Remediation actions do not sufficiently address weaknesses (NIST SP 800-53, Rev 3, Sect. 3.4 Monitoring Security Controls).
		5a(5) Initial dates of security weaknesses are not tracked (OMB M-04-25).
		5a(6) Security weaknesses are not appropriately prioritized (OMB M-04-25).
		5a(7) Estimated remediation dates are not reasonable (OMB M-04-25).
		5a(8) Initial target remediation dates are frequently missed (OMB M-04-25).
	✓	5a(9) POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, & OMB M-04-25).
		5a(10) Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 & (OMB M-04-25).
		5a(11) Agency CIO does not track and review POA&Ms (NIST SP 810-53m, Rev. 3, Control CA-5 & (OMB M-04-25).
	✓	5a(12) Other: **TIGTA:** IRS security weaknesses were closed in POA&Ms before effective corrective action was taken.
		Explanation for Other: **TIGTA:** In August 2009, the TIGTA reported that the IRS had prematurely reported resolution of six security control vulnerabilities for the Customer Accounts Data Engine in POA&Ms before effective corrective

		action was taken. In May 2010, the TIGTA reported that the IRS closed four POA&M weaknesses identified in the Modernized e-File system before effective corrective action was taken. During the 2010 FISMA evaluation period, the IRS took steps to improve its POA&M procedures; however, the TIGTA did not find information to indicate that required verifications were performed before closing these weaknesses as per IRS policy.
Comments: **Treasury OIG:** FMS did not record security vulnerabilities timely in Trusted Agent FISMA (TAF) for 2 of the 3 systems. OCC did not update, submit, and include all necessary elements of the reviewed system's POA&M. **TIGTA:** In May 2010, the TIGTA reported that security weaknesses identified by the IRS at seven of the eight contractor facilities we sampled were not maintained in POA&Ms as required by the FISMA. In addition, during the Fiscal Year 2010 FISMA evaluation period, the TIGTA completed fieldwork on an audit to evaluate IRS email servers and found that medium-risk weaknesses the IRS repeatedly detected on its email servers through monthly scans were not posted to POA&Ms.		

S6: Remote Access Management

Status of Remote Access Program [check one]	✓	a. The Agency has established and is maintaining a remote access program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access. 2. Protects against unauthorized connections or subversion of authorized connections. 3. Users are uniquely identified and authenticated for all access. 4. If applicable, multi-factor authentication is required for remote access. 5. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms. 6. Requires encrypting files sensitive files transmitted across public networks or stored on mobile devices and removable media such as CDs and flash drives. 7. Remote access sessions are timed-out after a maximum of 30 minutes of inactivity after which re-authentication is required.
		b. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a program for providing secure remote access.
6a. If b. checked above, check areas that need significant improvement:		6a(1) Remote access policy is not fully developed.
		6a(2) Remote access procedures are not fully developed, sufficiently detailed or consistently implemented.
		6a(3) Telecommuting policy is not fully developed (NIST 800-46 Section 5.1).
		6a(4) Telecommuting procedures are not fully developed or sufficiently detailed (NIST 800-46 Section 5.4).

		6a(5) Agency cannot identify all users who require remote access (NIST 800-46 Section 4.2, Section 5.1).
		6a(6) Multi-factor authentication is not properly deployed (NIST 800-46 Section 2.2, Section 3.3).
		6a(7) Agency has not identified all remote devices (NIST 800-46 Section 2.1).
		6a(8) Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46 Section 3.1 and Section 4.2).
		6a(9) Agency does not adequately monitor remote devices when connected to the agency's networks remotely (NIST 800-46 Section 3.2).
		6a(10) Lost or stolen devices are not disabled and appropriately reported (NIST 800-46 Section 4.3, US-CERT Incident Reporting Guidelines).
		6a(11) Remote access rules of behavior are not adequate (NIST 800-53, PL-4).
		6a(12) Remote access user agreements are not adequate (NIST 800-46 Section 5.1 & NIST 800-53, PS-6).
		6a(13) Other
		Explanation for Other:

S7: Identity and Access Management

Status of Account and Identity Management Program [check one]		a. The Agency has established and is maintaining an account and identity management program that is generally consistent with NIST's and OMB's FISMA requirements and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for account and identity management. 2. Identifies all users, including federal employees, contractors, and others who access Agency systems. 3. Identifies when special access requirements (e.g. multi-factor authentication) are necessary. 4. If multi-factor authentication is in use, it is linked to the Agency's PIV program. 5. Ensures that the users are granted access based on needs and separation of duties principles. 6. Identifies devices that are attached to the network and distinguishes these devices from users. 7. Ensures that accounts are terminated or deactivated once access is no longer required.
	✓	b. The Agency has established and is maintaining an account and identity management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established an account and identity management program.
7a. If b. checked above, check areas that need significant improvement:		7a(1) Account management policy is not fully developed.
	✓	7a(2) Account management procedures are not fully developed, sufficiently detailed or consistently implemented.
		7a(3) Active directory is not properly implemented (NIST 800-53, AC-2).
		7a(4) Other non-Microsoft account management software is not properly implemented (NIST 800-53, AC-2).
		7a(5) Agency cannot identify all User and Non-User accounts (NIST 800-53, AC-2).
		7a(6) Accounts are not properly issued to new users (NIST 800-53, AC-2).
	✓	7a(7) Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).

	7a(8)	Agency does not use multi-factor authentication when required (NIST 800-53, IA-2).
	7a(9)	Agency has not adequately planned for implementation of PIV for logical access (HSPD-12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01).
✓	7a(10)	Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).
	7a(11)	Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).
	7a(12)	Network devices are not properly authenticated (NIST 800-53, IA-3).
✓	7a(13)	Other
		Explanation for Other: **Treasury OIG:** Review of Inactive Accounts and Annual Reviews Are Not Being Consistently Conducted Physical Access to Restricted Areas Is Not Properly Reviewed and Administered

Comments: **Treasury OIG:** BEP did not document its reviews of user accounts for the selected system in accordance with their system security plan. DO's first system reviewed did not disable users after 90 days of inactivity. OCC's system reviewed lacked an automated capability to disable inactive account per their policy. OIG's system reviewed had accounts that had not been disabled after 90 days of inactivity. OTS did not review user access to the system reviewed on a regular basis. FinCEN's physical access to their data center was not reviewed annually. The OIG's physical access to their data center was not reviewed annually.

TIGTA: The IRS has not completed corrective actions to resolve the component of the IRS computer security material weakness relating to access controls. While the IRS's corrective action plan for this material weakness indicates progress has been made, corrective actions are still ongoing to ensure that effective access controls are implemented IRS-wide. In July 2009, the TIGTA reported that, in a sample of 7 IRS systems, 53 of 376 contractors had active user accounts but did not have a business need to access these systems. The TIGTA also identified 15 contractors whose system access was not deleted in a timely manner upon separation from the contract with the IRS. In addition, in March 2010, the TIGTA reported that a system was not configured to remove user accounts in accordance with IRS security policy. In July 2009, the TIGTA reported that, from a sample of 7 IRS systems, 12 system development contractors had access and full privileges to the production environment of the system on which they worked, in violation of the IRS policy on separation of duties. In addition, 39 system administration contractors also had database administrator privileges. In addition, in March 2010, the TIGTA reported that 6 of 109 sampled employees' system privileges on the Automated Collection System were not restricted to only those privileges needed to perform assigned duties. In addition, 58 employees had unneeded privileges that allowed them the authority to create, modify, or delete the system audit trails.

S8: Continuous Monitoring Management

Status of Continuous Monitoring Program [check one]		a. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following

		attributes: 1. Documented policies and procedures for continuous monitoring. 2. Documented strategy and plans for continuous monitoring, such as vulnerability scanning, log monitoring, notification of unauthorized devices, sensitive new accounts, etc. 3. Ongoing assessments of selected security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans. 4. Provides system 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.
	✓	b. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a continuous monitoring program.
8a. If b. checked above, check areas that need significant improvement:		8a(1) Continuous monitoring policy is not fully developed.
		8a(2) Continuous monitoring procedures are not fully developed or consistently implemented.
		8a(3) Strategy or plan has not been fully developed for entity-wide continuous monitoring (NIST 800-37).
		8a(4) Ongoing assessments of selected security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).
		8a(5) The following were not provided to the system authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&Ms (NIST 800-53, NIST 800-53A).
	✓	8a(6) Other: **TIGTA:** The IRS has not resolved its computer security material weakness relating to audit logging.
		Explanation for Other: **Treasury OIG:** BEP did not document reviews of audit logs for the system we reviewed in accordance with NIST SP 800-53 and Treasury policy. **TIGTA:** The IRS corrective action plan for resolving the audit logging component of the IRS computer security material weakness indicates that there are still ongoing corrective actions. Until corrective actions are completed, the IRS cannot effectively monitor key networks and systems to identify unauthorized activities and inappropriate system configurations. In July 2010, the TIGTA reported that the IRS has not taken sufficient actions or allocated sufficient resources to resolve the audit trail material weakness. Our review of 20 major systems found that events were not being adequately captured and reviewed on many databases, applications, and operating systems because: 1) very few systems have audit plans, 2) the IRS did not have adequate event capturing and report generating software tools, 3) audit reports were not being generated, and 4) the IRS determined that capturing required events could hurt system performance.

S9: Contingency Planning

Status of Contingency Planning Program [check one]		a. The Agency established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster. 2. The agency has performed an overall Business Impact Assessment. 3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures. 4. Testing of all system-specific contingency plans. 5. The documented business continuity and disaster recovery plans are ready for implementation. 6. Development of training, testing, and exercises (TT&E) approaches. 7. Performance of regular ongoing testing or exercising of continuity/disaster recovery plans to determine effectiveness and to maintain current plans.
	✓	b. The Agency has established and is maintaining an entity-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a business continuity/disaster recovery program.
9a. If b. checked above, check areas that need significant improvement:		9a(1) Contingency planning policy is not fully developed.
		9a(2) Contingency planning procedures are not fully developed or consistently implemented.
		9a(3) An overall business impact assessment has not been performed (NIST SP 800-34).
		9a(4) Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).
		9a(5) A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34).
		9a(6) A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34).
		9a(7) System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(8) Critical systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(9) Training, testing, and exercises approaches have not been developed (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(10) Training, testing, and exercises approaches have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(11) Disaster recovery exercises were not successful (NIST SP 800-34).
		9a(12) After-action plans did not address issues identified during disaster recovery exercises (FCD1, NIST SP 800-34).
		9a(13) Critical systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(14) Alternate processing sites are subject to same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).

		9a(15) Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(16) Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(17) Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).
	✓	9a(18) Other: **TIGTA**: The IRS has made significant progress, but has not resolved its material weakness relating to disaster recovery controls.
		Explanation for Other: **TIGTA**: The IRS has not yet fully implemented adequate processes to ensure disaster recovery capabilities are implemented IRS-wide. While the IRS's material weakness corrective action plan indicates progress has been made in mitigating disaster recovery issues, corrective actions are still ongoing.
Comments:		

S10: Contractor Systems

Status of Agency Program to Oversee Contractor Systems [check one]		a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities of the Agency obtains sufficient assurance that security controls of systems operated by contractors or others on its behalf are effectively implemented and comply with federal and agency guidelines. 2. A complete inventory of systems operated on the Agency's behalf by contractors or other entities. 3. The inventory identifies interfaces between these systems and Agency-operated systems. 4. The agency requires agreements (MOUs, Interconnect Service Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates. 5. The inventory, including interfaces, is updated at least annually. 6. Systems that are owned or operated by contractors or entities are subject to and generally meet NIST and OMB's FISMA requirements.
	✓	b. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. However, the Agency needs to make significant improvements as noted below.
		c. The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities.
10a.If (b) checked above, check areas that need significant improvement:		10a(1) Policies to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed.
		10a(2) Procedures to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed or consistently implemented.
	✓	10a(3) The inventory of systems owned or operated by contractors or other entities is not sufficiently complete.
		10a(4) The inventory does not identify interfaces between contractor/entity-operated systems to Agency-owned and operated systems.
		10a(5) The inventory of contractor/entity-operated systems, including interfaces, is not updated at least annually.
		10a(6) Systems owned or operated by contractors and entities are not subject to NIST and OMB's FISMA requirements (e.g., certification and accreditation requirements).
		10a(7) Systems owned or operated by contractors and entities do not meet NIST and OMB's FISMA requirements (e.g., certification and accreditation requirements).
		10a(8) Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained,
		10a(9) Other
		Explanation for Other:

Comments: **TIGTA:** The IRS was unable to provide the TIGTA a definitive inventory of contractor managed systems and agreed that this inventory required improvement. In May 2010, the TIGTA reported that current processes were not effective at identifying all contractors who receive IRS taxpayer data and therefore are subject to required security reviews. The IRS has implemented an automated mechanism to identify all contractors that have access to sensitive data. This information will be available to target sites for security reviews during the Fiscal Year 2012 review cycle. The IRS stated it will also use this information to determine which of these meet the definition of a contractor system.

APPENDIX III – APPROACH TO SELECTION OF SUBSET OF SYSTEMS

In Fiscal Year (FY) 2010, KPMG employed a risk-based approach to select a representative subset of United States Department of the Treasury (Treasury) information systems for the Federal Information Security Management Act (FISMA) audit. KPMG used the system inventory contained within Treasury's Trusted Agent FISMA (TAF) to identify the population and stratified the population by bureau and office to select a representative subset of non-IRS Treasury applications. KPMG performed procedures throughout the fieldwork phase to determine the completeness and accuracy of the non-IRS Treasury inventory of information systems.

Based on historical trends in the Treasury systems inventory and past reviews, KPMG selected 13.5 percent of Treasury's non-IRS information systems. KPMG selected the representative subset of non-IRS information systems from TAF on April 14, 2010, prior to the Treasury's FISMA year-end on June 30, 2010. This advanced selection allowed KPMG sufficient time to complete planning and prepare for the fieldwork phase, which commenced immediately after Treasury's FISMA year-end.

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

- Total number of systems per bureau
- Systems at smaller bureaus not historically included in FISMA audits or evaluations
- Number of systems at each bureau with a FIPS system impact level of "High"
- Date of the system's Authority to Operate
- Number of open issues per system
- Number of issues recently closed per system
- Number of issues identified in previous FISMA audits, FISMA evaluations, and other recent Office of the Inspector General reviews, and the
- Availability of users to access the system using the Internet.

Lastly, the total number of financial systems selected in the representative subset did not exceed the percentage of systems the financial systems represent in the Treasury inventory of information systems. KPMG defined financial systems as those information systems that were designated as "Financial" systems in the Treasury's TAF system.

Based on KPMG's analysis of the Treasury inventory of information systems as of April 14, 2010, we noted Treasury's inventory included 186 major applications and general support systems. The following table provides KPMG's analysis of the composition of the Treasury's inventory of major applications and general support systems.

	Total	IRS	Non-IRS	Non-IRS Financial Systems
Major Applications	133	53	80	39
General Support Systems	53	21	32	4
Total	186	74	112	43

From the analysis above, KPMG determined that IRS systems comprised 40 percent of the total population of Major Applications and General Support systems, and Non-IRS systems accounted for 60

percent. Applying the subset size percentage of 13.5 percent to the total population of 186 yielded a total subset size of 25 systems. When the IRS to Non-IRS weighting was applied to this total, the resulting sizes for the IRS and Non-IRS subsets were 10 and 15, respectively.

KPMG considered the ratio of Major Applications and General Support Systems as well as the ratio of financial to non-financial information systems. Considering these ratios, KPMG judgmentally selected a representative subset of information systems for testing during the 2010 FISMA audit. Based on these factors, KPMG determined the following composition for the representative subset of Non-IRS Major Applications and General Support Systems for the FY 2010 FISMA audit:

Total Selected	15
Total Major Applications	9
Total General Support Systems	6
Total Systems with a FIPS 199 System Impact Level of "High"	6
Total Systems with a FIPS 199 System Impact Level of "Moderate"	9
Total Systems with a FIPS 199 System Impact Level of "Low"	0
Total Systems Designated as Financial	6

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

Bureau	Total Systems	Percentage of Total Non-IRS Population	Total Number of Non-IRS Systems to be Selected
BEP	5	4%	1
BPD	14	13%	2
CDFI Fund	3	3%	1 (see note 1)
DO	23	21%	2
FinCEN	5	4%	1
FMS	31	28%	3
Mint	10	9%	1
OCC	9	8%	1
OIG	1	1%	1 (see notes 1 and 2)
OTS	7	6%	1
TIGTA	2	2%	0 (see note 2)
TTB	2	2%	1 (see note 1)
Total	112	100% (note 3)	15

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

(**Note 2**: A decision was made by the OIG to inspect only one (1) OIG system every year.)

(**Note 3:** Percentages do not sum to 100% due to rounding.)

APPENDIX IV – SELECTED SECURITY CONTROL CLASSES AND FAMILIES

Federal Information Security Management Act (FISMA) directs the National Institute of Standards and Technology (NIST) to develop and issue standards, guidelines, and other publications to assist federal agencies in defining minimum security requirements for non-national security systems used by agencies. NIST has developed such standards and guidelines as part of its implementation of FISMA. KPMG based its security evaluation on the security controls defined within NIST Special Publication 800-53 Revision 2, *Recommended Security Control for the Federal Information Systems*. 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 KPMG performed in accordance with NIST Special Publication 800-53. KPMG selected specific test procedures that were applicable to the computing environment; therefore, not all available security controls within each control family were performed.

Management Controls

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

KPMG assessed the following management control areas:

- Certification, Accreditation, and Security Assessments (CA)
- Planning (PL)
- Risk Assessment (RA)
- System and Services Acquisition (SA)

Certification, Accreditation, and Security Assessments:

The organization develops, disseminates, and periodically reviews/updates (i) formal, documented, security assessment and certification and accreditation 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, certification and accreditation policies, associated assessment certification, and accreditation controls.

Security Controls	Title
CA-2	Security Assessments
CA-4	Security Certification
CA-5	Plan of Action and Milestone
CA-6	Security Accreditation

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
PL-3	System Security Plan Update

Risk Assessment:

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented risk assessment 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 risk assessment policy and associated risk assessment controls.

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

System and Services Acquisition:

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, system and services acquisition policy that includes information security considerations and 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 system and services acquisition policy and associated system and services acquisition controls.

Procedure	Title
SA-7	User Installed Software

Operational Controls

The operational controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

KPMG assessed the following Operational control areas:

- Configuration Management (CM)
- Contingency Planning (CP)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)

Configuration Management:

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, configuration management 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 configuration management policy and associated configuration management controls.

Procedure	Title
CM-2	Baseline Configuration

Contingency Planning:

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, contingency 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 configuration management policy and associated configuration management controls.

Procedure	Title
CP-2	Contingency Plan
CP-4	Contingency Plan Testing and Exercises
CP-5	Contingency Plan Update

Maintenance:

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

Procedure	Title
MA-5	Maintenance Personnel

Media Protection:

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

Procedure	Title
MP-6	Media Sanitization and Disposal

Physical and Environmental Protection:

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

Procedure	Title
PE-2	Physical Access Authorizations
PE-3	Physical Access Control

Technical Controls

Technical security controls for information systems focus on information systems that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware of the system.

KPMG assessed the following Technical control areas:

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

Access Control:

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, access control policy that addresses 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-7	Unsuccessful Login Attempts

Audit and Accountability:

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, audit and accountability 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 audit and accountability policy and associated audit and accountability controls.

Procedure	Title
AU-2	Auditable Events
AU-6	Audit Monitoring, Analysis, and Reporting

Identification and Authentication:

The organization develops, disseminates, and periodically reviews/updates (i) a formal, documented, identification and authentication 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 identification and authentication policy and associated identification and authentication controls.

Procedure	Title
IA-2	User Identification and Authentication
IA-4	Identifier Management

System and Communication Protection:

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

Procedure	Title
SC-13	Use of Cryptography

APPENDIX V – LIST OF ACRONYMS

Acronym	Definition
AC	Access Control
ACIOCS	Associate CIO for Cyber Security
ATO	Authority to Operate
AU	Audit and Accountability
BEP	Bureau of Engraving and Printing
BPD	Bureau of the Public Debt
CA	Certification, Accreditation, and Security Assessment
CDFI	Community Development Financial Institution
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Planning
CSS	Cyber Security Sub-Council
DO	Departmental Offices
FDCC	Federal Desktop Core Configuration
FinCEN	Financial Crimes Enforcement Network
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FMS	Financial Management Service
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
IA	Identification and Authentication
IG	Inspector General
IRS	Internal Revenue Service
ISSO	Information System Security Officer
IT	Information Technology
KPMG	KPMG LLP
LAN	Local Area Network
MA	Maintenance
Mint	United States Mint
MP	Media Protection
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget

Acronym	Definition
OPTR	Office of Privacy and Treasury Records
OTS	Office of Thrift Supervision
PE	Physical and Environmental Protection
PII	Personally Identifiable Information
PL	Planning
POA&M	Plan of Action and Milestones
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communication Protection
SCAP	Security Content Automation Protocol
SIGTARP	Special Inspector General for Troubled Asset Relief Program
TAF	Trusted Agent FISMA
TARP	Troubled Asset Relief Program
TCIO	Treasury Chief Information Officer
TCSIRC	Treasury Computer Security Incident Response Capability
TD	Treasury Directive
TD P	Treasury Directive Publication
TIGTA	Treasury Inspector General for Tax Administration
TTB	Alcohol and Tobacco Tax and Trade Bureau
US	United States

ATTACHMENT 2

Treasury Inspector General for Tax Administration–Federal Information Security Management Act Report for Fiscal Year 2010, (Audit # 2011-20-003), November 10, 2010

Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2010

November 10, 2010

Reference Number: 2011-20-003

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

November 10, 2010

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

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2010 (Audit # 201020010)

We are pleased to submit the Treasury Inspector General for Tax Administration's Federal Information Security Management Act (FISMA)[1] report for the Fiscal Year 2010 FISMA evaluation period.[2] The FISMA requires the Office of Inspector General to perform an annual independent evaluation of each Federal agency's information security policies, procedures, and practices, as well as evaluate its compliance with FISMA requirements. This report reflects our independent evaluation of the Internal Revenue Service's (IRS) information technology security program for the period under review.

We based our evaluation of the IRS on the Office of Management and Budget's (OMB) FISMA 2010 Reporting Guidelines. During the 2010 evaluation period, we conducted 10 audits, as shown in Appendix II, to evaluate the adequacy of information security in the IRS. We considered the results of these audits in our evaluation. In addition, we evaluated a representative sample of 10 major IRS information systems for our FISMA work. For each system in the sample, we assessed the quality of the certification and accreditation process, the annual testing of controls for continuous monitoring, the testing of information technology contingency plans, and the quality of the Plan of Action and Milestones process. We also conducted tests to evaluate processes over configuration management, incident response and

[1] 44 U.S.C. §§ 3541–3549.
[2] The Fiscal Year 2010 FISMA evaluation period for the Department of the Treasury is July 1, 2009, through June 30, 2010. All subsequent references to 2010 refer to the FISMA evaluation period.

reporting, security training, remote access, account and identity management, and contractor oversight.

Included in Appendix I are our responses to the OMB's 2010 FISMA checklist for the Inspectors General. Major contributors to this report are listed in Appendix III.

Based on our 2010 evaluation, we determined that the IRS's information security program was generally compliant with the FISMA legislation, OMB information security requirements, and related information security standards published by the National Institute of Standards and Technology. We determined that the following program areas met the level of performance specified by the OMB's 2010 FISMA checklist.

- Certification and accreditation program.
- Incident response and reporting program.
- Remote access management.

While the information security program was generally compliant with the FISMA legislation, the program was not fully effective as a result of the conditions identified in the following areas.

- Configuration management.
- Security training.
- Plans of action and milestones.
- Identity and access management.
- Continuous monitoring management.
- Contingency planning.
- Contractor systems/financial audit.

Specific to the financial audit area, the Government Accountability Office (GAO) reported[3] newly identified and unresolved information security control weaknesses in key financial and tax processing systems continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information. Until these control weaknesses are corrected, the IRS remains unnecessarily vulnerable to insider threats related to the unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as the disruption of system operations and services. These conditions were the basis for GAO's determination that the IRS had a material weakness in internal controls over financial reporting related to information security in Fiscal Year 2009.

[3] *INFORMATION SECURITY: IRS Needs to Continue to Address Significant Weaknesses* (GAO-10-355, dated March 2010).

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.

Table of Contents

Abbreviations

CIO	Chief Information Officer
FCD1	Federal Continuity Directive 1
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
IRS	Internal Revenue Service
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
TIGTA	Treasury Inspector General for Tax Administration
TT&E	Training, Testing, and Exercises
US-CERT	United States Computer Emergency Response Team

Background

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

The Federal Information Security Management Act (FISMA)[1] was enacted to strengthen the security of information and systems within Federal agencies. As part of this legislation, each Federal Government agency is required to report annually to the Office of Management and Budget (OMB) on the effectiveness of its security programs. In addition, the FISMA requires the Offices of Inspector General to perform an annual independent evaluation of each Federal agency's information security policies and procedures, as well as evaluate its compliance with FISMA requirements. In compliance with the FISMA requirements, the Treasury Inspector General for Tax Administration (TIGTA) performs the annual independent evaluation of the information security program and practices of the IRS.

The OMB provides information security performance measures by which each agency is evaluated for the FISMA review. The OMB uses the information from the agencies and independent evaluations to help assess agency-specific and Federal Governmentwide security performance, develop its annual security report to Congress, and assist in improving and maintaining adequate agency security performance.

Attached is the TIGTA's Fiscal Year 2010 FISMA report. The report was forwarded to the Treasury Inspector General for consolidation into a report issued to the Department of the Treasury Chief Information Officer.

[1] 44 U.S.C. §§ 3541–3549.

Appendix I

Results of the Treasury Inspector General for Tax Administration's Federal Information Security Management Act Review[1]

The OMB issued a checklist for use by Offices of Inspectors General to assess the level of performance achieved by agencies in the specified program areas during the 2010 FISMA evaluation period. This appendix presents our completed OMB checklist for the IRS.

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

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

For our FISMA work, we evaluated a representative sample of 10 major IRS information systems, which included 9 IRS systems and 1 contractor-managed system. Of these 10 systems, 1 system had a Federal Information Processing Standards (FIPS) 199 impact level of high, and 9 systems were of a moderate impact level. All 10 systems had a current certification and accreditation, had security controls tested within the past year, and had contingency plans tested in accordance with policy.

[1] Due to the nature of the listing that follows, abbreviations are used exactly as presented in the original document reproduced and are not defined therein. Please see the Abbreviations page after the Table of Contents of this report for a listing of abbreviations.

RESPONSES TO FISCAL YEAR 2010 OMB QUESTIONS FOR INSPECTOR GENERALS

S1: Certification and Accreditation

Status of Certification and Accreditation Program [check one]	✓	a. The Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures describing the roles and responsibilities of participants in the certification and accreditation process. 2. Establishment of accreditation boundaries for Agency information systems. 3. Categorizes information systems. 4. Applies applicable minimum baseline security controls. 5. Assesses risks and tailors security control baseline for each system. 6. Assessment of the management, operational, and technical security controls in the information system. 7. Risks to Agency operations, assets, or individuals analyzed and documented in the system security plan, risk assessment, or an equivalent document. 8. The accreditation official is provided (i) the security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective actions; (ii) the plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and (iii) the updated system security plan with the latest copy of the risk assessment.
		b. The Agency has established and is maintaining a certification and accreditation program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a certification and accreditation program.
1a. If b. checked above, check areas that need significant improvement:		1a(1) Certification and accreditation policy is not fully developed.
		1a(2) Certification and accreditation procedures are not fully developed, sufficiently detailed, or consistently implemented.
		1a(3) Information systems are not properly categorized (FIPS 199/SP 800-60).
		1a(4) Accreditation boundaries for Agency information systems are not adequately defined.
		1a(5) Minimum baseline security controls are not adequately applied to information systems (FIPS 200/SP 800-53).
		1a(6) Risk assessments are not adequately conducted (SP 800-30).
		1a(7) Security control baselines are not adequately tailored to individual information systems (SP 800-30).

		1a(8) Security plans do not adequately identify security requirements (SP 800-18).
		1a(9) Inadequate process to assess security control effectiveness (SP 800-53A).
		1a(10) Inadequate process to determine risk to Agency operations, Agency assets, or individuals or to authorize information systems to operate (SP 800-37).
		1a(11) Inadequate process to continuously track changes to information systems that may necessitate reassessment of control effectiveness (SP 800-37).
		1a(12) Other.
		Explanation for Other:
Comments:		

S2: Configuration Management

Status of Security Configuration Management Program [check one]		a. The Agency has established and is maintaining a security configuration management program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for configuration management. 2. Standard baseline configurations. 3. Scanning for compliance and vulnerabilities with baseline configurations. 4. FDCC baseline settings fully implemented and/or any deviations from FDCC baseline settings fully documented. 5. Documented proposed or actual changes to the configuration settings. 6. Process for the timely and secure installation of software patches.
	✓	b. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a security configuration management program.
2a. If b. checked above, check areas that need significant improvement:		2a(1) Configuration management policy is not fully developed.
	✓	2a(2) Configuration management procedures are not fully developed or consistently implemented.
		2a(3) Software inventory is not complete (NIST 800-53: CM-8).
		2a(4) Standard baseline configurations are not identified for all software components (NIST 800-53: CM-8).
		2a(5) Hardware inventory is not complete (NIST 800-53: CM-8).
		2a(6) Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).
		2a(7) Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).
		2a(8) FDCC is not fully implemented (OMB) and/or all deviations are not fully documented.
		2a(9) Software scanning capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).

	✓	2a(10) Configuration-related vulnerabilities have not been remediated in a timely manner (NIST 800-53: CM-4, CM-6, RA-5, SI-2).
	✓	2a(11) Patch management process is not fully developed (NIST 800-53: CM-3, SI-2).
		2a(12) Other.
		Explanation for Other:

Comments:

2a(2): The IRS has not completed corrective actions to resolve the software configuration management component of the IRS computer security material weakness.[2] Although the IRS has made progress in implementing its configuration management program, the IRS corrective action plan for resolving this material weakness indicates ongoing corrective actions with scheduled completion dates ranging from April to December 2011. Until the IRS has implemented adequate configuration management controls Agencywide, it cannot ensure the security and integrity of system programs, files, and data.

- 1-3-20: Ensure security configuration requirements for all system software are documented in an IRS Internal Revenue Manual. (Planned implementation date of April 2011)
- 1-3-21: Implement and maintain baseline standard configurations on system software platforms and perform scheduled testing. This capability covers translation of Internal Revenue Manuals into standard build procedures and implementation/testing processes. (Planned implementation date of April 2011)
- 1-3-22: Ensure system software is controlled under a documented change control process with procedures for assessment of security impact, notifications to Designated Approving Authorities, and appropriate baseline configuration updates. (Planned implementation date of April 2011)
- 1-3-25: Establish and maintain collection and reporting of metrics to assess progress and track improvements in all component activity implementations over time. Successful operation of the policy, procedures, and plans for component activities for at least 2 consecutive quarters. Quarterly reviews by Cybersecurity and annual FISMA security reviews will revalidate compliance. (Planned implementation date of December 2011)

2a(10): In March 2010, TIGTA reported[3] that the IRS was not timely addressing high- and medium-risk system vulnerabilities that it identified on Automated Collection System servers. The IRS UNIX Policy Checker scans that the IRS ran on the servers from January through May 2009 reported that some high- and medium-risk vulnerabilities remained on the servers for 2 to 5 months before system administrators took corrective actions.

[2] The IRS declared its security program as a material weakness in 1997. The IRS further categorized the material weakness into nine areas relating to computer security: (1) network access controls; (2) key computer applications and system access controls; (3) software configuration; (4) functional business, operating, and program units security roles and responsibilities; (5) segregation of duties between system and security administrators; (6) contingency planning and disaster recovery; (7) monitoring of key networks and systems; (8) security training; and (9) certification and accreditation. An Executive Steering Committee oversees the plan, ensuring that material weakness areas are addressed by all affected organizations, appropriate policy and procedures are implemented, and actions resolve the systemic cause of the material weakness. The IRS has closed four of the material weakness areas: (4) functional business, operating, and program units security roles and responsibilities (5) segregation of duties between system and security administrators; (8) security training; and (9) certification and accreditation. The TIGTA did not concur with the IRS's closure of area (4), functional business, operating, and program units security roles and responsibilities.

[3] *Additional Security Controls Are Needed to Protect the Automated Collection System* (Reference Number 2010-20-028, dated March 30, 2010).

In addition, during the 2010 FISMA evaluation period, the TIGTA concluded fieldwork on an audit to evaluate IRS email servers and found that the IRS is not taking timely actions to correct medium-risk security vulnerabilities identified through monthly scans on its email servers. The Modernization and Information Technology Services organization's Enterprise Operations office uses the Windows Policy Checker to conduct monthly scans of its 70 email servers. The scans conducted from September 2009 through February 2010 determined the servers failed between 73 and 79 medium-risk security checks each month. The number of failed security checks on each server was the same each month. 2a(11): The IRS computer security material weakness relating to configuration management includes unresolved weaknesses in the IRS patch management process. The IRS corrective action plan for resolving the patch management weaknesses indicates the following two corrective actions will be completed in April 2011. • 1-3-23: Ensure system software is patched under a documented process that includes standard procedures and fall-back procedures, ensures patch testing, and ensures the dissemination, installation, and verification of patch installations for all components. (Planned implementation date of April 2011) • 1-3-24: Internal and external monitoring and reporting on secure configuration setting changes and patch levels. "Review" includes comparison to approved changes. "Remediation" includes followup on noncompliant components and testing and implementation of proposed corrections. (Planned implementation date of April 2011)

2b. Identify baselines reviewed:		
2b(1)	Software Name	None.
2b(2)	Software Version	None.

S3: Incident Response and Reporting

Status of Incident Response & Reporting Program [check one]	✓	a. The Agency has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for responding and reporting to incidents. 2. Comprehensive analysis, validation, and documentation of incidents. 3. When applicable, reports to US-CERT within established time frames. 4. When applicable, reports to law enforcement within established time frames. 5. Responds to and resolves incidents in a timely manner to minimize further damage.
		b. The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established an incident response and reporting program.
3a. If b. checked above, check areas that need significant improvement:		3a(1) Incident response and reporting policy is not fully developed.
		3a(2) Incident response and reporting procedures are not fully developed, sufficiently detailed, or consistently implemented.
		3a(3) Incidents were not identified in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).

		3a(4) Incidents were not reported to US-CERT as required (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
		3a(5) Incidents were not reported to law enforcement as required.
		3a(6) Incidents were not resolved in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
		3a(7) Incidents were not resolved to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
		3a(8) There is insufficient incident monitoring and detection coverage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
		3a(9) Other.
		Explanation for Other:
Comments:		

S4: Security Training

Status of Security Training Program [check one]		a. The Agency has established and is maintaining a security training program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for security awareness training. 2. Documented policies and procedures for specialized training for users with significant information security responsibilities. 3. Appropriate training content based on the organization and roles. 4. Identification and tracking of all employees with login privileges that need security awareness training. 5. Identification and tracking of employees without login privileges that require security awareness training. 6. Identification and tracking of all employees with significant information security responsibilities that require specialized training.
	✓	b. The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a security training program.
4a. If b. checked above, check areas that need significant improvement:		4a(1) Security awareness training policy is not fully developed.
		4a(2) Security awareness training procedures are not fully developed, sufficiently detailed, or consistently implemented.
		4a(3) Specialized security training policy is not fully developed.
		4a(4) Specialized security awareness training procedures are not fully developed or sufficiently detailed (SP 800-50, SP 800-53).
		4a(5) Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).
		4a(6) Identification and tracking of employees with login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).

		4a(7) Identification and tracking of employees without login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).
		4a(8) Identification and tracking of employees with significant security information security responsibilities is not adequate (SP 800-50, SP 800-53).
		4a(9) Training content for individuals with significant information security responsibilities is not adequate (SP 800-53, SP 800-16).
		4a(10) Less than 90 percent of employees with login privileges attended security awareness training in the past year.
		4a(11) Less than 90 percent of employees, contractors, and other users with significant security responsibilities attended specialized security awareness training in the past year.
	✓	4a(12) Other(s). (i): Not all contractors with staff-like access were provided with security awareness training. (ii): Until the IRS improves its identification and tracking of employees and contractors with significant security responsibilities, the percentage of those who completed specialized security training in the past year cannot be verified.
		Explanation for Other(s): (i): In accordance with FISMA requirements, IRS policy requires the Agency to provide security awareness training to inform all IRS employees and contractors of the information security risks associated with their activities and their responsibilities in complying with IRS policies and procedures designed to reduce these risks. However, in June 2010, the GAO reported that the IRS did not provide security awareness training for all IRS contractors, such as janitors and security guards, who are provided unescorted physical access to its facilities containing taxpayer receipts and information.[4] Based on the GAO's finding, the IRS stated it updated its policy as of September 7, 2010, to require all contractors to take security awareness training suitable to their type of access. The IRS also stated that it modified its contractor tracking system to track the completion of the required training modules for each contractor during the Fiscal Year 2011 FISMA evaluation period. (ii): We were unable to definitively determine the percentage of employees and contractors with significant security responsibilities that completed specialized security training in the Fiscal Year 2010 FISMA evaluation period. The IRS reported 6,014 of 6,029 (99.8 percent) employees completed their required hours of specialized security training for the Fiscal Year 2010 FISMA evaluation period. The IRS did not track

[4] *Management Report: Improvements Are Needed in IRS's Internal Controls and Compliance with Laws and Regulations* (GAO-10-565R, dated June 2010).

		contractor completion of specialized security training. In a recent TIGTA review,[5] we reported that the IRS needed to improve processes to identify all IRS employees and contractors performing in security roles requiring specialized training. The IRS had not yet documented in its official policy five security roles that the Department of the Treasury policy states must receive specialized training. As a result, the IRS agreed to update its policy to include all security roles in existence at the IRS and crosswalk these with its current training curriculum. In addition, the IRS stated it has recently modified its contractor tracking system to identify contractors that require specialized training and plans to write policy and associated security clauses to require contractors to comply with these training requirements, to be effective for the Fiscal Year 2012 FISMA evaluation period. Until the IRS completes these actions, we cannot verify the population of IRS employees and contractors that require specialized training or the numbers of those that completed their required training.
Comments:		

S5: POA&M

Status of Plan of Action & Milestones (POA&M) Program [check one]		a. The Agency has established and is maintaining a POA&M program that is generally consistent with NIST's and OMB's FISMA requirements and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for managing all known IT security weaknesses. 2. Tracks, prioritizes, and remediates weaknesses. 3. Ensures remediation plans are effective for correcting weaknesses. 4. Establishes and adheres to reasonable remediation dates. 5. Ensures adequate resources are provided for correcting weaknesses. 6. 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.
	✓	b. The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a POA&M program.
5a. If b. checked above, check areas that need significant improvement:		5a(1) POA&M policy is not fully developed.
		5a(2) POA&M procedures are not fully developed, sufficiently detailed, or consistently implemented.
	✓	5a(3) POA&Ms do not include all known security weaknesses (OMB M-04-25).

[5] *More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness* (Reference Number 2010-20-084, dated August 26, 2010).

	5a(4)	Remediation actions do not sufficiently address weaknesses (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls).
	5a(5)	Initial dates of security weaknesses are not tracked (OMB M-04-25).
	5a(6)	Security weaknesses are not appropriately prioritized (OMB M-04-25).
	5a(7)	Estimated remediation dates are not reasonable (OMB M-04-25).
	5a(8)	Initial target remediation dates are frequently missed (OMB M-04-25).
	5a(9)	POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, & OMB M-04-25).
	5a(10)	Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 & OMB M-04-25).
	5a(11)	Agency CIO does not track and review POA&Ms (NIST SP 810-53m, Rev. 3, Control CA-5 & OMB M-04-25).
✓	5a(12)	Other: Security weaknesses were closed in POA&Ms before effective corrective action was taken.
	Explanation for Other:	In August 2009, the TIGTA reported[6] that the IRS had prematurely reported resolution of 6 of 13 security control vulnerabilities in the POA&M for the Customer Accounts Data Engine before effective corrective action was taken. In May 2010, the TIGTA reported[7] that the IRS closed four POA&M weaknesses identified in the Modernized e-File system before effective corrective action was taken. During the 2010 FISMA evaluation period, the IRS took steps to improve its POA&M procedures, including requiring system owners to document sufficient detail regarding how weaknesses were remediated before changing their status to "completed." We reviewed the weaknesses that were closed during the 2010 FISMA cycle for our 10 sample systems and found system owners had documented information to support their corrective actions. However, we did not find information to indicate that required verifications were performed before closing these weaknesses as per IRS policy. The Cybersecurity organization indicated that this verification step may be implemented during the next FISMA cycle, depending on available resources.

Comments:

5a(3): In May 2010, the TIGTA reported[8] that security weaknesses identified by the IRS at seven of the eight contractor facilities we sampled were not maintained in POA&Ms as required by the FISMA. These weaknesses

[6] *Customer Account Data Engine Release 4 Includes Most Planned Capabilities and Security Requirements for Processing Individual Tax Account Information* (Reference Number 2009-20-100, dated August 28, 2009).
[7] *Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement* (Reference Number 2010-20-041, dated May 26, 2010).

included access control, configuration management control, and system integrity control issues. The IRS agreed with our report finding that these security weaknesses should be tracked in POA&Ms.

In addition, during the Fiscal Year 2010 FISMA evaluation period, the TIGTA completed fieldwork on an audit to evaluate IRS email servers and found that medium-risk weaknesses the IRS repeatedly detected on its email servers through monthly scans were not posted to POA&Ms. Monthly scans conducted from September 2009 through February 2010 determined that the servers failed between 73 and 79 medium-risk security checks each month.

S6: Remote Access Management

Status of Remote Access Program [check one]	✓	a. The Agency has established and is maintaining a remote access program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access. 2. Protects against unauthorized connections or subversion of authorized connections. 3. Users are uniquely identified and authenticated for all access. 4. If applicable, multi-factor authentication is required for remote access. 5. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms. 6. Requires encrypting sensitive files transmitted across public networks or stored on mobile devices and removable media such as CDs and flash drives. 7. Remote access sessions are timed-out after a maximum of 30 minutes of inactivity, after which re-authentication is required.
		b. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a program for providing secure remote access.
6a. If b. checked above, check areas that need significant improvement:		6a(1) Remote access policy is not fully developed.
		6a(2) Remote access procedures are not fully developed, sufficiently detailed, or consistently implemented.
		6a(3) Telecommuting policy is not fully developed (NIST 800-46 Section 5.1).
		6a(4) Telecommuting procedures are not fully developed or sufficiently detailed (NIST 800-46 Section 5.4).
		6a(5) Agency cannot identify all users who require remote access (NIST 800-46 Section 4.2, Section 5.1).
		6a(6) Multi-factor authentication is not properly deployed (NIST 800-46 Section 2.2, Section 3.3).

[8] *Taxpayer Data Used at Contractor Facilities May Be at Risk for Unauthorized Access or Disclosure* (Reference Number 2010-20-51, dated May 18, 2010).

		6a(7) Agency has not identified all remote devices (NIST 800-46 Section 2.1).
		6a(8) Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46 Section 3.1 and Section 4.2).
		6a(9) Agency does not adequately monitor remote devices when connected to the Agency's networks remotely (NIST 800-46 Section 3.2).
		6a(10) Lost or stolen devices are not disabled and appropriately reported (NIST 800-46 Section 4.3, US-CERT Incident Reporting Guidelines).
		6a(11) Remote access rules of behavior are not adequate (NIST 800-53, PL-4).
		6a(12) Remote access user agreements are not adequate (NIST 800-46 Section 5.1 & NIST 800-53, PS-6).
		6a(13) Other.
		Explanation for Other:

S7: Identity and Access Management

Status of Account and Identity Management Program [check one]		a. The Agency has established and is maintaining an account and identity management program that is generally consistent with NIST's and OMB's FISMA requirements and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for account and identity management. 2. Identifies all users, including Federal employees, contractors, and others who access Agency systems. 3. Identifies when special access requirements (e.g., multi-factor authentication) are necessary. 4. If multi-factor authentication is in use, it is linked to the Agency's PIV program. 5. Ensures that the users are granted access based on needs and separation of duties principles. 6. Identifies devices that are attached to the network and distinguishes these devices from users. 7. Ensures that accounts are terminated or deactivated once access is no longer required.
	✓	b. The Agency has established and is maintaining an account and identity management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established an account and identity management program.
7a. If b. checked above, check areas that need significant improvement:		7a(1) Account management policy is not fully developed.
	✓	7a(2) Account management procedures are not fully developed, sufficiently detailed, or consistently implemented.
		7a(3) Active directory is not properly implemented (NIST 800-53, AC-2).
		7a(4) Other non-Microsoft account management software is not properly implemented (NIST 800-53, AC-2).

	7a(5)	Agency cannot identify all User and Non-User accounts (NIST 800-53, AC-2).
	7a(6)	Accounts are not properly issued to new users (NIST 800-53, AC-2).
✓	7a(7)	Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).
	7a(8)	Agency does not use multi-factor authentication when required (NIST 800-53, IA-2).
	7a(9)	Agency has not adequately planned for implementation of PIV for logical access (HSPD-12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01).
✓	7a(10)	Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).
	7a(11)	Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).
	7a(12)	Network devices are not properly authenticated (NIST 800-53, IA-3).
	7a(13)	Other.
		Explanation for Other:

Comments:

7a(2): The IRS has not completed corrective actions to resolve the component of the IRS computer security material weakness relating to access controls. While the IRS's corrective action plan for this material weakness indicates progress has been made in completing the planned actions, there are still ongoing corrective actions with scheduled completion dates ranging from April to December 2011. These involve ensuring that effective access controls are implemented IRS-wide. Until the IRS completes these corrective actions, it cannot ensure that access to key computer applications and systems is limited to authorized persons for authorized purposes.

- 1-2-20: Develop implementation plan to ensure that corrective actions 1-2-11, 12, 13, 14, 15, and 16[9] can be applied to all organizations, systems, and applications to full levels of effectiveness regarding policies, procedures, implementations, monitoring, and testing. (Planned implementation date of April 2011)
- 1-2-21: Execute implementation plan to ensure that corrective actions 1-2-11, 12, 13, 14, 15, and 16 can be applied to all organizations, systems, and applications to full levels of effectiveness regarding policies, procedures, implementations, monitoring, and testing. (Planned implementation date of April 2011)
- 1-2-22: Establish and maintain collection and reporting of metrics to assess progress and track improvements in all component activity implementations over time. Successful operation of the policy, procedures, and plans for component activities for at least two consecutive quarters. Quarterly review by Cybersecurity and annual FISMA security review will revalidate compliance. (Planned implementation date of December 2011)

7a(7): In July 2009, the TIGTA reported[10] that, in a sample of 7 systems, 53 of 376 contractors had active user accounts but did not have a business need to access these systems. These 53 contractors consisted of contractors whose job duties or access privileges had changed and no longer needed system access, contractors who had

[9] These corrective actions listed relate to account management procedures, including controlling user authorizations and levels of privileges on all systems, applications, databases, and other software. This footnote also applies the corrective action 1-2-21.
[10] *Computer System Access Controls Over Contractors Need to Be Improved* (Reference Number 2009-20-108, dated July 24, 2009).

separated from the contract with the IRS, and contractors who had never logged on to the system or had not logged on to the system within 45 calendar days. We also identified 15 contractors whose system access was not deleted in a timely manner upon separation from the contract with the IRS. The IRS agreed with our report findings. The IRS stated that, effective September 7, 2010, it began tracking information from contractors concerning employee status changes, including separations and changes in duties, to ensure timely account termination when access is no longer required.

In addition, in March 2010, the TIGTA reported[11] that the Registered User Portal, which allows tax professionals to electronically submit and retrieve tax-related information, was not configured to disable and remove users' access accounts in accordance with IRS security policies and procedures. Rather than implement the control to disable inactive accounts after 45 days as required by IRS policy, the IRS set the control to 720 days. In addition, the IRS did not implement a control to remove inactive accounts. Inactive accounts unnecessarily increase the opportunity for malicious individuals to gain access to taxpayer data through an unused account.

7a(10): In July 2009, the TIGTA reported[12] that, from a sample of 7 IRS systems, 12 system development contractors had access and full privileges to the production environment of the system on which they worked, in violation of the IRS policy on separation of duties. Developers with access to the production system could bypass controls and make unapproved and untested changes. In addition, 39 system administration contractors also had database administrator privileges. This lack of separation of duties could jeopardize the integrity of the data and allow unauthorized changes to the data to go undetected. The IRS stated it is now notifying contractors during the on-boarding process of the separation of duties requirement and requiring contractors to identify which one of those duties they will perform, if any.

In addition, in March 2010, the TIGTA reported[13] that 6 of 109 sampled employees' system privileges on the Automated Collection System were not restricted to only those privileges needed to perform assigned duties. Excessive privileges granted included the ability to increase the privileges of other users and to perform management queries to view large amounts of sensitive tax collection data. When users are granted access permissions beyond their assigned responsibilities, the risks of malicious actions and unauthorized disclosure of taxpayer data are increased. In addition, 58 employees had unneeded privileges that allowed them the authority to create, modify, or delete the system audit trails. These actions, taken either accidently or intentionally, could conceal unauthorized activity and compromise the integrity of the audit trail.

[11] *Additional Security Is Needed for Access to the Registered User Portal* (Reference Number 2010-20-027, dated March 31, 2010).
[12] *Computer System Access Controls Over Contractors Need to Be Improved* (Reference Number 2009-20-108, dated July 24, 2009).
[13] *Additional Security Controls Are Needed to Protect the Automated Collection System* (Reference Number 2010-20-028, dated March 30, 2010).

S8: Continuous Monitoring Management

Status of Continuous Monitoring Program [check one]		a. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for continuous monitoring. 2. Documented strategy and plans for continuous monitoring, such as vulnerability scanning, log monitoring, notification of unauthorized devices, sensitive new accounts, etc. 3. Ongoing assessments of selected security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans. 4. Provides system 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.
	✓	b. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a continuous monitoring program.
8a. If b. checked above, check areas that need significant improvement:		8a(1) Continuous monitoring policy is not fully developed.
		8a(2) Continuous monitoring procedures are not fully developed or consistently implemented.
		8a(3) Strategy or plan has not been fully developed for entity-wide continuous monitoring (NIST 800-37).
		8a(4) Ongoing assessments of selected security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).
		8a(5) The following were not provided to the system authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&Ms (NIST 800-53, NIST 800-53A).
	✓	8a(6) Other: The IRS has not resolved its computer security material weakness relating to audit logging.
		Explanation for Other: The IRS has not completed corrective actions to resolve the audit logging component of the IRS computer security material weakness. The IRS corrective action plan for resolving the audit logging weakness indicates that there are still ongoing corrective actions with scheduled completion dates ranging from February 2011 to October 2013. Until corrective actions are completed to resolve the audit logging material weakness, the IRS cannot effectively monitor key networks and systems to identify unauthorized activities and inappropriate system configurations.

		During the 2010 FISMA evaluation period, the TIGTA reported that the IRS continues to have problems with audit logging. In March 2010, the TIGTA reported[14] that the IRS does not analyze the audit logs for the Registered User Portal system to detect unlawful or unauthorized activities. Consequently, unauthorized access to taxpayer data could go undetected. In March 2010, the TIGTA reported[15] that the IRS is not capturing all of the required auditable events in Automated Collection System audit trails. The IRS informed us that enabling all required auditing events would negatively affect system performance. In July 2010, the TIGTA reported[16] **********2(f)**********.
Comments:		

S9: Contingency Planning

Status of Contingency Planning Program [check one]		a. The Agency established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster. 2. The Agency has performed an overall Business Impact Assessment. 3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures. 4. Testing of all system-specific contingency plans. 5. The documented business continuity and disaster recovery plans are ready for implementation. 6. Development of training, testing, and exercises (TT&E) approaches. 7. Performance of regular ongoing testing or exercising of continuity/disaster recovery plans to determine effectiveness and to maintain current plans.

[14] *Additional Security Is Needed for Access to the Registered User Portal* (Reference Number 2010-20-027, dated March 31, 2010).
[15] *Additional Security Controls Are Needed to Protect the Automated Collection System* (Reference Number 2010-20-028, dated March 30, 2010).
[16] *Additional Actions and Resources Are Needed to Resolve the Audit Trail Portion of the Computer Security Material Weakness* (Reference Number 2010-20-082, dated July 28, 2010).

	✓	b. The Agency has established and is maintaining an entity-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a business continuity/disaster recovery program.
9a. If b. checked above, check areas that need significant improvement:		9a(1) Contingency planning policy is not fully developed.
		9a(2) Contingency planning procedures are not fully developed or consistently implemented.
		9a(3) An overall business impact assessment has not been performed (NIST SP 800-34).
		9a(4) Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).
		9a(5) A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34).
		9a(6) A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34).
		9a(7) System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(8) Critical systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(9) Training, testing, and exercises approaches have not been developed (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(10) Training, testing, and exercises approaches have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(11) Disaster recovery exercises were not successful (NIST SP 800-34).
		9a(12) After-action plans did not address issues identified during disaster recovery exercises (FCD1, NIST SP 800-34).
		9a(13) Critical systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(14) Alternate processing sites are subject to same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(15) Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(16) Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(17) Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).
	✓	9a(18) Other: The IRS has made significant progress, but has not resolved its material weakness relating to disaster recovery controls.
		Explanation for Other: The IRS has not yet fully implemented adequate processes to ensure disaster recovery capabilities are implemented IRS-wide. While the IRS's material weakness corrective action plan indicates progress has been made in mitigating disaster recovery issues, the following disaster recovery corrective actions are still ongoing with scheduled completion dates

		ranging from October 2010 to December 2011. These involve ensuring effective disaster recovery controls are implemented IRS-wide. Until the IRS has completed its corrective actions to resolve this weakness, it cannot ensure critical business systems can be timely restored when unexpected events occur. • 1-6-16 – Disaster Recovery Compliance: Complete internal auditing of the disaster recovery efforts to ensure accuracy and completeness as it relates to day-to-day operations and efforts to mitigate the material weakness. Establish and maintain metrics documentation to assess progress and track improvements in all component activities over time. Conduct an annual evaluation to revalidate compliance. (Planned implementation date of July 2011) • 1-6-17 – Disaster Recovery Plans: Develop and maintain Information Technology contingency plans associated with general support systems to include all components that support critical applications. Establish and maintain data and processing backup-recovery capability. Ensure maximum allowable outage times meet the recovery time objectives of the applications being supported. (Planned implementation date of December 2010) • 1-6-19 – Technical Assessment: Perform annual system risk assessments. Develop a true redundancy/resilience analysis. Based on the critical business processes, develop a site-based restoration vulnerability analysis. Create a Recovery Point Objective and Recovery Time Objective analysis and gain concurrence from both the business operating divisions and the Modernization and Information Technology Services organizations. Incorporate a technical assessment tool that will provide an infrastructure impact analysis in the event of a disaster. Implement backup-recovery capabilities to meet application maximum allowable outages and recovery time objectives of all Information Technology systems supporting the critical business processes. (Planned implementation date of July 2011) • 1-6-20 – Metrics: Establish and maintain metrics to assess progress and track improvements in all component activities over time. Successful operation of the policy, procedures, and plans for component activities for at least two quarters. Annual FISMA testing will revalidate compliance. (Planned implementation date of December 2011)
Comments:		

S10/S11: Contractor Systems/Financial Audit

Status of Agency Program to Oversee Contractor Systems [check one]		a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities of the Agency obtains sufficient assurance that security controls of systems operated by contractors or others on its behalf are effectively implemented and comply with Federal and Agency guidelines. 2. A complete inventory of systems operated on the Agency's behalf by contractors or other entities. 3. The inventory identifies interfaces between these systems and Agency-operated systems. 4. The Agency requires agreements (MOUs, Interconnect Service Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates. 5. The inventory, including interfaces, is updated at least annually. 6. Systems that are owned or operated by contractors or entities are subject to and generally meet NIST's and OMB's FISMA requirements.
	✓	b. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. However, the Agency needs to make significant improvements as noted below.
		c. The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities.
10a.If (b) checked above, check areas that need significant improvement:		10a(1) Policies to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed.
		10a(2) Procedures to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed or consistently implemented.
	✓	10a(3) The inventory of systems owned or operated by contractors or other entities is not sufficiently complete.
		10a(4) The inventory does not identify interfaces between contractor/ entity-operated systems to Agency-owned and operated systems.
		10a(5) The inventory of contractor/entity-operated systems, including interfaces, is not updated at least annually.
		10a(6) Systems owned or operated by contractors and entities are not subject to NIST's and OMB's FISMA requirements (e.g., certification and accreditation requirements).
		10a(7) Systems owned or operated by contractors and entities do not meet NIST's and OMB's FISMA requirements (e.g., certification and accreditation requirements).
		10a(8) Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained.
		10a(9) Other.
		Explanation for Other:

<table>
<tr><td colspan="2">Comments:

10a(3): The IRS was unable to provide us with a definitive inventory of contractor managed systems and agreed that this inventory required improvement. In May 2010, the TIGTA reported[17] that current processes were not effective at identifying all contractors who receive IRS taxpayer data and therefore are subject to required security reviews. The IRS agreed with our finding and has implemented an automated mechanism to identify all contractors that have access to sensitive data. This information will be available to target sites for security reviews during the Fiscal Year 2012 review cycle. The IRS stated it will also use this information to determine which of these meet the definition of a contractor system. In addition, where contracts may not fall into the definition of a contract system, the IRS is working towards developing new contract language to address security requirements and to potentially provide these contractors with IRS-configured laptops to help enforce security policy.</td></tr>
<tr><td>11. Financial Audit</td><td>11a. For the latest Financial Audit Report issued for the Agency, please provide the date of the report and indicate whether there was a material weakness or reportable condition concerning information security.</td></tr>
<tr><td></td><td>Input for 11a:

In March 2010, the GAO reported[18] newly identified and unresolved information security control weaknesses in key financial and tax processing systems continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information. Until these control weaknesses and program deficiencies are corrected, the IRS remains unnecessarily vulnerable to insider threats related to the unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as the disruption of system operations and services. The new and unresolved weaknesses and deficiencies at the IRS were the basis for the GAO's determination that the IRS had a material weakness in internal controls over financial reporting related to information security in Fiscal Year 2009.</td></tr>
</table>

[17] *Taxpayer Data Used at Contractor Facilities May Be at Risk for Unauthorized Access or Disclosure* (Reference Number 2010-20-051, dated May 18, 2010).
[18] *INFORMATION SECURITY: IRS Needs to Continue to Address Significant Weaknesses* (GAO-10-355, dated March 2010).

Appendix II

Treasury Inspector General for Tax Administration Information Technology Security Reports Issued During the 2010 Evaluation Period

1. *Computer System Access Controls Over Contractors Need to Be Improved* (Reference Number 2009-20-108, dated July 24, 2009).
2. *Customer Account Data Engine Release 4 Includes Most Planned Capabilities and Security Requirements for Processing Individual Tax Account Information* (Reference Number 2009-20-100, dated August 28, 2009).
3. *Significant Improvements Have Been Made to Protect Sensitive Data on Laptop Computers and Other Portable Electronic Media Devices* (Reference Number 2009-20-120, dated August 31, 2009).
4. *Progress Has Been Made, but Additional Steps Are Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses* (Reference Number 2009-20-119, dated September 9, 2009).
5. *While Effective Actions Have Been Taken to Address Previously Reported Weaknesses in the Protection of Federal Tax Information at State Government Agencies, Additional Improvements Are Needed* (Reference Number 2010-20-003, dated November 10, 2009).
6. *Additional Security Controls Are Needed to Protect the Automated Collection System* (Reference Number 2010-20-028, dated March 30, 2010).
7. *Additional Security Is Needed for Access to the Registered User Portal* (Reference Number 2010-20-027, dated March 31, 2010).
8. *Taxpayer Data Used at Contractor Facilities May Be at Risk for Unauthorized Access or Disclosure* (Reference Number 2010-20-051, dated May 18, 2010).
9. *Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement* (Reference Number 2010-20-041, dated May 26, 2010).
10. *Implementation of General Support System Security Controls Needs Improvement to Protect Taxpayer Data* (Reference Number 2010-20-063, dated June 7, 2010).

Appendix III

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Joan Bonomi, Senior Auditor
Richard Borst, Senior Auditor
Bret Hunter, Senior Auditor
Louis Lee, Senior Auditor
Larry Reimer, Senior Auditor
Frank O'Connor, Auditor
Victor Taylor, Auditor

Appendix IV

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
Liaison: Chief Technology Officer OS:CTO