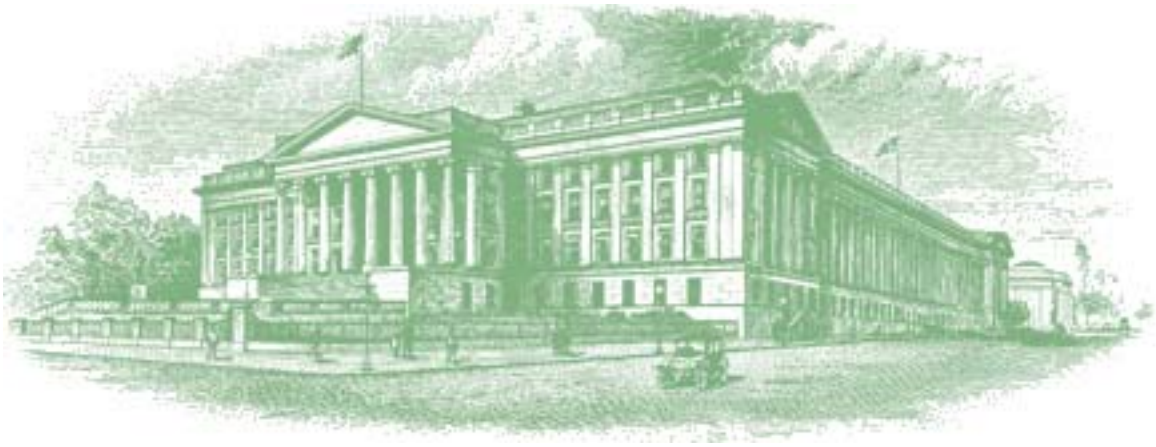
Evaluation Report



EVALUATION REPORT

INFORMATION TECHNOLOGY: The Department of the Treasury Federal Information Security Management Act Fiscal Year 2009 Evaluation (OIG-CA-10-003)

November 13, 2009

Office of Inspector General

Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

November 13, 2009

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

MICHAEL DUFFY
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 2009 Evaluation

I am pleased to transmit the following reports:

- Federal Information Security Management Act Fiscal Year 2009 Evaluation–November 13, 2009
- Treasury Inspector General for Tax Administration (TIGTA)–Federal Information Security Management Act Report for Fiscal Year 2009, Audit #200920010, October 27, 2009

The Federal Information Security Management Act (FISMA) of 2002 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 public accounting firm, to perform the FISMA evaluation of Treasury's Non-Internal Revenue Service (IRS) unclassified systems. Attachment 1 contains the KPMG report and our Office of Management and Budget (OMB) submission, which incorporates the responses of TIGTA as well. Attachment 2 contains TIGTA's evaluation of FISMA compliance for Treasury's IRS systems.[1]

[1] 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.

Based on the results reported by KPMG and TIGTA, we determined that Treasury's information security program is in place and is generally consistent with FISMA. However, the KPMG evaluation of Treasury's non-IRS unclassified systems 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 (NIST) standards and guidelines and FISMA requirements. Specifically, KPMG reported that:

1. NIST Federal Information Processing Standard 200 minimum security control baselines were not sufficiently tested or implemented (repeat finding)
2. Breach notification policy required by OMB Memorandum 07-16 has not been finalized and issued (repeat finding)
3. The Departmental Offices Federal Desktop Core Configuration image is not fully implemented (repeat finding)
4. The Bureau of Public Debt (BPD) is not using a Security Content Automation Protocol validated tool
5. Financial Management Service (FMS) Plan of Action and Milestone estimate to completion dates and milestones were not consistently updated in accordance with FMS policy
6. Frequency of vulnerability assessment scanning at BPD is not in line with bureau and Treasury policy
7. E-authentication risk assessment was not performed at the Financial Crimes Enforcement Network.

TIGTA reported that IRS had made steady progress in complying with FISMA requirements. TIGTA also found significant improvements in IRS information technology contingency plan testing and additional improvements in annual security controls testing, which were identified as areas needing improvement in its 2008 FISMA evaluation. TIGTA noted that IRS still needs to take action in the areas of certification and accreditation, and configuration management.

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 Audits, at (202) 927-5768. For questions pertaining to the TIGTA FISMA evaluation, please contact Michael R. Phillips, Deputy Inspector General for Audit, at (202) 622-6510.

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 2009 Evaluation,
November 13, 2009

The Department of the Treasury
Federal Information Security Management Act
Fiscal Year 2009 Evaluation

November 13, 2009

The Department of the Treasury
Federal Information Security Management Act Fiscal Year 2009 Evaluation

Table of Contents

FISMA Evaluation Report

Appendices

Executive Summary

This report presents the results of the evaluation conducted to address the objectives relative to the Fiscal Year (FY) 2009 Federal Information Security Management Act of 2002 (FISMA) of the 12 non-Internal Revenue Service (IRS) bureaus and offices [1] of the United States Department of the Treasury (Treasury). The IRS was not included within the scope of this FISMA evaluation. The Treasury Inspector General for Tax Administration (TIGTA) performed the FISMA evaluation of the IRS. As part of this FISMA evaluation, we only incorporated the results of the TIGTA FISMA evaluation of the IRS into the Office of Management and Budget (OMB) FY 2009 FISMA Reporting Template (see Appendix I).

This evaluation was conducted in accordance with the Council of Inspectors General on Integrity and Efficiency – Quality Standards for Inspections and the General Standards contained within the *Generally Accepted Government Auditing Standards* (GAGAS), issued by the Comptroller General of the United States.

The objectives of this evaluation were to determine, as of June 30, 2009, whether non-IRS Treasury bureaus had implemented:

- An information security program, consisting of plans, policies, procedures, and security controls, consistent with FISMA[2]
- The security control catalog contained in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 2 (Rev. 2), *Recommended Security Controls for Federal Information Systems*.[3]

Our evaluation was performed during the period of March 23, 2009 through October 7, 2009.

To accomplish our objectives, we evaluated controls in accordance to applicable legislation, Presidential directives, OMB policy, and NIST standards and guidelines. We reviewed the Treasury information security program from both a Department-level perspective for Treasury-wide program level controls and Bureau-level implementation perspective, including an in-depth assessment of the implementation of selected security control catalog outlined in NIST SP 800-53 Rev. 2. We utilized the assessment guidance in NIST SP 800-53A as our security control assessment methodology. We considered each objective above to reach conclusions with regard to the Treasury's information security program and practices.

During the FY 2009 FISMA Evaluation, we noted that the 12 non-IRS Treasury bureaus and offices have made progress in improving information security controls and practices.[4] Following our FY 2008 FISMA

[1] The Treasury is comprised of 14 bureaus and offices. The scope of this evaluation excluded the IRS. Additionally, while the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) is one (1) of the 14 Treasury bureaus and offices and is considered a non-IRS office for purposes of this report; information technology assets and responsibilities are managed by the Treasury Departmental Offices. Thus, the SIGTARP is considered a component of the Treasury Departmental Offices for FISMA reporting purposes. The 14 bureaus and offices of the Treasury are described on page 5 of this report.

[2] This objective includes the completion of the OMB *FY 2009 FISMA Reporting Template for IGs*, which is presented in Appendix I of this report.

[3] The conclusion for this objective is based on (five) 5 of the 18 systems selected in the representative subset of Treasury systems with a NIST Federal Information Processing Standard (FIPS) 199 system impact level of Moderate.

[4] The FISMA evaluation of the IRS is performed by TIGTA.

audit[5], Treasury has continued to strengthen its inventory reporting processes by more effectively using the Trusted Agent FISMA (TAF) system[6] to serve as the consolidated FISMA inventory system of record for the Treasury. In addition, Treasury has implemented a training tool to facilitate the uniform delivery of security awareness training and specialized security training. As of the close of fieldwork, 11 of the 12 non-IRS bureaus and offices were using this tool[7]. This tool also has mechanisms to allow bureau-level Chief Information Officer (CIO) and Treasury Office of the Chief Information Officer (OCIO) Cyber Security Program personnel to track compliance with Information Technology (IT) training requirements. Lastly, Treasury continues to implement NIST SP 800-70 compliant secure configurations baselines across all non-Federal Desktop Core Configuration (FDCC) platforms.

In addition, we noted that eight (8) of the 11 findings reported during the FY 2008 FISMA Performance Audit have been resolved and one (1) finding was partially closed.

However, we also noted areas needing improvement where Treasury should take additional steps to ensure that its information security risk management program and practices fully comply with applicable NIST standards and guidelines and FISMA requirements. Specifically,

1. **NIST Federal Information Processing Standard (FIPS) 200 Minimum Security Control Baselines Were Not Sufficiently Tested or Implemented (Repeat Finding).** Treasury has continued to make progress in addressing information security risk management requirements of FISMA and NIST, including the certification and accreditation of information systems and the implementation of minimum security controls outlined in NIST FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems* and NIST SP 800-53 Rev. 2. The OCIO Cyber Security Program has built a program to oversee the certification and accreditation efforts of all Treasury bureaus. In addition, the majority of bureaus evaluated have made progress in implementing the NIST SP 800-53 Rev. 2 minimum security control baseline within systems under their control. However, we noted that the minimum security controls required by NIST FIPS 200 were not tested or fully implemented for three (3) systems within our representative subset of non-IRS Treasury information systems and one (1) system previously identified during the FY 2008 FISMA Audit. Specifically, during the FY 2008 audit we noted that the Bureau of Engraving and Printing (BEP), the Office of Thrift Supervision (OTS), and the Alcohol and Tobacco Tax and Trade Bureau (TTB) had not sufficiently tested or implemented the NIST SP 800-53 Rev. 2 security control baseline for systems under their control. At the conclusion of the FY 2009 FISMA Evaluation, the systems under the control of OTS within our scope did not have a sufficiently implemented or tested security control baseline. We also noted that FMS has not sufficiently tested the NIST SP 800-53 Rev. 2 security control baseline for two (2) systems under their control.

2. **Breach Notification Policy Required by OMB Memorandum 07-16 has not been Finalized and Issued (Repeat Finding).** OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* issued on May 22, 2007, required that policy be developed for the Personally Identifiable Information (PII) breach notifications. OMB Memorandum 07-16 required that this policy be issued within 120 days after the date of the memorandum,

[5] In FY 2008 the engagement was conducted as a performance audit and the FY 2009 engagement was performed in accordance with the Council of Inspectors General on Integrity and Efficiency – Quality Standards for Inspections.

[6] TAF is an enterprise tool for aggregating data reported by Treasury bureaus to gauge how well the Department is complying with key information security practices and controls.

[7] Only the Office of the Comptroller of Currency (OCC) was not using the Treasury training tool.

September 22, 2007. To date, Treasury Directive (TD) 25-08, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, has not been finalized and issued.

3. **The Departmental Offices (DO) FDCC Image is Not Fully Implemented (Repeat Finding).** At the conclusion of the FY 2008 FISMA Audit, we noted that four (4) of the 12 non-IRS Treasury bureaus and offices, DO, the Financial Crimes Enforcement Network (FinCEN), the OIG, and OTS, had not fully implemented their FDCC baselines. As of the conclusion of the FY 2009 FISMA Evaluation, we noted that only DO still had not implemented the FDCC secure configuration baseline on all workstations in accordance with Treasury Chief information Officer Memorandum 07-14, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, and OMB Memorandum 07-11, *Implementation of Common Security Configurations for IT Systems Using Windows XP or Vista*.

4. **The Bureau of Public Debt (BPD) is Not Using a Security Content Automation Protocol (SCAP) Validated Tool.** As of the conclusion of the FY 2009 FISMA reporting period, BPD was not using a SCAP validated tool to scan the BPD FDCC secure configuration baseline in accordance with OMB Memorandum 08-22, *Guidance on the Federal Desktop Core Configuration*.

5. **FMS Plan of Action and Milestone (POA&M) Estimate to Completion Dates and Milestones Were Not Consistently Updated in Accordance with FMS Policy.** Discrepancies were identified in the management of the POA&M weaknesses for three (3) of five (5) systems selected at FMS. Specifically, 11 out of 15 weaknesses sampled across these systems had open weaknesses listed with a status of delayed and were past estimated completion dates.

6. **Frequency of Vulnerability Assessment Scanning at BPD is not In Line with Bureau and Treasury Policy.** The frequency of vulnerability scanning over a system selected at BPD is not in compliance with Treasury-wide and BPD policy and the control requirements outlined in the system's security plan. Currently, this system is scanned for vulnerabilities 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, while BPD bureau-wide IT policy is semiannually.

7. **E-Authentication Risk Assessment Was Not Performed at the Financial Crimes Enforcement Network (FinCEN).** Treasury has established policies requiring an E-Authentication Risk Assessment for information systems with Web-based identification and authentication mechanisms. We identified one (1) system within our representative subset of non-IRS Treasury systems at FinCEN as having a Web-based identification and authentication mechanism; however, an E-Authentication Risk Assessment was not performed.

Overall, while continued improvements are still needed across five (5) of 12 non-IRS bureaus and offices, we determined that an information security program is in place and is generally consistent with FISMA. All of our findings are included in the results section of this report, which warrants management attention and corrective actions. Management concurs with all reported findings and recommendations. The OCIO's written response to our draft report, dated November 2, 2009, is included within this report.

Background

On December 17, 2002, the President signed into law H.R. 2458, the E-Government Act of 2002 (Public Law 107-347). Title III of the E-Government Act of 2002, commonly referred to as FISMA, focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA assigns specific responsibilities to agency heads and Inspectors Generals (IG) and is supported by security policy promulgated through OMB and risk-based standards and guidelines published by NIST.

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. FISMA directs federal agencies to report annually to the OMB Director, Comptroller General, and selected Congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG.

In support of agency responsibilities, OMB regularly issues policies through annual reporting instructions and other guidelines for agencies to follow in meeting FISMA annual reporting requirements. Additionally, in response to the FISMA mandate and OMB policy, NIST developed standards and guidelines as part of a comprehensive risk management framework to assist agencies in establishing an information security management program. This risk management framework is designed to help agencies categorize information and systems, define minimum-security baselines, test security controls, authorize systems into production, and perform monitoring activities. This includes the NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, issued in February 2004, as the first of two (2) mandatory security standards required by FISMA. NIST FIPS 199 establishes security categories for federal agencies to use in categorizing information and information systems based on the potential impact associated with the loss of confidentiality, integrity, or availability on an agency mission or individual.

NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is the second of the mandatory security standards developed in response to FISMA and provides direction to agencies in determining the minimum "foundational" level of security controls to select for protecting the confidentiality, integrity, and availability of information and systems. Specifically, NIST FIPS 200 states that selected set of security controls must include one (1) of three (3) appropriately tailored security control baselines from NIST SP 800-53 Rev. 2, which are associated with the designated impact levels of the organizational information systems as determined during the security categorization process. NIST SP 800-53 Rev. 2 features 17 control families organized into management, operational, and technical control areas for protecting federal information and information systems. In accordance with security requirements in NIST FIPS 200, organizations must employ all security controls in the respective security control baselines unless specific exceptions are allowed based on the tailoring guidance provided in NIST SP 800-53 Rev. 2. This includes (i) selecting an initial set of baseline security controls based on a NIST FIPS 199 worst-case, impact analysis; (ii) tailoring the baseline security controls; and (iii) supplementing the security controls, as necessary, based on an organizational assessment of risk. As a companion to

NIST SP 800-53 Rev. 2, NIST in July 2008 released SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, which covers both the security control assessment and continuous monitoring steps in the Risk Management Framework and provides guidance on the security assessment process.

Treasury Bureaus and Offices

Treasury is comprised of 14 operating bureaus and offices, including:

- **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.
- **Bureau of Engraving and Printing (BEP) –** Designs and manufactures U.S. (paper) currency, securities, and other official certificates and awards.
- **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.
- **Community Development Financial Institution (CDFI) Fund –** Created to expand the availability of credit, investment capital, and financial services in distressed urban and rural communities.
- **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.
- **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.
- **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.
- **Internal Revenue Service (IRS) –** Responsible for determining, assessing, and collecting internal revenue in the United States.
- **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.
- **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.
- **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.
- **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.
- **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. 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.
- **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.

Treasury Information Security Management and Program

Treasury OCIO

The Treasury CIO is responsible for providing Treasury-wide leadership and direction for all areas of information and technology management, as well as the oversight of a number of IT programs. Among these programs is Cyber Security, which has responsibility for the implementation and management of Treasury-wide IT security programs and practices. Through its mission, the Treasury 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:

- Cyber Security Policy and Program Performance
- Cyber Security FISMA Performance and Technical Review
- Vulnerability Analysis
- Configuration and Planning
- Cyber Critical Infrastructure Protection (CIP)
- Treasury Computer Security Incident Response Capability (TCSIRC)
- Cyber Security Sub-Council (CSS) of the Treasury CIO Council.

The Treasury CIO has tasked the Associate CIO 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 OCIO

Bureau OCIO organizations are managed by a bureau CIO. The bureau CIOs first have the responsibility of managing the IT security program for the bureau, as well as advising the bureau head on significant issues related to the bureau IT security program. Bureau 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 are tasked by the bureau 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 chaired by the ACIOCS. 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 IT security-related information sharing 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.

Treasury Privacy and Data Protection Program

Treasury established a department-wide privacy program to protect the PII it manages from unauthorized use, access, disclosure, or sharing and to safeguard associated information systems from unauthorized access, modification, disruption, or destruction. Key components of the Treasury's privacy program include, but are not limited to:

- The role of Chief Privacy Officer (CPO) and Senior Agency Official for Privacy is held by the Assistant Secretary for Management/Chief Financial Officer.

- The Office of Privacy and Treasury Records (OPTR) was established on March 24, 2008 as the program management office that supports the Treasury CPO in developing and implementing privacy requirements including policies and procedures for managing and protecting PII. OPTR also provides privacy and data protection programs oversight of all Treasury bureaus and offices in carrying out directives and policies developed by OPTR. Additionally, OPTR is responsible for establishing a privacy awareness program disseminated to bureaus regarding Treasury employee privacy responsibilities. OPTR includes the Office of Privacy and Civil Liberties, Office of Disclosure Services, Treasury Records, Treasury Library, and the Orders and Directives Program.

- Each of the 14 Treasury bureaus and offices has also established a bureau privacy officer. The role of the bureau privacy officer is to act as a liaison between the bureau's system owners and the OPTR and the CPO to ensure that privacy and data protection programs are operating effectively at the bureau level. This includes performance of Privacy Threshold Analysis and Privacy Impact Assessments (PIA) on all information systems. Bureau privacy officers work with the system owners to analyze the data being processed in the system and make a determination if the data contains PII.

Objective, Scope, and Methodology

The objectives of our evaluation were to determine, as of June 30, 2009, whether non-IRS Treasury bureaus had implemented:

- An information security program, consisting of plans, policies, procedures, and security controls consistent with FISMA[8]
- The security controls catalog contained in the NIST SP 800-53 Rev. 2.[9]

To accomplish our objectives, we evaluated controls in accordance with applicable legislation, Presidential directives, OMB policy, and NIST standards and guidelines. We reviewed the Treasury information security program from both the Department-level perspective for Treasury-wide program level controls and Bureau-level implementation perspective, including NIST SP 800-53 Rev. 2 minimum security control baselines established by NIST FIPS 200. We considered each area above to reach conclusions with regard to Treasury's information security program and practices.

Department Level

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/NIST standards, as well as guidelines developed in response to FISMA. This included program controls applicable to information security governance, security and contingency planning, certification and accreditation, incident response, configuration management, and security awareness and training.

Bureau Level

As required by FISMA, we also performed tests for a representative subset of 18 information systems out of a total population of 121 non-IRS major applications and general support systems as of April 2, 2009 to determine whether bureaus were effective in implementing Treasury's security program in meeting minimum security standards to protect information and information systems (see Appendix II detailing our system selection approach). The subset of systems encompassed systems managed and operated by 12 of 14 Treasury bureaus and offices, excluding the IRS.

A key component of assessing controls for the representative subset of systems was to assess implementation of minimum security control requirements per guidance provided from the NIST SP 800-53 Rev. 2 for a selection of security controls across five (5) of the 18 systems within the representative subset of non-IRS Treasury information systems selected for FISMA reporting. As shown in Table 1, NIST SP 800-53 Rev. 2 features 17 control families that are organized into management, operational, and technical control areas for protecting federal information and information systems.

[8] This objective includes the completion of the OMB FY 2009 FISMA Reporting Template for IGs, which is presented in Appendix I of this report.

[9] The conclusion for this objective is based on (five) 5 of the 18 systems selected in the representative subset of Treasury systems with a NIST FIPS 199 system impact level of Moderate.

Table 1: Security Control Classes and Families[10]

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

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

- Highly volatile controls that have the potential to affect a significant number of information systems, such as common controls or those critical to a specific system which are likely to change over time.
- Specific high-risk controls that are crucial to the protection of a system were considered for selection as part of the testing requirement. These are not necessarily the same as highly volatile controls and may or may not be POA&M items.
- Testing of a system's security-relevant changes that occur out of the certification and accreditation cycle but do not necessarily constitute a major change necessitating a new certification and accreditation.

Our methodology for the assessment of the selected controls was based on the recommended guidance in NIST SP 800-53A.

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 12 non-IRS bureaus and offices. We also evaluated Treasury and bureaus' policies, procedures, and guidelines. Lastly, we evaluated selected security-related documents and files, including certification and accreditation packages, configuration assessment results, IT service contracts, training records, and strategic and annual performance plans.

[10] Source: NIST SP 800-53 Rev. 2

We performed our evaluation at Treasury's headquarters offices in Washington, D.C., and bureau locations in Washington, D.C.; Hyattsville, Maryland; McLean, Virginia; Parkersburg, West Virginia; and Richmond, Virginia during the period of March 23, 2009 through November 2, 2009. During our evaluation, we met with Treasury management to discuss our preliminary conclusions. This evaluation was conducted in accordance with the Council of Inspectors General on Integrity and Efficiency – Quality Standards for Inspections and the General Standards contained within GAGAS, issued by the Comptroller General of the United States.

Applicable Criteria

Our approach to this FISMA evaluation is based on federal information security criteria developed by NIST and OMB. NIST SPs provide guidelines that are considered essential to the development and implementation of agencies' security programs.[11] The following is a listing of the criteria used in the performance of the FY 2009 FISMA Evaluation:

- OMB Circular A-130, *Management of Federal Information Resources*
- NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
- NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP:
  - 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*
  - 800-18 Rev. 1, *Guide for Developing Security Plans for Information. Technology System*
  - 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 Rev. 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*

[11] 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 (specifically in the 800 series) in how agencies apply the guidance. However, NIST FIPS are mandatory. Unless specified by additional implementing policy by OMB, guidance documents published by NIST generally allow agencies latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable and compliant with the guidance.

- 08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)*
- 09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*

Results

During our FY 2009 FISMA evaluation, we noted that the 12 non-IRS Treasury bureaus and offices continue to make progress in improving information security controls and practices.[12] Following our FY 2008 FISMA Audit, Treasury has continued to strengthen its inventory reporting processes by more effectively using the TAF system to serve as the consolidated FISMA inventory system of record for the Treasury.[13] In addition, Treasury has implemented a Treasury-wide training tool to facilitate the uniform delivery of security awareness training and specialized security training. As of the close of fieldwork, 11 of the 12 non-IRS bureaus and offices were using this tool[14]. This tool also has mechanisms to allow bureau-level CIOs and Treasury OCIO Cyber Security Program personnel to track compliance with IT training requirements. Lastly, Treasury continues to implement NIST SP 800-70 compliant secure configurations baselines across all non-FDCC platforms. However, based on our FY 2009 FISMA evaluation, we noted seven (7) areas needing improvement. These areas are:

1. NIST FIPS 200 minimum security control baselines not sufficiently tested or implemented.
2. Breach notification policy required by OMB Memorandum 07-16 has not been not finalized and issued.
3. DO FDCC image not fully implemented.
4. BPD is not using a security content automation protocol validated tool.
5. FMS POA&M estimate to completion dates and milestones were not consistently updated in accordance with FMS policy.
6. Frequency of Vulnerability Assessment Scanning at BPD is not In Line with Bureau and Treasury Policy.
7. E-Authentication risk assessment was not performed at FinCEN.

Treasury should take additional steps to ensure that its information security risk management program and practices fully comply with applicable NIST standards and guidelines, and FISMA requirements.

[12] The FISMA evaluation of the IRS is performed by TIGTA.
[13] TAF is an enterprise tool for aggregating data reported by Treasury bureaus to gauge how well the Department is complying with key information security practices and controls.
[14] Only the Office of the Comptroller of Currency (OCC) was not using the Treasury training tool.

Findings

1. NIST FIPS 200 Minimum Security Control Baselines Not Sufficiently Tested or Implemented (Repeat Finding)

Treasury has continued to make progress in addressing information security risk management requirements of FISMA and NIST, including the certification and accreditation of information systems and the implementation of minimum security controls outlined in NIST FIPS 200 and NIST SP 800-53 Rev. 2. The majority of bureaus evaluated have made progress in implementing the NIST SP 800-53 Rev. 2 minimum security control baseline within systems under their controls. In addition, the OCIO Cyber Security Program has built a program to oversee the certification and accreditation efforts of all Treasury bureaus. However, we noted that the minimum security controls required by NIST FIPS 200 were not tested or fully implemented for three systems within our representative subset of non-IRS Treasury information systems and one system previously identified during the FY 2008 FISMA Audit. Specifically, for the three (3) information systems reviewed and one system that was identified to have a deficiency in our FY 2008 FISMA Audit report, we noted:

- Two (2) systems at FMS operating under a full authority to operate at the conclusion of the FY 2009 FISMA reporting period[15] were identified as having incomplete testing over the full NIST SP 800-53 Rev. 2 minimum security control baselines. In addition, a full risk assessment, per NIST SP 800-30, was not performed over either system as part of these efforts. Due to limited resource and time constraints, FMS made a risk-based decision to give priority to the assessment of the NIST SP 800-53 Rev. 2 technical security control families during the recertification of each system. FMS management decided to base the initial reaccreditation on the results of these technical testing activities alone due to the overarching need to keep these systems operational. The certification letters of both systems documented this scope limitation. FMS management then intended to continue with the full recertification and accreditation of each system, with the goal of reissuing a full authority to operate during the FY 2010 FISMA reporting cycle. FMS created a weakness in the POA&M for one (1) system to complete the testing of the NIST SP 800-53 Rev. 2 management and operational security control families by September 30, 2009; however, a POA&M weakness was not created for the second system. The complete Security Assessment Report for this second system, which included a risk assessment and testing of all management, operational, and technical controls in the NIST SP 800-53 Rev. 2 security baseline for a system with a FIPS 199 system impact level of High, had not been finalized as of the conclusion of fieldwork. FMS was planning to reissue a full authority to operate for this system once the Security Assessment Report had been completed, as well as complete the full recertification of the first system by September 30, 2009.

  By not performing a risk assessment, FMS management may be unaware of the likelihood and impact of the threats and related vulnerabilities posed to FMS information and information systems. Subsequently, FMS may not have the appropriate controls in place to mitigate these threats and related vulnerabilities.

  By not fully testing the minimum security control baseline according to NIST FIPS 200 and NIST SP 800-53 Rev. 2, the confidentiality, integrity, and availability of sensitive information

[15] The FY 2009 FISMA reporting period is July 1, 2008 through June 30, 2009.

systems that support the mission of the FMS under the control of both systems are susceptible to compromise.

- **(Repeat Finding)** During FY 2008, OTS reorganized the FISMA system inventory into functional IT units. The authorities to operate for each system expired during the FY 2007 FISMA reporting period. OTS did not re-perform the certification and accreditation of each system due to a planned process to redefine the FISMA system inventory, which occurred in the FY 2008 FISMA reporting period.

  Because of this reorganization and the subsequent certification and accreditation efforts, OTS management noted that the full NIST FIPS 200 and NIST SP 800-53 Rev. 2 minimum security control baseline had not been implemented for one system selected as part of the FY 2008 FISMA audit representative subset of non-IRS Treasury systems. Specifically, the security test and evaluation of this system identified that several security controls outlined in the Moderate baseline were not in place and an Interim Authority to Operate (IATO) was issued on June 27, 2008 for a period of 180 days. According to OTS management, the designated approving authority assessed the risks presented as part of the certification and accreditation process, then granted this system an IATO until December 31, 2008. During the FY 2009 FISMA Evaluation, many of these security weaknesses in this system remained open, causing OTS management to issue an extension to the IATO on June 25, 2009 to September 25, 2009.

  As part of the FY 2009 FISMA Evaluation, a second OTS system was selected for this FY 2009 FISMA Evaluation. This second system inherits a number of security controls from the system selected as part of the FY 2008 FISMA Audit. Because of this, the second system also remained in an IATO status as of the end of the FY 2009 FISMA reporting period. This second system was also issued an extension of the IATO on June 25, 2009 to September 25, 2009 by OTS management.

  At the conclusion of the FY 2009 FISMA reporting period, both systems identified above were not fully accredited. OTS is currently in the process of resolving the identified security weaknesses with the intent of obtaining a full authority to operate for both systems early in the FY 2010 FISMA reporting period. OTS management had developed a POA&M to track the IT security weaknesses identified during the certification and accreditation process. However, neither system was fully accredited at the conclusion of the FY 2009 FISMA reporting period.

  The confidentiality, integrity, and availability of sensitive or personally identifiable information contained within either OTS systems could be susceptible to compromise when a minimum security control baseline has not been fully implemented.

We recommend that FMS management:

1. Complete the full certification and accreditation of the first FMS system identified above by the estimated completion date being tracked in the POA&M.

2. Finalize the security assessment reporting process and reissue the full authority to operate for the second FMS system identified above.

We recommend that OTS management:

3. Continue with plans to resolve the one (1) remaining high-risk weakness identified during the certification and accreditation process and achieve a full authority to operate during the FY 2010 FISMA reporting period.

2. Breach Notification Policy Required by OMB Memorandum 07-16 has not been not Finalized and Issued (Repeat Finding)

OMB Memorandum 07-16, issued on May 22, 2007, required that a policy be developed for the PII breach notifications. OMB Memorandum 07-16 required that this policy be issued within 120 days after the date of the memorandum, September 22, 2007. To date, TD 25-08 has not been finalized. According to the OPTR management, several major rewrites of TD 25-08 occurred while the document was in the clearance process, causing delays in implementation. At the conclusion of our FY 2009 FISMA Evaluation fieldwork, OPTR management stated that TD 25-08 has been re-written and is awaiting formal clearance process. The planned implementation date is December 31, 2009.

Without formal policy related to the collection, use, sharing, disclosure, transfer, and storage of PII in place at the Treasury, information in identifiable form may not be adequately protected.

The recommendation remains open from FY 2008.

3. DO FDCC Image Not Fully Implemented

At the conclusion of the FY 2008 FISMA Audit, we noted that four (4) of the 12 non-IRS Treasury bureaus and offices, DO, the Financial Crimes Enforcement Network (FinCEN), the OIG, and OTS, had not fully implemented their FDCC baselines. As of the conclusion of the FY 2009 FISMA Evaluation, we noted that only DO still had not implemented the FDCC secure configuration baseline on all workstations in accordance with Treasury Chief information Officer Memorandum 07-14, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, and OMB Memorandum 07-11, *Implementation of Common Security Configurations for IT Systems Using Windows XP or Vista*.

DO IT management stated that DO is manually applying their FDCC image to all headquarters workstations to provide end users training on the new FDCC desktop configurations. As of the end of the FY 2009 FISMA reporting period, DO has implemented their FDCC image on about 80% of headquarters workstations and expects to be completed by November 15, 2009. DO IT management is tracking the progress of this weakness via a POA&M weakness.

By not applying the FDCC secure baseline configuration requirements for Microsoft® Windows® XP, DO information systems are under increased risk of exposure relative to the confidentiality, integrity, and availability of sensitive information and information systems controlled by these operating systems.

We recommend that DO management:

4. Fully implement the DO FDCC secure baseline configurations on all headquarters end-user workstations by the due date outlined in the POA&M.

4. BPD Not Using a Security Content Automation Protocol Validated Tool

As of the conclusion of the FY 2009 FISMA reporting period, BPD was not using a SCAP validated tool to scan the BPD FDCC secure configuration baseline in accordance with OMB Memorandum 08-22, which requires that agencies use SCAP tools to scan FDCC configurations and approved configuration deviations. BPD had been using a freeware version of a SCAP validated tool. However, BPD management was not satisfied with the quality of the results the tool provided and discontinued using it. BPD then began manually validating their FDCC image against the NIST FDCC secure configuration baseline. BPD has since purchased a license for a second SCAP validated tool; however, as of the close of the FY 2009 FISMA reporting period this tool was not implemented.

By not using a SCAP tool to validate the implementation of the FDCC secure configuration baseline, BPD may be unable ensure continued compliance with FDCC.

We recommend that BPD management:

5. Continue with efforts to implement a SCAP-validated tool.

6. Utilize a SCAP-validated tool to monitor the BPD FDCC secure configuration baseline image.

5. FMS POA&M Estimate to Completion Dates and Milestones Were Not Consistently Updated in Accordance with FMS Policy.

Treasury has developed policies and procedures for the development and maintenance of POA&Ms. In addition, Treasury has implemented the TAF tool to serve as a central repository for POA&M weakness maintenance and tracking. Through this tool, the OCIO Cyber Security Program is also able to oversee the bureau-level management and tracking of the POA&M process and perform quality control reviews of the POA&M process. However, discrepancies in the management of the POA&M process were identified at FMS. Specifically, for three (3) of the five (5) FMS systems selected, estimate to complete dates were not consistently managed in accordance with FMS policy and TDP 85-01. Of the 15 weaknesses sampled out of a population of 222 across these three (3) FMS systems, 11 have estimate to complete dates that have passed with no actual completion date listed.

According to FMS, the System Owner and Information System Security Officer of each of these systems inadvertently neglected to update the estimate to complete date or milestones after they had passed.

By not consistently managing the estimate to complete dates and milestones being tracked on the POA&M, FMS's ability to correct IT security weaknesses in a timely manner may be impaired.

We recommend that FMS management:

7. Update the estimate to complete dates and milestones for each of the identified weaknesses to reflect the status.

8. 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.

6. Frequency of Vulnerability Assessment Scanning at BPD is not In Line with Bureau and Treasury Policy.

The frequency of vulnerability scanning over one (1) system selected at BPD is not in compliance with Treasury-wide policy and the control requirements outlined in the system's security plan. Currently, this system is scanned for vulnerabilities annually. 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, however BPD bureau-wide IT policy is semiannually. A recent vulnerability assessment performed by BPD on the infrastructure that supports this system identified potential high-risk vulnerabilities. At the time of the evaluation, BPD was performing follow-up efforts to evaluate raw scan results and determine if potential vulnerabilities were legitimate threats or false positives.

BPD IT management has not been able to dedicate the resources necessary to conduct vulnerability scans on a more frequent basis. BPD IT management has identified this as an IT security weakness and is tracking it as a weakness in the POA&M of the BPD general support system with an estimated completion date of February 1, 2010.

By not performing regular vulnerability scanning on major applications, BPD IT management may be unaware of all of the vulnerabilities present within the information system. A threat agent, either internal or external, could then compromise the vulnerabilities on these systems and affect the confidentiality, integrity, or availability of the information system and the information contained within.

We recommend that BPD management:

9. Continue follow-up efforts to resolve of all potential vulnerabilities identified during the recent vulnerability assessment.

10. Review and update internal BPD bureau-wide IT policies as appropriate.

11. Conduct vulnerability scans on at least a quarterly-basis as required by TDP 85-01.

7. E-Authentication Risk Assessment Was Not Performed at FinCEN

Treasury has established a policy requiring the performance of an E-Authentication Risk Assessment for information systems with Web-based identification and authentication mechanisms. One (1) system within our representative subset of non-IRS Treasury systems at FinCEN was identified as having Web-based identification and authentication mechanisms; however, an E-Authentication Risk Assessment was not performed. An external accreditation agent informed FinCEN that this system did not require an E-Authentication Risk Assessment since it did not process financial transactions, even though the system has a web-based authentication mechanism. OMB Memorandum 04-04 requires that an E-Authentication Risk Assessment be performed on any information system performing remote authentication of human users of Federal agency IT systems for the purposes of conducting government business electronically. OMB Memorandum 04-04 does not limit E-Authentication Risk Assessments to systems processing financial transactions.

By not performing an E-Authentication Risk Assessment, FinCEN may be unable to provide an appropriate level of assurance in the protection of authentication information.

We recommend that FinCEN management:

12. Perform an E-Authentication Risk Assessment for the one (1) system selected at FinCEN for the FY 2009 FISMA Evaluation.

Conclusions

As part of the FISMA evaluation of the non-IRS systems at Treasury, we assessed the effectiveness of Treasury's information security programs and practices and the implementation of the security control catalog contained in NIST SP 800-53 Rev. 2. Overall, while continued improvements are still needed across five (5) of 12 non-IRS bureaus and offices, we determined that an information security program is in place and is generally consistent with FISMA.

Management Response to Draft Report

The following is the OCIO's response to the draft FY 2009 FISMA Evaluation report, dated November 2nd, 2009.

November 2, 2009

MEMORANDUM FOR MARLA A. FREEDMAN
ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: Michael D. Duffy /s/
Deputy Assistant Secretary for Information Systems
and Chief Information Officer

Melissa Hartman /s/
Acting Deputy Assistant Secretary for Privacy and Treasury Records

SUBJECT: Management Response to Draft Evaluation Report-The Department of the Treasury Federal Information Security Management Act Fiscal Year 2009 Evaluation

Thank you for the opportunity to review and comment on the draft report entitled: "The Department of the Treasury Federal Information Security Management Act Fiscal Year 2009 Evaluation." We are pleased that the evaluation identifies no significant deficiencies or management challenges and acknowledges Treasury's continued efforts to advance its Federal Information Security Management Act (FISMA) processes. The Department agrees with all findings and recommendations.

We appreciate the Office of Inspector General's recognition of our commitment to strengthen the inventory reporting process and implement a uniform delivery of security awareness and privacy awareness training. In an effort to continuously improve the Department's information technology security program, the Office of the Chief Information Officer has implemented the Trusted Agent FISMA (TAF) Certification and Accreditation module and continued efforts to upgrade TAF, the FISMA reporting tool, which aids in the inventory reporting process.

The Office of the Deputy Assistant Secretary for Privacy and Treasury Records has strengthened its privacy program by signing Treasury Directive Publication (TD P) 25-07, "Privacy Impact Assessment Manual," providing guidance to ensure appropriate measures are followed regarding the proper use and protection of Personally Identifiable Information collected within Treasury's information systems.

We remain committed to sustaining an evolving IT security program, and providing appropriate protection of critical information throughout the Department. Should you have any questions pertaining to this response, please do not hesitate to contact Michael Duffy at 202-622-1200 or Melissa Hartman at 202-622-5710.

Attachment

MANAGEMENT RESPONSE TO TREASURY OIG DRAFT RECOMMENDATIONS

OIG Finding 1: NIST Federal Information Processing Standard 200 Minimum Security Control Baselines Were Not Sufficiently Tested or Implemented (Repeat Finding)

OIG Recommendation 1: For FMS, we recommend that management: Complete full certification and accreditation of the first FMS system identified by the estimated completion date being tracked in the POA&M.

Treasury Response: Treasury concurs with this recommendation.
FMS has completed a full Certification and Accreditation of System (C&A) 1 as identified in the findings. This action was completed by September 29, 2009 and has met the POA&M target date of September 30, 2009.

Responsible Official: Charles Simpson, FMS, Chief Information Officer

OIG Recommendation 2: For FMS, we recommend that management: Finalize the security assessment reporting process and reissue the full authority to operate for the second FMS system identified.

Treasury Response: Treasury concurs with this recommendation.
FMS has completed a full C&A of system 2 as identified in the finding. This action is complete as of September 29, 2009 and met the POA&M target date of October 31, 2009.

Responsible Official: Charles Simpson, FMS, Chief Information Officer

OIG Recommendation 3: For OTS, we recommend that management: Continue with plans to resolve the one (1) remaining high-risk weakness identified during the certification and accreditation process and achieve a full authority to operate during the FY 2010 FISMA reporting period.

Treasury Response: Treasury concurs with this recommendation.
In the FY2010 FISMA reporting period, OTS will pursue their C&A plans to resolve security weaknesses to achieve full Authority to Operate. Target completion date is December 31, 2009.

Responsible Official: Wayne Leiss, OTS, Chief Information Officer

OIG Finding 2: Breach Notification Policy Required by OMB Memorandum 07-16 has not been Finalized and Issued (Repeat Finding)

The recommendation remains open from FY 2008.

Treasury Response: Treasury concurs.

Treasury Directive (TD) 25-08, "Safeguarding Against, and Responding to, the Breach of Personally Identifiable Information (PII)," is in the final clearance stage and will be signed by December 31, 2009, in accordance with the Planned Corrective Action. This Treasury-wide policy provides guidelines for safeguarding privacy-related information as well as the process for responding to any breaches.

Responsible Official: Melissa Hartman, Acting Deputy Assistant Secretary for Office of Privacy and Treasury Records

OIG Finding 3: DO FDCC Image Not Fully Implemented

OIG Recommendation 4: For DO, we recommend that management: Fully implement the DO FDCC secure baseline configurations on all headquarters end-user workstations by the November 15, 2009 due date outlined in the POA&M.

Treasury Response: Treasury concurs with this recommendation.

In the FY2010 FISMA reporting period, DO has implemented FDCC secure configuration baselines on all headquarters end-user workstations. Target completion date is November 15, 2009.

Responsible Official: Diane Litman, Acting Associate CIO for Infrastructure Operations

OIG Finding 4: BPD Not Using a Security Content Automation Protocol Validated Tool

OIG Recommendation 5: For BPD, we recommend that management: Continue with efforts to implement a SCAP-validated tool.

Treasury Response: Treasury concurs with this recommendation.

In August 2009, a SCAP-validated tool from Tenable Security System was procured and implemented. A scan of the network was completed on September 25, 2009.

Responsible Official: Kim McCoy, BPD, Assistant Commissioner, Office of Information Technology

OIG Recommendation 6: For BPD, we recommend that management: Utilize a SCAP-validated tool to monitor the BPD FDCC secure configuration baseline image.

Treasury Response: Treasury concurs with this recommendation.
The FDCC secure baseline image will be monitored using the SCAP-validated tool on an ongoing basis to ensure compliance with the FDCC secure configuration baseline. A scan of the network was completed on September 25, 2009.

Responsible Official: Kim McCoy, BPD, Assistant Commissioner, Office of Information Technology

OIG Finding 5: **FMS POA&M Estimate to Completion Dates and Milestones Were Not Consistently Updated in Accordance with FMS Policy.**

OIG Recommendation 7: For FMS, we recommend that management: Update the estimate to complete dates and milestones for each of the identified weaknesses to reflect the status.

Treasury Response: Treasury concurs with this recommendation.
In the FY2010 FISMA reporting period, FMS will update the estimate to completion dates and milestones for each identified weakness to reflect status. Target completion date is April 30, 2010.

Responsible Official: Charles Simpson, FMS, Chief Information Officer

OIG Recommendation 8: 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.

Treasury Response: Treasury concurs with this recommendation.
FMS management will review its oversight and guidance process to ensure the FISMA process is managed in accordance with all policies and guidance published by FMS, Treasury, and OMB policy guidance. Based on this review, FMS will implement changes deemed necessary. Target completion date is April 30, 2010.

Responsible Official: Charles Simpson, FMS, Chief Information Officer

OIG Finding 6: Frequency of Vulnerability Assessment Scanning at BPD is Not In Line with Bureau and Treasury Policy.

OIG Recommendation 9: For BPD, we recommend that management: Continue follow-up efforts to resolve or dispose of all potential vulnerabilities identified during the recent vulnerability assessment.

Treasury Response: Treasury concurs with this recommendation.
In the FY2010 FISMA reporting period, BPD will continue follow-up efforts to resolve all potential vulnerabilities identified during the assessment. This will be completed by March 31, 2010.

Responsible Official: Kim McCoy, BPD, Assistant Commissioner, Office of Information Technology

OIG Recommendation 10: For BPD, we recommend that management: Review and update internal BPD bureau-wide IT policies as appropriate.

Treasury Response: Treasury concurs with this recommendation.
We are currently replacing our Information Technology Security Manual with a series of policy documentation and will rely upon the Treasury policy to define the required scanning frequency for systems. This will be completed by March 31, 2010.

Responsible Official: Kim McCoy, BPD, Assistant Commissioner, Office of Information Technology

OIG Recommendation 11: For BPD, we recommend that management: Conduct vulnerability scans on at least a quarterly-basis as required by TDP 85-01.

Treasury Response: Treasury concurs with this recommendation.
In the FY2010 FISMA reporting period, BPD will conduct required vulnerability scans of the system infrastructure in line with Treasury policy. This will be completed by March 31, 2010.

Responsible Official: Kim McCoy, BPD, Assistant Commissioner, Office of Information Technology

OIG Finding 7: E-Authentication Risk Assessment Was Not Performed at FinCEN

OIG Recommendation 12: For FinCEN we recommend that management: Perform an E-Authentication Risk Assessment for one (1) system selected at FinCEN for the FY2009 FISMA Evaluation.

Treasury Response: Treasury concurs with this recommendation.
FinCEN has mitigated this finding. FinCEN has performed and documented an E-Authentication Risk Assessment for a system that was selected for the FY2009 FISMA Evaluation, as well as documented E-Authentication Risk Assessments for all other FISMA systems. E-Authentication Risk Assessment updates were completed on August 10, 2009.

Responsible Official: Amy Taylor, FINCEN, Associate Director, Office of Information Technology and Chief Information Officer

Appendix I –Responses to the FY 2009 OMB FISMA Reporting Questions

OMB's FY 2009 FISMA Reporting Template for IGs includes the following questions, which are to be addressed by the Treasury OIG and TIGTA:[16]

- Question 1 – Systems Inventory
- Question 2 – Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing
- Question 3 – Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory
- Question 4 – Evaluation of Agency POA&M Process
- Question 5 – IG Assessment of the Certification and Accreditation Process
- Question 6 – IG Assessment of the Privacy Program and PIA Process
- Question 7 – Configuration Management
- Question 8 – Incident Reporting
- Question 9 – Security Awareness Training
- Question 10 – Peer-to-Peer File Sharing

The responses to OMB's questions have been divided into the two sections below. The first section, entitled "Detailed Description of the Responses to the FY 2009 Reporting Template for IGs," includes the analysis and conclusions used to complete the reporting template for the non-IRS bureau of the Treasury.

The second section contains the FY 2009 Reporting Template for IGs. The Treasury's responses to the FY 2009 FISMA Reporting Instructions for the FISMA and Agency Privacy Management contained in OMB Memorandum 08-21 represented the consolidation of the responses for the IRS developed by the TIGTA and the responses for all 12 non-IRS bureaus and offices.

Detailed Description of the Responses to the FY 2009 Reporting Template for IGs[17]

System Inventory/Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory (Questions 1 and 3)

Treasury implemented the TAF during the FY 2007 FISMA reporting period as the centralized repository for all Treasury systems and FISMA-related artifacts. Since its implementation, TAF has helped improve the quality of the Treasury's FISMA system inventory by serving as a centralized repository for common FISMA artifacts across the Department. The Treasury OCIO Cyber Security program has issued policy and guidance on TAF usage and provides training for all new users. No discrepancies were identified with respect to the completeness or quality of the FISMA systems inventory.

For the system selected in our representative subset operated by a contractor, we noted that Treasury had implemented policies and oversight procedures for contractor systems. We identified that contracts contain terms and conditions that stipulated agency and contractor responsibilities related to FISMA. In addition, Memoranda of Understanding are in place to define responsibilities of both the agency and the contractor with respect to the information system security.

[16] The Treasury's IGs include both the Treasury OIG and TIGTA.
[17] Individual non-IRS bureaus and offices have been notified of the detail observations identified during fieldwork separately.

Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing (Question 2)

Treasury has followed documented policies and procedures for certification and accreditation, security controls testing, and contingency plan testing. However, one (1) Treasury system selected at OTS within our representative subset of information systems is operating with an Interim Authority to Operate (IATO). In addition, one (1) Treasury system at OTS identified in the FY 2008 FISMA Audit report was still operating with an IATO at the conclusion of the FY 2009 FISMA Evaluation. Per NIST SP 800-37, an IATO does not represent a full system accreditation, nor is an IATO recognized as a system accreditation by OMB. Lastly, two (2) Treasury systems selected at FMS within our representative subset of information systems did not have a risk assessment or complete testing of the full NIST SP 800-53 Rev. 2 security controls baseline prior to granting a full authority to operate. With the exception of the systems within this Treasury bureau's FISMA systems inventory, Treasury has tested the security controls and contingency plans for all systems within our representative subset of systems during the FY 2009 FISMA reporting period. Refer to Finding No. 1 in the Results section of this report on page 12.

Evaluation of Agency POA&M Process (Question 4)

Refer to Finding No. 5 in the Results section of this report on page 15.

IG Assessment of the Certification and Accreditation (C&A) Process (Question 5)

Refer to Finding No. 1 in the Results section of this report on page 12.

IG Assessment of the Privacy Program and PIA Process (Question 6)

The Treasury Office of Privacy and Treasury records has created TD 25-07, which outlines policy and assigned responsibility for implementing the privacy provisions of the E-Government Act of 2002. TD 25-07 also authorized TD P 25-07, *Privacy Impact Assessment Manual*. TD P 25-07 serves as a standard set of policies and procedures for the performance of PIAs for Treasury information systems. TD P 25-07 has been consistently applied across all 12 non-IRS Treasury bureaus and offices. Specifically, out of the 18 non-IRS systems in our representative subset of Treasury systems that contain PII, each had a PIA consistent with the requirements of TD P 25-07. However, Treasury OPTR has yet to implement policies required by OMB Memorandum 07-16. Refer to Finding No. 3 in the Results section of this report on page 15.

Configuration Management (Question 7)

Refer to Findings No. 2 and No. 6 in the Results section of this report on page 14 and 16 respectively.

Incident Reporting (Question 8)

Treasury has established Treasury-wide computer security incident response and reporting policy and procedures in TD P 85-01. Treasury has also established the TCSIRC to serve as the organization for coordinating computer security incident response and reporting amongst all 14 bureaus and offices of the Treasury and to serve as a single point of contact for reporting computer security incidents to US-CERT and external law enforcement. Each of the 12 non-IRS

bureaus and offices in scope has also developed a computer security incident reporting capability and had reported all computer security incidents internally and in a timely manner.

Security Awareness Training (Question 9)

Treasury has implemented policy in TD P 85-01 that requires each bureau CIO to ensure IT security awareness training is provided annually to IT users (i.e., full time employees, contractors, and any other individuals with system access) in accordance with applicable guidance. In addition, new hires and new contractors are required to attend security awareness training prior to being granted access to information systems. Lastly, all employees and contractors are required to attend security awareness refresher training on an annual basis.

Treasury has continued to make improvements to its security awareness training program since the FY 2008 FISMA Audit. Out of a sample of 170 employees and contractors across Treasury, only one (1) did not attend IT security awareness training within the FY 2009 FISMA reporting period. We noted that this deviation represented only a minimal rate of control failure, based on the total sample size of 170 employees and contractors across all 12 non-IRS bureaus and offices, and did not represent a control weakness.

Peer-to-Peer File Sharing (Question 10)

Treasury has established a Treasury-wide policy in TD P 85-01 for the inclusion of peer-to-peer file sharing in IT security awareness training programs. TD P 85-01 requires bureaus to approve the use of all software, while use of pirated software is prohibited. In addition, bureaus must approve all software use. The TD P 85-01 also references the OMB Memorandum M-04-26, *Personal Use Policies and "File-Sharing" Technology* for additional guidance pertaining to use of peer-to-peer technology. In addition, all non-IRS bureaus and offices have incorporated peer-to-peer file sharing within their IT security awareness training programs, including the Treasury-wide training solution.

OMB FY 2009 Reporting Template for IGs

Question 1: Systems Inventory – Identify the number of agency and contractors systems by component and FIPS 199 impact level (low, moderate, high). Please also identify the number of systems that are used by your agency but owned by another federal agency (i.e., ePayroll, etc.) by component and FIPS 199 impact level.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing – Identify the number of agency and contractors systems by component and FIPS 199 impact level (low, moderate, high). Please also identify the number of systems that are used by your agency but owned by another federal agency (i.e., ePayroll, etc.) by component and FIPS 199 impact level.

		Question 1						Question 2[18]					
		a. Agency Systems		b. Contractor Systems		c. Total number of systems (Agency and Contractor systems)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Bureau Name	**FIPS 199 System Impact Level**	**Number**	**Number Reviewed**	**Number**	**Number Reviewed**	**Total Number**	**Total Number Reviewed**	**Total Number**	**Percent of Total**	**Total Number**	**Percent of Total**	**Total Number**	**Percent of Total**
BEP	High	0	0	0	0	0	0	0	0	0	0	0	0
	Moderate	32	1	2	0	34	1	1	100%	1	100%	1	100%
	Low	8	0	0	0	8	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Subtotal	**40**	**1**	**2**	**0**	**42**	**1**	**1**	100%	**1**	100%	**1**	100%
BPD	High	2	0	0	0	2	0	0	0	0	0	0	0
	Moderate	11	2	0	0	11	2	2	100%	2	100%	2	100%
	Low	6	0	0	0	6	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Subtotal	**19**	**2**	**0**	**0**	**19**	**2**	**2**	100%	**2**	100%	**2**	100%

[18] This template is based on the FISMA Reporting Instructions developed by OMB. These reporting instructions allow the agency to report on a representative subset of agency systems. The Totals and Percent Totals in Question 2 are calculated using the total number of systems in our representative subset of Treasury systems as the denominator, as identified in "Total Number Reviewed" column of Question 1 c. "Total number of systems (Agency and Contractor systems).

		Question 1						Question 2[18]					
		a. Agency Systems		b. Contractor Systems		c. Total number of systems (Agency and Contractor systems)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Bureau Name	**FIPS 199 System Impact Level**	**Number**	**Number Reviewed**	**Number**	**Number Reviewed**	**Total Number**	**Total Number Reviewed**	**Total Number**	**Percent of Total**	**Total Number**	**Percent of Total**	**Total Number**	**Percent of Total**
CDFI	High	0	0	0	0	0	0	0	0	0	0	0	0
	Moderate	3	1	0	0	3	1	1	100%	1	100%	1	100%
	Low	0	0	0	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Subtotal	**3**	**1**	**0**	**0**	**3**	**1**	**1**	100%	**1**	100%	**1**	100%
DO	High	10	0	2	1	12	1	1	100%	1	100%	1	100%
	Moderate	22	2	3	1	25	3	3	100%	3	100%	3	100%
	Low	13	0	2	0	15	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Subtotal	**45**	**2**	**7**	**2**	**52**	**4**	**4**	100%	**4**	100%	**4**	100%
FinCEN	High	5	1	0	0	5	1	1	100%	1	100%	1	100%
	Moderate	2	0	0	0	2	0	0	0	0	0	0	0
	Low	1	0	0	0	1	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Subtotal	**8**	**1**	**0**	**0**	**8**	**1**	**1**	100%	**1**	100%	**1**	100%
FMS	High	8	2	3	1	11	3	3	100%	3	100%	3	100%
	Moderate	29	2	2	0	31	2	2	100%	2	100%	2	100%
	Low	9	0	0	0	9	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Subtotal	**46**	**4**	**5**	**1**	**51**	**5**	**5**	100%	**5**	100%	**5**	100%
IRS	High	4	0	0	0	**4**	**0**	0	0	0	0	0	0
	Moderate	181	11	6	1	**187**	**12**	12	100%	12	100%	12	100%
	Low	44	0	0	0	**44**	**0**	0	0	0	0	0	0
	Not Categorized	0	0	0	0	**0**	**0**	0	0	0	0	0	0

		Question 1						Question 2[18]					
		a. Agency Systems		b. Contractor Systems		c. Total number of systems (Agency and Contractor systems)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Bureau Name	**FIPS 199 System Impact Level**	**Number**	**Number Reviewed**	**Number**	**Number Reviewed**	**Total Number**	**Total Number Reviewed**	**Total Number**	**Percent of Total**	**Total Number**	**Percent of Total**	**Total Number**	**Percent of Total**
	Subtotal	**229**	**11**	**6**	**1**	**235**	**12**	**12**	100%	**12**	100%	**12**	100%
Mint	High	0	0	0	0	0	0	0	0	0	0	0	0
	Moderate	15	0	1	1	16	1	1	100%	1	100%	1	100%
	Low	3	0	0	0	3	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Subtotal	**18**	**0**	**1**	**1**	**19**	**1**	**1**	100%	**1**	100%	**1**	100%
OCC	High	0	0	0	0	0	0	0	0	0	0	0	0
	Moderate	17	1	0	0	17	1	1	100%	1	100%	1	100%
	Low	0	0	0	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Subtotal	**17**	**1**	**0**	**0**	**17**	**1**	**1**	100%	**1**	100%	**1**	100%
OIG	High	0	0	0	0	0	0	0	0	0	0	0	0
	Moderate	1	0	0	0	1	0	0	0	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Subtotal	**1**	**0**	**0**	**0**	**1**	**0**	**0**	0	**0**	0	**0**	0
OTS	High	0	0	0	0	0	0	0	0	0	0	0	0
	Moderate	8	1	0	0	8	1	0	0%	1	100%	1	100%
	Low	0	0	0	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Subtotal	**8**	**1**	**0**	**0**	**8**	**1**	**0**	0%	**1**	100%	**1**	100%
TIGTA	High	0	0	0	0	0	0	0	0	0	0	0	0
	Moderate	2	0	0	0	2	0	0	0	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0	0	0	0

		Question 1						Question 2[18]					
		a. Agency Systems		b. Contractor Systems		c. Total number of systems (Agency and Contractor systems)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Bureau Name	**FIPS 199 System Impact Level**	**Number**	**Number Reviewed**	**Number**	**Number Reviewed**	**Total Number**	**Total Number Reviewed**	**Total Number**	**Percent of Total**	**Total Number**	**Percent of Total**	**Total Number**	**Percent of Total**
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Subtotal	**2**	**0**	**0**	**0**	**2**	**0**	**0**	0	**0**	0	**0**	0
TTB	High	0	0	0	0	0	0	0	0	0	0	0	0
	Moderate	17	1	0	0	17	1	1	100%	1	100%	1	100%
	Low	1	0	0	0	1	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Subtotal	**18**	**1**	**0**	**0**	**18**	**1**	**1**	**100%**	**1**	**100%**	**1**	**100%**
Agency Totals	**High**	**29**	**3**	**5**	**2**	**34**	**5**	**5**	**100%**	**5**	**100%**	**5**	**100%**
	Moderate	**340**	**22**	**14**	**3**	**354**	**25**	**24**	**96%**	**25**	**100%**	**25**	**100%**
	Low	**85**	**0**	**2**	**0**	**87**	**0**	**0**	**0%**	**0**	**0%**	**0**	**0%**
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0%**	**0**	**0%**	**0**	**0%**
	Total	**454**	**25**	**21**	**5**	**475**	**30**	**29**	**97%**	**30**	**100%**	**30**	**100%**

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory – The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.	
Does the agency have policies for oversight of contractors? Yes/No	Yes
If the answer above is Yes, Is the policy implemented?	Yes (See Comment 1 Below)
The agency has a materially correct inventory of major information systems (including national security systems) operated by or under the control of such agency. Yes/No	Yes (Note: National Security Systems are reported in a separate report)
Does the agency maintain an inventory of interfaces between the agency systems and all other systems, such as those not operated by or under the control of the agency? Yes/No	Yes
Does the agency require agreements for interfaces between systems it owns or operates and other systems not operated by or under the control of the agency? Yes/No	Yes
The IG generally agrees with the CIO on the number of agency-owned systems. Yes/No	Yes
The agency inventory is maintained and updated at least annually. Yes/No	Yes
The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes/No	Yes

If the IG does not indicate that the agency has a materially correct inventory, please identify any known missing major systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the systems as presented in the FY 2009 Exhibit 300 (if known), and indicate if the system is an agency or contractor system.

Component/Bureau	System Name	Exhibit 300 Unique Project Identifier (UPI)	Agency or Contractor system?
Not applicable – the Treasury OIG and TIGTA agreed that Treasury has a materially correct inventory			

Number of known systems missing from inventory:	0

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory – The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.	
Comments:	**Comment 1 – TIGTA Comment:** The response to this question is based on our evaluation of the annual testing of 1 contractor system in the sample of 12 systems reviewed. The Treasury Inspector General for Tax Administration (TIGTA) is currently conducting an audit of the effectiveness of contractor managed systems, the results of which will be reflected in future FISMA evaluation results.

Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process – Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process, providing explanatory detail in the area provided.		
Has the Agency developed and documented an adequate policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts? Yes/No		Yes
Has the Agency fully implemented the policy? Yes/No		Yes
Is the Agency currently managing and operating a POA&M process?		Yes (See Overall Comment - Treasury OIG Below)
Is the agency's POA&M process an agency-wide process, incorporating all known IT security weakness, including IG/external audit findings associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency? Yes/No		Yes
Does the POA&M process prioritize IT security weakness to help ensure significant IT security weaknesses are corrected in a timely manner and receive appropriate resources? Yes/No		Yes
When an IT security weakness is identified, do program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)? Yes/No		Yes
For Systems Reviewed:	**a. Are deficiencies tracked and remediated in a timely manner? Yes/No**	Yes

Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process – Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process, providing explanatory detail in the area provided.		
	b. Are the remediation plans effective for correcting the security weakness? Yes/No	Yes
	c. Are the estimated dates for remediation reasonable and adhered to? Yes/No	Yes
Do Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly)? Yes/No		Yes
Does the Agency CIO centrally track, maintain, and independently review/validate POA&M activities on at least a quarterly basis? Yes/No		Yes
POA&M process comments:	**Overall Comment - Treasury OIG:** While there were no findings reported in the POA&M process at 11 of the 12 non-IRS bureau of the Treasury, it was noted that FMS did not consistently update POA&M weakness estimated completion dates for a subset of the POA&M weaknesses sampled. While this discrepancy was identified and reported to management, overall all 12 non-IRS bureaus and offices have generally developed, implemented, and are managing a POA&M process. **(See Finding Number 5 on page 15 in the body of this report)**	

Question 5: IG Assessment of the Certification and Accreditation Process – Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199 (February 2004), Standards for Security Categorization of Federal Information and Information Systems, to determine a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Provide explanatory detail in the area provided.		
Has the Agency developed and documented an adequate policy for establishing a certification and accreditation process that follows the NIST framework? Yes/No		Yes
Is the Agency currently managing and operating a C&A process in compliance with its policies? Yes/No		Yes (See Comment 2 Below)
For systems reviewed, does the C&A process adequately provide:(Yes/No)	**Appropriate risk categories**	Yes
	Adequate risk assessments	Yes
	Selection of appropriate controls	Yes
	Adequate testing of controls	No (See Comment 3 Below)
	Regular monitoring of system risks and the adequacy of controls	Yes
For systems reviewed, is the Authorizing Official presented with complete and reliable C&A information to facilitate an informed system Authorization to Operate decision based on risks and controls implemented? Yes/No		Yes
C&A process comments:	**Comment 2 - Treasury OIG:** We identified that Treasury has generally managed and operated a certification and accreditation process in compliance with its policies. However, deviations were identified at FMS and OTS. Specifically, NIST FIPS 199 security control baselines were not adequately tested for two (2) systems at FMS and not fully implemented over two (2) systems at OTS. **(See Finding Number 1 on page 12 in the body of this report)** **Comment 3 - TIGTA:** Controls were not adequately tested for 3 of the 12 sampled systems reviewed. For each of the three systems, controls were selected and tested during 2009 for continuous monitoring of security. However, tests of the operational and technical controls for the three systems were not sufficient to determine if the controls were in place and operating as intended. Specifically, 11 (31 percent) of 35 operational controls and	

Question 5: IG Assessment of the Certification and Accreditation Process – Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199 (February 2004), Standards for Security Categorization of Federal Information and Information Systems, to determine a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Provide explanatory detail in the area provided.	
	15 (27 percent) of 56 technical controls selected for the 3 systems, collectively, were not adequately tested. The tests were limited to examining certification and accreditation documentation or conducting interviews without examining system evidence. For example, configuration change control is an operational control that ensures changes to the information system are authorized, documented, and controlled. For one of the systems, the IRS evaluated this control by examining the test results from the system's last certification and accreditation in 2007. For another system, the IRS evaluated the control by referring to a description of the control in the system's System Security Plan. In both examples, the IRS did not actually test the control.

Questions 6 : IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process – Provide a qualitative assessment of the agency's process, as discussed in Section D, for protecting privacy-related information, including adherence to existing policy, guidance and standards. Provide explanatory information in the area provided.	
Has the Agency developed and documented adequate policies that comply with OMB guidance in M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information? Yes/No	No (See Comment 3 Below)
Is the Agency currently managing and operating a privacy program with appropriate controls in compliance with its policies? Yes/No	No (See Comment 3 Below)
Has the Agency developed and documented an adequate policy for Privacy Impact Assessments? Yes/No/NA	Yes
Has the Agency fully implemented the policy and is the Agency currently managing and operating a process for performing adequate privacy impact assessments? Yes/No/NA	Yes

Questions 6 : IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process – Provide a qualitative assessment of the agency's process, as discussed in Section D, for protecting privacy-related information, including adherence to existing policy, guidance and standards. Provide explanatory information in the area provided.	
Comments:	**Comment 3 – Treasury OIG:** While the TIGTA has reported "Yes" to these questions with respect to the IRS, the Treasury Office of Privacy and Treasury Records have yet to finalize Treasury-wide policy for safeguarding privacy-related information, as required by OMB Memorandum 07-016. **(See Finding Number 4 on page 15 in the body of this report)**

Question 7: Configuration Management	
Is there an agency-wide security configuration policy? Yes or No.	Yes
For each OS/platform/system for which your Agency has a configuration policy, please indicate the status of implementation for that policy?	See Comment 4 Below
Agency has documented deviations from FDCC standard configuration. Yes/No	Yes
New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology", is included in all contracts related to common security settings. Yes/No.	No (See Comment 5 Below)

Comments:

Comment 4 - Treasury OIG: The following table includes the consolidated Treasury OIG and TIGTA results for all 14 Treasury bureaus and offices:

OS/Platform/System	**Implementation Status**	**Monitoring Compliance (if Policy fully implemented)**	
		Tool/Technique/Technology	**Category**
Microsoft Windows NT 4.0	Policy Fully Implemented	Windows Policy Checker	Configuration Scanner
Microsoft Windows 2000 Professional	Policy Fully Implemented	Windows Policy Checker	Configuration Scanner
Microsoft Windows Server 2000	Policy Fully Implemented	McAfee Foundstone	Vulnerability Scanner
		Tenable Security Nessus	Vulnerability Scanner
		Microsoft Baseline Security Analyzer	Configuration Scanner
		Qualysis	Vulnerability Scanner
		System Center Configuration Manager/System Management Service	Other – Patch Management

Question 7: Configuration Management				
			Windows Policy Checker	Configuration Scanner
	Microsoft Windows Server 2003	Policy Fully Implemented	McAfee Foundstone	Vulnerability Scanner
			Tenable Security Nessus	Vulnerability Scanner
			Microsoft Baseline Security Analyzer	Configuration Scanner
			Qualysis	Vulnerability Scanner
			System Center Configuration Manager/System Management Service	Other – Patch Management
			Windows Policy Checker	Configuration Scanner
	Microsoft Windows XP	Policy Fully Implemented	ThreatGuard Secutor Prime	Configuration Scanner
			ThreatGuard Secutor Magnus	Configuration Scanner
			Tenable Security Nessus	Configuration Scanner
			Secure Fusion	Configuration Scanner
			GFI LANguard	Vulnerability Scanner
			System Center Configuration Manager/System Management Service	Other – Patch Management
			Windows Policy Checker	Configuration Scanner
			Security Compliance Checker	Configuration Scanner
	Sun Solaris	Policy Fully Implemented	McAfee Foundstone	Vulnerability Scanner
			Tenable Security Nessus	Vulnerability Scanner
			Qualysis	Vulnerability Scanner
			Unix Policy Checker	Configuration Scanner
	IBM AIX	Policy Fully Implemented	McAfee Foundstone	Vulnerability Scanner
			Tenable Security Nessus	Vulnerability Scanner
			Qualysis	Vulnerability Scanner
			Checklist	Other
	HP-UX	Policy Fully Implemented	McAfee Foundstone	Vulnerability Scanner
			Tenable Security Nessus	Vulnerability Scanner
			Qualysis	Vulnerability Scanner
			Unix Policy Checker	Configuration Scanner
	Red Hat Linux	Policy Fully Implemented	McAfee Foundstone	Vulnerability Scanner
			Tenable Security Nessus	Vulnerability Scanner
			Qualysis	Vulnerability Scanner
			Checklist	Other
	IBM OS390	Policy Fully Implemented	Mainframe Policy Checker	Configuration Scanner
	Microsoft SQL Server	Policy Fully Implemented	AppDetective	Configuration Scanner

Question 7: Configuration Management

2000		Checklist	Other
Microsoft SQL Server 2005	Policy Fully Implemented	Checklist	Other
IBM DB2	Policy Fully Implemented	AppDetective	Configuration Scanner
		Checklist	Other
Oracle Database 8i	Policy Fully Implemented	AppDetective	Configuration Scanner
		Checklist	Other
Oracle Database 9i	Policy Fully Implemented	Checklist	Other
Oracle Database 10g	Policy Fully Implemented	Checklist	Other
Cisco IOS	Policy Fully Implemented	OPNETDoctor	Configuration Scanner
Other	Policy Fully Implemented	Other – Enterasys Dragon	Intrusion Detection and Prevention Systems
		Other - Snort	Intrusion Detection and Prevention Systems
		Other – IBM zOS Manual Technique	Configuration Scanner

Note: While this table contains the combined results of the Treasury OIG and TIGTA FISMA evaluations, we have also maintained the separate TIGTA specific comment below.

Comment 4 - TIGTA: The IRS uses the following tools and techniques for monitoring compliance with configuration policy:

- Windows Policy Checker for Windows XP, Windows NT, Windows 2000 Professional, Windows 2000 Server, and Windows 2003 Server
- Security Compliance Checker for Windows XP
- UNIX Policy Checker for UNIX, Solaris, and HP-UX
- Mainframe Policy Checker for Mainframes
- OPNET Doctor for Cisco Router and Switches
- Checklists for Linux, Oracle, SQL, DB2, and AIX

Comment 5 – Treasury OIG/TIGTA: While the Treasury OIG reported "Yes" for this question for the 12 non-IRS Treasury bureaus, TIGTA reported "No". Specifically, in March 2009, TIGTA issued a report[19] in which they identified that 27 of 30 contracts for new software products that reviewed did not include the required FDCC contract language. The IRS has not yet implemented policy that would require the inclusion of the FDCC language in contracts for new software products. The IRS responded to the report that it planned to issue an agency-wide policy that will incorporate the FDCC contract language in information technology acquisitions.

Been Slow in Implementing Federal Security Configurations on Employee Computers (Reference Number 2009-20-055, dated March 27, 2009).

Question 8: Incident Reporting	
How often does the Agency comply documented policies and procedures for identifying and reporting incidents internally? Answer will be a percentage range	90-100% (See Comment 6 Below)
How often does the Agency comply with documented policies and procedures for timely reporting of incidents to US CERT? Answer will be a percentage range	90-100% (See Comment 7 Below)
How often does the Agency comply documented policy and procedures for reporting to law enforcements? Answer will be a percentage range	90-100% (See Comment 8 Below)
Comments:	**General Comment - Treasury OIG:** No significant discrepancies in incident reporting were identified at the 12 non-IRS bureau of the Treasury. **Comment 6 – TIGTA:** This percentage rate is based on an August 2009 TIGTA audit report[20] which showed that IRS employees reported 96 percent of all incidents involving the loss of information technology assets to the IRS Computer Security Incident Response Center, whose mission is to be proactive in preventing, detecting, and responding to computer security incidents targeting IRS enterprise information technology assets.. **Comment 7 – TIGTA:** Not applicable. The IRS does not report incidents directly to US-CERT. The IRS reports incidents to the Department of the Treasury. The Department of the Treasury serves as the central point for reporting Treasury bureau incidents to the US-CERT. **Comment 8 – TIGTA:** 90 percent– 100 percent. This percentage rate is based on an August 2009 TIGTA audit report that showed that the IRS reported 96 percent of all incidents involving the loss of information technology assets to the TIGTA Office of Investigations, the law enforcement agency for the IRS.

Question 9: Security Awareness Training – Has the agency ensured IT security awareness training of all users with log in privileges, including contractors and those employees with significant IT security responsibilities? Provide explanatory detail in the space provided.	
Has the Agency developed and documented an adequate policy for identifying all general users, contractors, and system owners/employees who have log in privileges, and providing them with	Yes

[20] *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).

Question 9: Security Awareness Training – Has the agency ensured IT security awareness training of all users with log in privileges, including contractors and those employees with significant IT security responsibilities? Provide explanatory detail in the space provided.	
suitable IT security awareness training? Yes/No/NA	(See Comment 9 Below)
Total number of people with log in privileges to agency systems	104, 231
Number of people with log in privileges to agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" (October 2003).	124,773 (See Comment 10 Below)
Total number of employees with significant information security responsibilities.	7,778
Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (April 1998)	7,633
Comments:	**General Comment - Treasury OIG:** Our conclusions in Question 9 are based on totals provided by the Treasury OCIO and verified by test work over a samples of employees and contractors at each of the 12 non-IRS bureaus and offices of the Treasury to determine if individuals with log in privileges to agency systems received information security awareness training during the past fiscal year and to determine if employees with significant security responsibilities received specialized training. **Comment 9 – TIGTA:** The IRS identifies all employees and contractors including those with log in privileges as well as those without system access. **Comment 10 - TIGTA:** 107,568 people received information security awareness training. This included individuals with log in privileges as well as those without system access.

Question 10: Peer-to-Peer File Sharing	
Does the agency explain policies regarding the use of peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes/No.	Yes

Appendix II – Approach to the Selection of the Subset of Systems

In FY 2009, we employed a risk-based approach to determine the representative subset of Treasury information systems for the FISMA evaluation. The universe for this representative subset will only include major applications and general support systems.

We used a total subset size of 15% of the total population of Treasury major applications and general support systems. We then applied the weighting of IRS systems to non-IRS bureau systems to the total subset size in order to determine the IRS and non-IRS bureau subset sizes. We determined that, as of April 2, 2009, 60% of the population of Treasury information systems are non-IRS major applications and general support systems. We also determined that 40% of the population of Treasury information system were IRS major applications and general support systems. Based on our analysis, we noted 203 major applications and general support systems are contained within the Treasury-wide inventory. The following table provides our analysis of the composition of the Treasury's inventory of major applications and general support systems.

	Total	IRS	non-IRS	non-IRS Financial Systems
Major Applications	148	59	89	43
General Support Systems	55	23	32	4
Total	203	82	121	47

Applying the subset size percentage of 15% to the total population of 203 yields a total subset size of 30 systems. When the IRS to non-IRS weighting is applied to this total subset size, the resulting sizes for the IRS and non-IRS subsets are 12 and 18, respectively.

We determined that Major Applications account for 74% of the population of the non-IRS population and General Support Systems account for 26%. We further determined that systems designated as "Financial" in TAF account for 39% of all non-IRS Major Applications and General Support Systems. Lastly, we determined that 26% of the non-IRS Major Applications and General Support Systems are assigned a FIPS 199 System Impact Level of "High," while 66% are assigned a FIPS 199 System Impact Level of "Moderate" and 7% are assigned a FIPS 199 System Impact Level of "Low." (Note: Based on their lower risk, we elected not to select any systems with a FIPS 199 System Impact Level of "Low." Rather, we substituted these systems for a system with a FIPS 199 System Impact Level of "Moderate.")

To select the subset, we stratified the full population of Treasury major applications and general support systems by bureau and by FIPS 199 system impact level.

Total Selected	18
Total Major Applications	14
Total General Support Systems	4
Total Systems with a FIPS 199 System Impact Level of "High"	5
Total Systems with a FIPS 199 System Impact Level of "Moderate"	13
Total Systems with a FIPS 199 System Impact Level of "Low"	0
Total Systems Designated as Financial	7

We further stratified the number of information system 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 system. This information was used as a baseline when determining the total number of systems to select at each bureau:

Bureau	Total Systems	Percentage of Total non-IRS Population	Total Number of non-IRS Systems to be Selected
BEP	8	7%	1
BPD	13	11%	2
CDFI Fund	3	2%	1
DO	27	22%	4
FinCEN	5	4%	1
FMS	33	27%	5
Mint	10	8%	2
OCC	8	8%	1
OIG	1	1%	0
OTS	8	7%	1
TIGTA	2	1%	0
TTB	3	2%	1
Total	121	100%	18

We then used a risk-based approach to selecting systems out of each stratum. We considered the following factors to select each system:

- Total number of systems per bureau
- Systems at smaller bureaus not historically included in FISMA audits or evaluations
- Number of systems at each bureau with a FIPS system impact level of "High"
- 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 OIG reviews
- Availability of the system via the Internet.

From our representative subset of 18 non-IRS Treasury systems, we also selected five (5) to perform in-depth testing over specific controls selected from the NIST SP 800-53 Rev. 2 minimum security control baseline. We selected five (5) major applications with a NIST FIPS 199 system impact level of Moderate. We selected one system each from the five (5) non-IRS Treasury bureaus with the highest concentration of systems or had prior year findings in the implementation of the NIST SP 800-53 Rev. 2 minimum security control baseline.

Appendix III – Acronym Listing

Acronym	Definition
ACIOCS	Associate Chief Information Officer for Cyber Security
BEP	Bureau of Engraving and Printing
BPD	Bureau of the Public Debt
CDFI	Community Development Financial Institution
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CPO	Chief Privacy Officer
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
IATO	Interim Authority to Operate
IG	Inspector General
IRS	Internal Revenue Service
IT	Information Technology
Mint	United States Mint
NIST	National Institute of Standards and Technology

Acronym	Definition
OCC	Office of the Comptroller of Currency
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OPTR	Office of Privacy and Treasury Records
OIG	Office of the Inspector General
OTS	Office of Thrift Supervision
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
Rev	Revision
SAOP	Senior Agency Official for Privacy
SCAP	Security Content Automation Protocol
SIGTARP	Special Inspector General for the Troubled Asset Relief Program
SP	Special Publication
TAF	Trusted Agent FISMA
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-CERT	United States Computer Emergency Readiness Team

ATTACHMENT 2

Treasury Inspector General for Tax Administration–Federal Information Security Management Act Report for Fiscal Year 2009, October 27, 2009

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 27, 2009

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

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 2009 (Audit # 200920010)

We are pleased to submit the Treasury Inspector General for Tax Administration's Federal Information Security Management Act (FISMA)[1] report for Fiscal Year 2009. The FISMA requires the Office of Inspector General to perform an annual independent evaluation of information security policies, procedures, and practices, as well as evaluate 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 on the Office of Management and Budget (OMB) FISMA 2009 Reporting Guidelines. During the 2009 evaluation period,[2] we conducted eight audits, as shown in Attachment I, to evaluate the adequacy of information security in the IRS. We considered the results of these audits in our evaluation. In addition, we evaluated a representative sample of 12 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, 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 inventory accuracy, configuration management, incident reporting, security awareness and specialized security training, and the information privacy program.

Included in Attachment II are our responses to the OMB Fiscal Year 2009 FISMA questions for the Inspector General. We are confident that the IRS has:

- Established a materially correct inventory.
- Implemented a certification and accreditation process that follows the National Institute for Standards and Technology (NIST) framework.

[1] 44 U.S.C. §§ 3541 - 3549.
[2] The FISMA evaluation period for the Department of the Treasury is July 1, 2008, through June 30, 2009. All subsequent references to 2009 refer to the FISMA evaluation period.

- Sufficiently tested its information technology contingency plans.
- Implemented an adequate Plan of Action and Milestones process to ensure that security weaknesses are remediated.
- Followed policies and procedures for reporting computer security incidents.
- Provided employees security awareness and specialized security training.
- Implemented adequate policies to protect privacy-related information.

Since the enactment of the FISMA in Calendar Year 2002, overall, the IRS has made steady progress in complying with FISMA requirements. In addition, the IRS continues to place a high priority on efforts to improve its security program. We observed significant improvements in information technology contingency plan testing and additional improvements in annual security controls testing, two security areas we identified as needing improvement in our 2008 FISMA evaluation.[3] However, based on our 2009 evaluation, we believe the IRS still needs to take additional actions in the areas of certification and accreditation, and configuration management to better secure its systems and data.

Certification and Accreditation Process The OMB guidelines for minimum security controls in Federal Government information systems require that all systems be certified and accredited every 3 years, or when major system changes occur. The NIST provides guidelines for conducting the system certifications and accreditations. Five of the 12 systems in our sample were certified and accredited in 2009. We evaluated the quality of the certification and accreditation process for these five systems and determined that all of them were properly certified and accredited in accordance with NIST guidelines.

The OMB also requires that system security controls be tested for every system at least annually. In years when a system will not be certified and accredited, a subset of security controls must be tested. The NIST provides guidelines for annual testing of security controls. We reviewed the adequacy of annual testing of security controls for 7 of the 12 systems in our sample that were not certified and accredited in 2009. We found that an appropriate subset of management, operational, and technical controls was selected, documented, and approved for each of the seven systems. However, tests of the operational and technical controls for three of the seven systems were not sufficient to determine if the controls were in place and operating as intended. Specifically, 11 (31 percent) of 35 operational controls and 15 (27 percent) of 56 technical controls selected for the 3 systems, collectively, were not adequately tested. The tests were limited to examining certification and accreditation documentation or conducting interviews without examining system evidence. For example, configuration change control is an operational control that ensures changes to the information system are authorized, documented, and controlled. For one of the systems, the IRS evaluated this control by examining the test results from the system's last certification and accreditation in 2007. For another system, the IRS evaluated the control by referring to a description of the control in the system's System

[3] *Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2008* (Reference Number 2008-20-173, dated September 10, 2008).

Security Plan. In both examples, the IRS did not actually test the control. As a result, these tests were insufficient to determine whether the security controls were operating as intended.

Configuration Management The OMB required Federal Government agencies that use the Windows XP or VISTA operating systems to adopt a standard set of configuration settings by February 1, 2008. These configuration settings are referred to as the Federal Desktop Core Configuration (FDCC). The IRS has made significant progress in implementing FDCC standard settings. As of the end of the 2009 evaluation period, the IRS had implemented or had deviations approved by the Department of the Treasury for 265 (94 percent) of 282 FDCC settings. The IRS continues to test the remaining FDCC configurations and has a plan in place to reach full implementation by February 2010. The IRS has not, however, modified its software contracts to ensure purchased software will operate properly with the FDCC settings. In March 2009, we issued a report[4] in which we identified that 27 of 30 software contracts that we examined did not include the required FDCC contract language. The IRS has not yet developed a policy that would require the inclusion of the FDCC language in contracts for new software products. The IRS responded to the report that it planned to issue an agency-wide policy that will incorporate the FDCC contract language in information technology acquisitions.

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) 622-8510.

Attachments

[4] *Progress Has Been Slow in Implementing Federal Security Configurations on Employee Computers* (Reference Number 2009-20-055, dated March 27, 2009).

Attachment I

Treasury Inspector General for Tax Administration Information Technology Security Reports Issued During the 2009 Evaluation Period

1. *The Office of Research, Analysis, and Statistics Needs to Address Computer Security Weaknesses* (Reference Number 2008-20-176, dated September 17, 2008).
2. *Weaknesses in Business Resumption Plans Could Delay Recovery From a Disaster* (Reference Number 2008-20-178, dated September 17, 2008).
3. *The Internal Revenue Service Deployed Two of Its Most Important Modernized Systems With Known Security Vulnerabilities* (Reference Number 2008-20-163, dated September 24, 2008).
4. *The Internal Revenue Service Deployed the Modernized e-File System With Known Security Vulnerabilities* (Reference Number 2009-20-026, dated December 30, 2008).
5. *Better Emergency Preparedness Planning Could Improve Business Continuity Efforts* (Reference Number 2009-20-038, dated February 13, 2009).
6. *While Controls Have Been Implemented to Address Malware, Continued Attention Is Needed to Address This Growing Threat* (Reference Number 2009-20-045, dated March 10, 2009).
7. *Progress Has Been Slow in Implementing Federal Security Configurations on Employee Computers* (Reference Number 2009-20-055, dated March 27, 2009).
8. *The Homeland Security Presidential Directive 12 Program Office Has Addressed Prior Weaknesses, but Progress Is Slower Than What Has Been Reported* (Reference Number 2009-20-084, dated June 25, 2009).

Attachment II

Treasury Inspector General for Tax Administration Responses to the 2009 Office of Management and Budget Federal Information Security Management Act Inspector General Questions

Question 1: System Inventory
Identify the number of agency and contractor systems by component and Federal Information Processing Standard (FIPS) 199 impact level (low, moderate, high). Please also identify the number of systems that are used by your agency but owned by another Federal agency (i.e., ePayroll, etc.) by component and FIPS 199 impact level.

Internal Revenue Service (IRS)				
FIPS 199 System Impact Level	**Agency Systems**	**Contractor Systems**	**Total Systems (Agency and Contractor Systems)**	**Systems Owned by Another Federal Agency**
High	4	0	4	*
Moderate	181	6	187	*
Low	44	0	44	*
Total	**229**	**6**	**235**	*

* This information will be provided by the Department of the Treasury for all agency components.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing
For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

FIPS 199 System Impact Level	Systems Reviewed	Number of systems with a current certification and accreditation	% of Total	Systems with security controls tested and reviewed within the past year	% of Total	Systems with contingency plans tested in accordance with policy	% of Total
High	0						
Moderate	12	12	100%	12	100%	12	100%
Low	0						
Total	**12**	**12**	**100%**	**12**	**100%**	**12**	**100%**

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory

The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.

Does the agency have policies for oversight of contractors? Yes/No

Yes.

If the answer above is yes, is the policy implemented?

Yes. The response to this question is based on our evaluation of the annual testing of 1 contractor system in the sample of 12 systems reviewed. The Treasury Inspector General for Tax Administration (TIGTA) is currently conducting an audit of the effectiveness of contractor managed systems, the results of which will be reflected in future FISMA evaluation results.

The agency has a materially correct inventory of major information systems (including national security systems) operated by or under the control of such agency. Yes/No

Yes.

Does the agency maintain an inventory of interfaces between the agency systems and all other systems, such as those not operated by or under the control of the agency? Yes/No

Yes.

Does the agency require agreements for interfaces between systems it owns or operates and other systems not operated by or under the control of the agency? Yes/No

Yes.

The IG generally agrees with the CIO on the number of agency-owned systems. Yes/No

Yes.

The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes/No

Yes.

The agency inventory is maintained and updated at least annually. Yes/No

Yes.

If the IG does not indicate that the agency has a materially correct inventory, please identify any known missing major systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the systems as presented in the FY 2009 Exhibit 300 (if known), and indicate if the system is an agency or contractor system.

Not applicable as the TIGTA agrees that the IRS has a materially correct inventory.

Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process

Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process, providing explanatory detail in the area provided.

Has the agency developed and documented an adequate policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts? Yes/No

Yes.

Has the agency fully implemented the policy? Yes/No

Yes.

Is the agency currently managing and operating a POA&M process?

Yes.

Is the agency's POA&M process an agency-wide process, incorporating all known IT security weaknesses, including IG/external audit findings associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency? Yes/No

Yes.

Does the POA&M process prioritize IT security weaknesses to help ensure significant IT security weaknesses are corrected in a timely manner and receive appropriate resources? Yes/No

Yes.

When an IT security weakness is identified, do program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)? Yes/No

Yes.

For Systems Reviewed:

a. Are deficiencies tracked and remediated in a timely manner? Yes/No

Yes.

b. Are the remediation plans effective for correcting the security weakness? Yes/No

Yes.

c. Are the estimated dates for remediation reasonable and adhered to? Yes/No

Yes.

Do Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly)? Yes/No

Yes.

Does the Agency CIO centrally track, maintain, and independently review/validate POA&M activities on at least a quarterly basis? Yes/No

Yes.

Question 5: IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199 (February 2004), Standards for Security Categorization of Federal Information and Information Systems, to determine a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Provide explanatory detail in the area provided.

Five of the 12 systems reviewed were certified and accredited during the past year. Security controls were selected and tested for the remaining seven systems as part of the continuous monitoring of security controls.

Has the agency developed and documented an adequate policy for establishing a certification and accreditation process that follows the NIST framework? Yes/No

Yes.

Is the agency currently managing and operating a C&A process in compliance with its policies? Yes/No

Yes.

For systems reviewed, does the C&A process adequately provide: (check all that apply)

- ✓ Appropriate risk categories
- ✓ Adequate risk assessments
- ✓ Selection of appropriate controls
- X Adequate testing of controls
- ✓ Regular monitoring of system risks and the adequacy of controls

Controls were not adequately tested for 3 of the 12 sampled systems reviewed. For each of the three systems, controls were selected and tested during 2009 for continuous monitoring of security. However, tests of the operational and technical controls for the three systems were not sufficient to determine if the controls were in place and operating as intended. Specifically, 11 (31 percent) of 35 operational controls and 15 (27 percent) of 56 technical controls selected for the 3 systems, collectively, were not adequately tested. The tests were limited to examining certification and accreditation documentation or conducting interviews without examining system evidence. For example, configuration change control is an operational control that ensures changes to the information system are authorized, documented, and controlled. For one of the systems, the IRS evaluated this control by examining the test results from the system's last certification and accreditation in 2007. For another system, the IRS evaluated the control by referring to a description of the control in the system's System Security Plan. In both examples, the IRS did not actually test the control.

For systems reviewed, is the Authorizing Official presented with complete and reliable C&A information to facilitate an informed system Authorization to Operate decision based on risks and controls implemented? Yes/No

Yes.

Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process
Provide a qualitative assessment of the agency's process, as discussed in Section D, for protecting privacy-related information, including adherence to existing policy, guidance, and standards. Provide explanatory information in the area provided.

Has the Agency developed and documented adequate policies that comply with OMB guidance in M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information? Yes/No

Yes.

Is the Agency currently managing and operating a privacy program with appropriate controls in compliance with its policies? Yes/No

Yes.

Has the Agency developed and documented an adequate policy for Privacy Impact Assessments? Yes/No/Not Applicable

Yes.

Has the Agency fully implemented the policy and is the Agency currently managing and operating a process for performing adequate privacy impact assessments? Yes/No/Not Applicable

Yes.

Question 7: Configuration Management

Is there an agency-wide security configuration policy? Yes/No

Yes.

What tools, techniques is your agency using for monitoring compliance?

The IRS uses the following tools and techniques for monitoring compliance with configuration policy:

- Windows Policy Checker for Windows XP, Windows NT, Windows 2000 Professional, Windows 2000 Server, and Windows 2003 Server.
- Security Compliance Checker for Windows XP.
- Unix Policy Checker for Unix, Solaris, and HP-UX.
- Mainframe Policy Checker for Mainframes.
- OPNET Doctor for Cisco Router and Switches.
- Checklists for Linux, Oracle, SQL, DB2, and AIX.

Indicate the status of the implementation of FDCC at your agency:
Agency has documented deviations from FDCC standard configuration. Yes/No

Yes.

New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology," is included in all contracts related to common security settings. Yes/No

No. In March 2009, we issued a report[1] in which we identified that 27 of 30 contracts for new software products that we reviewed did not include the required FDCC contract language. The IRS has not yet implemented policy that would require the inclusion of the FDCC language in contracts for new software products. The IRS responded to the report that it planned to issue an agency-wide policy that will incorporate the FDCC contract language in information technology acquisitions.

Question 8: Incident Reporting

How often does the agency comply with documented policies and procedures for identifying and reporting incidents internally? Answer will be a percentage range.

90 percent– 100 percent. This percentage rate is based on an August 2009 TIGTA audit report[2] which showed that IRS employees reported 96 percent of all incidents involving the loss of

[1] *Progress Has Been Slow in Implementing Federal Security Configurations on Employee Computers* (Reference Number 2009-20-055, dated March 27, 2009).
[2] *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).

information technology assets to the IRS Computer Security Incident Response Center, whose mission is to be proactive in preventing, detecting, and responding to computer security incidents targeting IRS enterprise information technology assets.

How often does the agency comply with documented policies and procedures for timely reporting of incidents to US CERT? Answer will be a percentage range.

Not applicable. The IRS does not report incidents directly to US-CERT. The IRS reports incidents to the Department of the Treasury. The Department of the Treasury serves as the central point for reporting Treasury bureau incidents to the US-CERT.

How often does the agency comply with documented policy and procedures for reporting to law enforcement? Answer will be a percentage range.

90 percent– 100 percent. This percentage rate is based on an August 2009 TIGTA audit report[3] that showed that the IRS reported 96 percent of all incidents involving the loss of information technology assets to the TIGTA Office of Investigations, the law enforcement agency for the IRS.

Question 9: Security Awareness Training

Has the agency ensured IT security awareness training of all users with log in privileges, including contractors and those employees with significant IT security responsibilities? Provide explanatory detail in the space provided.

Has the agency developed and documented an adequate policy for identifying all general users, contractors, and system owners/employees who have log in privileges, and providing them with suitable IT security awareness training? Yes/No/Not Applicable

Yes. The IRS identifies all employees and contractors including those with log in privileges as well as those without system access.

Report the following for your agency:

Total number of people with log in privileges to agency systems.

86,535.

Number of people with log in privileges to agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" (October 2003).

107,568 people received information security awareness training. This included individuals with log in privileges as well as those without system access.

Total number of employees with significant information security responsibilities.

5,919.

Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (April 1998).

5,913.

[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).

Question 10: Peer-to-Peer File Sharing

Does the agency explain policies regarding the use of peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes/No

Yes.