Audit Report

AUDIT REPORT

INFORMATION TECHNOLOGY: Federal Information Security Management Act Fiscal Year 2008 Performance Audit (OIG-08-046)

September 26, 2008

Office of Inspector General

Department of the Treasury

September 26, 2008

**OFFICE OF
INSPECTOR GENERAL**

MEMORANDUM FOR PETER B. MCCARTHY
ASSISTANT SECRETARY FOR MANAGEMENT AND
CHIEF FINANCIAL OFFICER

MICHAEL DUFFY
CHIEF INFORMATION OFFICER

FROM: Joel Grover /s/
Deputy Assistant Inspector General for Financial Management
and IT Audits

SUBJECT: 2008 Audit of Treasury's Federal Information Security
Management Act Implementation

I am pleased to transmit the following reports:

- Federal Information Security Management Act Fiscal Year 2008 Performance
  Audit–September 26, 2008
- Treasury Inspector General for Tax Administration (TIGTA)–Federal Information
  Security Management Act Report for Fiscal Year 2008, Audit #200820024,
  September 10, 2008

The Federal Information Security Management Act of 2002 (FISMA) requires an annual
independent evaluation of the Department of the Treasury's information security
program and practices. To meet FISMA requirements, we contracted with KPMG LLP,
an independent certified public accounting firm, to perform the FISMA audit of
Treasury's unclassified systems, except for those of the Internal Revenue Service
(IRS). Attachment 1 contains the KPMG report and our Office of Management and
Budget submission[1], which incorporates the responses from TIGTA. Attachment 2
contains TIGTA's evaluation of FISMA compliance for IRS systems.[2]

---

[1] The Office of Management and Budget Memorandum M-08-21, *"FY 2008 Reporting Instructions for
the Federal Information Security Management Act and Agency Privacy Management,"* dated July 14,
2008, requires completion of FISMA reporting template by the Inspector General of each agency.
[2] We did not review the work performed by TIGTA to evaluate the information security program and
practices of IRS. Our overall conclusions, insofar as they relate to IRS, are based solely on TIGTA's
report (attachment 2). We did, however, coordinate with TIGTA on the scope and methodology,
including sample selection, of our respective engagements.

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. Also, Treasury had implemented all provisions of HSPD-7 paragraphs 1 through11. However, the KPMG audit of Treasury's unclassified systems (except for those of IRS) indicated that additional steps are required to ensure that Treasury's information security risk management program and practices fully comply with applicable National Institute of Standards and Technology (NIST) standards and guidelines and FISMA requirements. Specifically, KPMG reported that (1) NIST FIPS 200 minimum security control baselines were not sufficiently documented, tested, and/or implemented; (2) computer security incidents were not consistently reported timely or correctly categorized; (3) common security configuration baselines were not fully compliant; and (4) federal desktop core configurations were not fully implemented.

TIGTA reported that IRS had made significant improvements in the areas of security identified as needing improvement in TIGTA's 2007 FISMA evaluation and had improved the efficiency of its certification and accreditation process. Additionally, TIGTA found that IRS had completed certification and accreditation for the last of its systems. TIGTA noted the most significant area of concern was IRS's implementation of configuration management standards.

If you have any questions or require further information, you may contact me at (202) 927-5768, or Tram Dang at (202) 927-5171. For questions pertaining to the TIGTA FISMA evaluation, please contact Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Attachments

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

ATTACHMENT 1

Federal Information Security Management Act
Fiscal Year 2008 Performance Audit,
September 26, 2008

United States Department of the Treasury
Federal Information Security Management Act
Fiscal Year 2008 Performance Audit

Prepared for the United States Department of the Treasury
Office of the Inspector General

Prepared by KPMG LLP

September 26, 2008

TABLE OF CONTENTS

FISMA PERFORMANCE AUDIT REPORT

APPENDICES

KPMG LLP
2001 M Street, NW
Washington, DC 20036

EXECUTIVE SUMMARY

September 26, 2008

Joel Grover
Deputy Assistant Inspector General for Financial Management and Information Technology Audits
United States Department of the Treasury
740 15th Street, N.W., Suite 600
Washington, D.C. 20220

Dear Mr. Grover:

This report presents the results of our performance audit conducted to address the objectives relative to the Fiscal Year (FY) 2008 Federal Information Security Management Act of 2002 (FISMA) of the 12 non-Internal Revenue Service (IRS) bureaus of the United States Department of the Treasury (Treasury). The IRS was not included within the scope of this FISMA audit. The Treasury Inspector General for Tax Administration (TIGTA) performed the FISMA evaluation of the IRS. As part of this FISMA audit, we only incorporated the results of the TIGTA FISMA evaluation of the IRS into the Office of Management and Budget (OMB) FY 2008 FISMA Reporting Template (See Appendix I). Our audit was performed during the period of May 13 through August 29, 2008. The Treasury Office of the Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct a performance audit of the Treasury's non-IRS information security program and practices pursuant to FISMA.

We conducted this performance audit in accordance with the standards applicable to such audits contained in *Generally Accepted Government Auditing Standards* (GAGAS), issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of our audit were to determine as of June 30, 2008, whether non-IRS Treasury bureaus had implemented:

- An information security program, consisting of plans, policies, procedures, and security controls, consistent with FISMA[1]
- 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*
- Plans for protecting the physical and cyber critical infrastructure and key resource (CI/KR) consistent with paragraphs 1 through 11 of Homeland Security Presidential Directive (HSPD)-7, *Critical Infrastructure Identification, Prioritization, and Protection.*

---

[1] This objective includes the completion of the OMB *FY 2008 FISMA Reporting Template for IGs*, which is presented in Appendix I of this report.

To accomplish our objectives, KPMG 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 the Top-Down Department level for Treasury-wide program level controls and Bottom-Up Bureau level implementation perspective, including the implementation of the security control catalog outlined in NIST SP 800-53 Rev. 2. We also reviewed Treasury's progress in preparing plans to protect information technology (IT)-related CI/KR. We considered each area above to reach conclusions with regard to the adequacy of the Treasury's information security program and practices.

During our FY 2008 audit, we noted that the 12 non-IRS Treasury bureaus have made progress in improving information security controls and practices.[2] Following our 2007 security evaluation, Treasury strengthened its inventory reporting and Plan of Action and Milestones (POA&M) processes by more effectively using the Trusted Agent FISMA (TAF) system to serve as the consolidated FISMA inventory system of record for Treasury and as the POA&M centralized, Treasury-wide system for tracking IT security weaknesses.[3]

Based on our 2008 FISMA audit, we determined that Treasury had implemented all provisions of HSPD-7 and OMB Memorandum 04-15 *Development of Homeland Security Presidential Directive (HSPD) - 7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources*. This included the development of critical infrastructure plans in identifying, prioritizing, protecting, and planning for contingencies related to IT-related CI/KR of Treasury bureaus and those under direction and control of the Office of the Chief Information Officer (OCIO).

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 Standards (FIPS) 200 Minimum Security Control Baselines Were Not Sufficiently Documented, Tested, and/or Implemented.** Treasury has made progress in addressing information security risk management requirements as required by 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. However, we noted that the minimum security controls required by NIST FIPS 200 were not documented, tested, and/or implemented for the eight (8) non-IRS information systems (or 35% of the representative subset of Treasury information systems) reviewed as part of our representative subset of Treasury information systems. In addition, one (1) deficiency related to certification and accreditation documentation in our FY 2007 report had not been resolved.

2. **Computer Security Incidents Were Not Consistently Reported Timely or Correctly Categorized.** Nine (9) computer security incidents across six (6) bureaus were not assigned the correct United States Computer Emergency Readiness Team (US-CERT) incident categorization as required by Treasury policy, and nine (9) other computer security incidents across seven (7) bureaus were not reported within the timeframes outlined by the US-CERT.

3. **Common Security Configuration Baselines Were Not Fully Compliant.** Treasury has established a Department-wide configuration management policy requiring all information systems to implement NIST SP 800-70 common security configuration baselines. However, we

---

[2] The FISMA evaluation of the IRS is performed by TIGTA.
[3] 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.

noted two (2) systems (or 17% of the representative subset of Treasury information systems) had not utilized NIST SP 800-70 common security configurations.

4. **Federal Desktop Core Configurations Were Not Fully Implemented.** Treasury has made substantial progress in the implementation of Federal Desktop Core Configuration (FDCC) secure configuration baselines since the issuance of OMB Memorandum 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*. However, we noted four (4) bureaus had not completed the implementation and validation of FDCC secure baseline configurations.

As part of the FISMA audit 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. Overall, we determined that an information security program is in place and is generally consistent with FISMA; however, Treasury did not fully comply with the requirements of NIST SP 800-53, as of June 30, 2008. Specifically, we determined from a sample of systems reviewed that 35% of Treasury non-IRS systems did not fully comply with NIST SP 800-53 minimum security control catalog requirements. We are reporting exceptions with the extent NIST 800-53 minimum security control catalogs were documented, implemented or tested. All of our findings are included in the results section of this report, which warrants management attention and corrective action. Management concurs with all reported findings and recommendations. The OCIO's written response to our draft report, dated September 15, 2008, is included within this report.

This performance audit did not constitute an audit of financial statements in accordance with *Government Auditing Standards*. KPMG was not engaged to, and did not, render an opinion on Treasury's internal controls over financial reporting or over financial management systems (for purposes of OMB Circular No. A-127, *Financial Management Systems*, July 23, 1993, as revised). KPMG cautions that projecting the results of our evaluation to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

Sincerely,

KPMG LLP

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. The Act assigns specific responsibilities to agency heads and Inspectors General (IGs) supported by security policy promulgated through OMB and risk-based standards and guidelines published by NIST. For FY 2008, the OIG awarded a contract to KPMG to perform the FISMA audit for Treasury's non-IRS unclassified systems in accordance with GAGAS.

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 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, the standard states that selected set of security controls must include one of three 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 to 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 this guide, 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.

On December 17, 2003, the President signed HSPD-7, which established a national policy for Federal departments and agencies to identify and prioritize United States CI/KR in order to protect them from terrorist-related attacks. HSPD-7 instructed Federal agencies and departments to prepare plans for the protection of physical and cyber-related CI/KR, both owned and operated. On June 17, 2004, the OMB issued Memorandum M-04-15, with the purpose of further defining the requirements of HSPD-7, as well as for providing instructions for the development of Critical Infrastructure Protection (CIP) plans. The purpose of the CIP plan is to identify, prioritize, protect, and plan for contingencies related to the CI/KR of each agency and department.

Treasury Information Security Management and Program

Treasury is comprised of 13 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, many stamps, 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.
- **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.
- **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.

- **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 OCIO

The Treasury Chief Information Officer (CIO) is responsible for providing Department-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. Through its mission, the Treasury 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 Treasury 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 CIP
- 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, 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 and the Cyber Security program have the responsibility of managing Treasury's IT CIP program for Treasury assets.

Bureau OCIO

Bureau OCIO organizations are led 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 both Treasury OCIO policy and guidance and Federal statutes, regulations, policy, and guidance. 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.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objectives of our audit were to determine as of June 30, 2008, whether non-IRS Treasury bureaus had implemented:

- An information security program, consisting of plans, policies, procedures, and security controls consistent with FISMA[4]
- The security controls catalog contained in the NIST SP 800-53 Rev. 2
- Plans for protecting physical and cyber CI/KR consistent with paragraphs 1 through 11 of HSPD-7.

To accomplish our objectives, KPMG 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 Top-Down Department Level for Treasury-wide program level controls and Bottom-Up Bureau Level implementation perspective, including NIST SP 800-53 minimum security control baselines established by NIST FIPS 200. We also reviewed Treasury's progress in preparing plans to protect cyber Critical Infrastructure. We considered each area above to reach conclusions with regard to the adequacy of Treasury's information security program and practices.

Top-Down Department Level

To gain an overall enterprise-level understanding, KPMG 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.

Bottom-Up Bureau Level

As required by FISMA, KPMG also performed tests for a representative subset of 23 information systems 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 sampling approach). The subset of systems encompassed systems managed and operated by 12 of 13 Treasury bureaus 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. 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.

---

[4] This objective includes the completion of the OMB FY 2008 FISMA Reporting Template for IGs, which is presented in Appendix I of this report.

Table 1: Security Control Classes and Families[5]

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

In accordance to 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. 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 this guide, NIST in July 2008 released SP 800-53A, which provides recommended guidance for agencies to follow in their security control assessment and continuous monitoring process. KPMG's control evaluation review for controls selected was based on the assessment steps recommended in NIST SP 800-53A.

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

- Highly volatile controls that have the potential to affect the greatest 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.

---

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

HSPD--7

KPMG assessed Treasury's progress in preparing plans to protect IT-related CI/KR, owned or operated including leased facilities. This included assessing development of CIP plans in accordance to OMB Memorandum 04-15. These plans must address identification, prioritization, protection, and contingency planning, including recovery and reconstitution of essential capabilities. In particular, we assessed whether plans address protection priorities, ability to ensure continuity of operations during a cyber attack, and where current capabilities are lacking, POA&Ms to achieve the necessary level of performance.

Other Considerations

In performing our control evaluations, KPMG interviewed key Treasury OCIO personnel who had significant information security responsibilities as well as personnel across the 12 non-IRS operating bureaus. 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.

We also relied on security-related audit, review, and evaluation reports issued by the OIG, Treasury, and the Government Accountability Office (GAO) as of August 29, 2008. To assure ourselves that we could rely on pertinent information contained in these reports, we performed procedures, such as obtaining an understanding of the methodologies, assumptions, and conclusions described therein. We also performed procedures to assure ourselves that computer-based data was valid and reliable when that data was significant to our evaluation findings and conclusions. Such procedures included verifying selected automated data to source documentation and corroborating automated data through interviews with appropriate Treasury personnel.

We performed our audit at Treasury's headquarters offices in Washington, DC and bureau locations in Washington, DC, Hyattsville, MD, McLean, VA, and Parkersburg, WV during the period of May through August 2008. During our audit, we met with Treasury management to discuss our preliminary conclusions. Our audit was conducted in accordance with GAGAS (prescribed by the Comptroller General of the United States) and included such tests as we considered necessary.

Applicable Criteria

KPMG's approach to this FISMA performance audit 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.[6]

- OMB Circular A-130, *Management of Federal Information Resources*
- NIST FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*

---

[6] 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.

- NIST FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP:
  - 800-53 Rev. 2 *Recommended Security Controls for Federal Information Systems*
  - 800-53A *Guide for Assessing the Security Controls in Federal Information Systems*
  - 800-39 *Managing Risk from Information Systems: An Organizational Perspective*
  - 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*
  - 800-70 *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*
  - 800-18 Rev. 1 *Guide for Developing Security Plans for Information. Technology System*
  - 800-16 *Information Technology Security Training Requirements: A Role- and Performance-Based Model*
  - 800-61 *Computer Security Incident Handling Guide*
  - 800-60 *Guide for Mapping Types of Information and Information Systems to Security Categories*
  - 800-34 *Contingency Planning Guide for Information Technology Systems*
  - 800-30 *Risk Management Guide for Information Technology Systems*
- OMB Memoranda
  - 08-21 *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
  - 04-04 *E-Authentication Guidance for Federal Agencies*
  - 04-15 *Development of Homeland Security Presidential Directive (HSPD) - 7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources*
  - 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*
  - 07-18 *Ensuring New Acquisitions Include Common Security Configurations*
- HSPD-7 paragraphs 1 through 11

RESULTS

During our FY 2008 FISMA audit, we noted that the 12 non-IRS Treasury bureaus have made progress in improving information security controls and practices.[7] Following our 2007 security evaluation, Treasury strengthened its inventory reporting and POA&M processes by more effectively using the TAF system to serve as the consolidated FISMA inventory system of record for the department and as the centralized Department-wide POA&M system for tracking IT security weaknesses.[8]

Based on our FY 2008 FISMA audit, we noted four areas needing improvement. These areas are i) NIST FIPS 200 minimum security control baselines were not sufficiently documented, tested, and/or implemented; ii) computer security incidents were not consistently reported timely or correctly categorized; iii) common security configuration baselines were not fully compliant; and iv) FDCCs were not fully implemented. 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.

In addition, we determined that Treasury had implemented all provisions of HSPD-7 and OMB Memorandum 04-15. Specifically, Treasury had implemented a program to identify, prioritize, and protect all IT/cyber-related CI/KR in accordance with HSPD-7 and OMB Memorandum 04-15. We reviewed documentation and processes for CIP plans to determine if CI/KR are managed in accordance with the applicable criteria. The Treasury OCIO Cyber Security program manages the CIP process. The OCIO Cyber Security program has developed a CIP policy in TD P 85-01 that was derived from guidance in HSPD-7 and OMB Memorandum 04-15. Additionally, the OCIO Cyber Security program developed CIP processes and procedures in a CIP plan in accordance with OMB Memorandum 04-15. The CIP plan was finalized in December 2005 and is updated annually. The CIP plan addresses the identification, prioritization, and protection of IT-related CI/KR for all Treasury bureaus in three phases: prepare and prevent, detect and respond, and recover and reconstitute.

FINDINGS

1. **NIST FIPS 200 Minimum Security Control Baselines Were Not Sufficiently Documented, Tested, and/or Implemented**

   Treasury has made progress in addressing information security risk management requirements as required by 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.   However, we noted that the minimum security controls required by NIST FIPS 200 were not documented, tested, and/or implemented for eight (8) systems with our representative subset of non-IRS Treasury information systems. Specifically, for the eight (8) information systems (or 35% of the representative subset of Treasury information systems) reviewed, and one system that was identified as a deficiency in our FY 2007 report, we noted:

   - Instances of inadequate testing were identified over the minimum security control baselines implemented for four (4) systems at BEP and three (3) systems at TTB. In addition, the system security plan for each of these systems had not been updated to document the

---

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

[8] 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.

minimum security control baseline implemented, per NIST FIPS 200, NIST SP 800-53 Rev. 2, and NIST SP 800-18 Rev. 1.

Regarding the four (4) BEP systems, the system security plan was originally developed prior to the release of the final version of NIST SP 800-53. As a result, the system security plan only included the 17 NIST SP 800-53 control families, but not the specific controls within each family. In 2008, BEP management had not yet updated the system security plan to include each specific security control with the NIST SP 800-53 Rev. 2 security control baseline for a system with a FIPS 199 system impact level of Moderate. Additionally, during the security test and evaluation and continuous security control monitoring of the one (1) BEP system, only those specific controls outlined in the original system security plan were tested.

Regarding the three (3) TTB systems, a third party was used to perform the security test and evaluation and the continuous security controls monitoring. TTB management believed that the methodology employed by this third party incorporated NIST SP 800-53 and NIST SP 800-53A to assess all minimum security controls over a three-year period. However, it was found that only technical controls had been tested. TTB management also stated that the results of testing over each specific NIST SP 800-53 control in the security control baseline were not documented in the security test and evaluation report or in continuous security controls monitoring documentation prior to granting the authority to operate in June of the FY 2008 FISMA reporting period.

- The weaknesses identified through the security test and evaluation related to one (1) system at OTS selected as part of our representative subset identified that the 17 security control families required by NIST FIPS 200 for a system with a NIST FIPS 199 system impact level of Moderate had not been fully implemented. This system has been issued an Interim Authority to Operate (IATO) by OTS because of the security control weaknesses identified during the security test and evaluation. The previous OTS FISMA system inventory organized systems into business process, rather then functional IT units. The authorities to operate for each system in the prior OTS FISMA system inventory expired during the FY 2007 FISMA reporting period. OTS elected not to recertify and accredit each system due to plans to redefine the bureau's FISMA system inventory, which occurred in the FY 2008 FISMA report period. The security test and evaluation undertaken for the one (1) system selected identified a number of security weaknesses relative to the NIST SP 800-53 security control baseline for a Moderate system, which subsequently created an operating environment that was inadequate to support full system accreditation.

- The contingency plan for one (1) system at the CDFI Fund was missing elements required by NIST SP 800-34. This condition was also noted in the 2007 FISMA evaluation. CDFI Fund management stated that sufficient resources have not been dedicated to update the plan in accordance with NIST SP 800-34. In FY 2008, CDFI Fund management had only dedicated limited resources to update the plan; however, the updates were not completed by the end of the FISMA reporting period. CDFI Fund management estimates that the plan will be updated by the end of the FY 2009 FISMA reporting period.

The Treasury OCIO Cyber Security program has implemented program-level controls for the oversight of the certification and accreditation process across the Department. The program controls are outlined as roles and responsibilities in TD P 85-01 – Treasury Information Technology Security Manual. This document states that one of the responsibilities of the ACIOCS is to monitor and evaluate the status of the Treasury IT security posture by performing

compliance reviews of bureau IT security programs and system controls, including reviews of certification and accreditation documentation. To execute this responsibility, the ACIOCS has directed the Cyber Security program to perform two (2) types of monitoring and evaluation activities. The first type of activity is a Technical Security Review, which includes vulnerability assessments, penetration tests, and configuration reviews (including FDCC). The second type of activity is a Security Program Review, which encompasses reviews of bureau level policies, procedures, and the certification and accreditation documentation. The ACIOCS has developed a plan to perform a Technical Security Review and Security Program Review at each bureau on an annual basis. Through the Security Program Review, the Cyber Security program performs procedures to determine if a bureau has loaded all of the required FISMA artifacts into TAF and if the artifacts have been developed in accordance with OCIO policies, as well as OMB and NIST laws, policies, and guidance. However, based on the documentation provided, these procedures appear to only be designed to determine if a bureau has loaded all FISMA artifacts into TAF and not determine compliance with Treasury policy, as well as OMB and NIST laws, policy, and guidance.

The Treasury OCIO Cyber Security program is performing these activities as stated. However, oversight and improvements by the ACIOCS and the Cyber Security program are needed to ensure a consistent approach to the design, implementation, and/or testing of NIST SP 800-53 minimum security control baselines required by NIST FIPS 200. While it was noted that a Security Program Review was conducted at all 12 non-IRS Treasury bureaus during the FY 2008 FISMA reporting period, we were unable to determine if these reviews would identify the specific deviations identified.

In all cases noted above, there is a risk that the confidentiality, integrity, and availability of the bureau's sensitive or Personally Identifiable Information (PII) and information systems that support the mission of the bureau are susceptible to compromise by not applying minimum security standards in accordance to NIST FIPS 200 requirements.

For BEP, we recommend that management:

1. The system security plan be updated to include all baseline security controls for a system with a FIPS 199 system impact level of Moderate.

2. All security controls be tested within the NIST FIPS 200 minimum security control baseline, based on the system's FIPS 199 system impact level during the systems recertification and accreditation in the FY 2009 FISMA reporting period, or during the next three-year certification and accreditation period through continuous monitoring.

For TTB, we recommend that management:

3. Implement, document, and test management, operational, and technical security controls across each of the 17 security control families of NIST SP 800-53 Rev. 2.

4. Re-consider the decision to issue a full authority to operate based on the assessment of the implementation of the management, operational, and technical security controls across all 17 security controls families of NIST SP 800-53 Rev. 2.

5. Review its certification and accreditation process to prevent other systems from being granted full authority to operate when NIST FISP 200 minimum security standards are not met.

For OTS, we recommend that management:

6. Continue with bureau plans to resolve the security weaknesses identified during the certification and accreditation process by the end of the interim authorization period, December 31, 2008, and achieve a full authority to operate during the FY 2009 FISMA reporting period.

For CDFI, we recommend that management:

7. The one (1) system contingency plan be updated to include a business impact analysis and equipment replacement strategy in accordance with NIST SP 800-34.

In addition, we recommend that the Treasury OCIO management:

8. Provide additional oversight to monitor and enforce compliance with Treasury OCIO policies, as well as OMB and NIST laws, policies, and guidance with respect to the documentation, implementation, and testing of the minimum security control baselines required by NIST FIPS 200.

2. Computer Security Incidents were not Consistently Reported Timely or Correctly Categorized

We reviewed thirty-eight (38) computer security incidents out of a population of 147, and noted the following discrepancies:

- Nine (9) computer security incidents across six (6) bureaus were not assigned the correct US-CERT incident categorization as required by Treasury Chief Information Officer (TCIO) Memorandum 06-12, *Cyber Security Incident Response (Non-National Security Systems)* and TCIO Memorandum 08-02, *Cyber Security Incident Handling Guidelines and Clarifications for Treasury Directive Publication 85-01*. Of the nine (9) computer security incidents, one (1) involved a breach of PII and eight (8) involved the loss of portable computing equipment.

- Three (3) computer security incidents across three (3) bureaus were not reported within the timeframes outlined by the US-CERT.

TCIO Memorandum 06-02, *Cyber Security Incident Response (Non-National Security Systems)* requires that each bureau's Computer Security Incident Response Capability (CSIRC) categorize significant incidents based on the US-CERT definitions for Category 1-4 computer security incidents. Table 2 outlines the US-CERT definitions of Category 1-4 computer security incidents.

Table 2: US-CERT Definition of Category 1-4 Computer Security Incidents[9]

Category	Category Name	Description	Reporting Timetable
Category 1	**Unauthorized Access**	In this category, an individual gains logical or physical access without permission to a Federal agency network, system, application, data, or other resource.	Within one (1) hour of discovery/detection.
Category 2	**Denial of Service (DoS)**	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
Category 3	**Malicious Code**	*Successful* installation of malicious software (i.e., virus, worm, spyware, bots, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application). Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection *if* widespread across agency.
Category 4	**Improper Usage**	A person violates acceptable computing use policies.	Weekly.

In addition, per TCIO Memorandum 06-02, the Department of Homeland Security has clarified that a US-CERT category 1 computer security incident reporting level should be used for physical loss of equipment that could result in unauthorized access to systems or information.

Our analysis concluded that improvements are needed to provide for an enterprise-wide approach to the TCSIRC processes. The policy specifies that the TCSIRC serves as the central clearing house for external computer security incident reporting. In addition, Treasury OCIO policy also states that it is the responsibility of each bureau-level CSIRC to create computer security incident response training programs, or to include computer security incident response training with their specialized security training programs. However, the Treasury OCIO Cyber Security program and the TCSIRC are not providing the needed oversight to ensure the consistency and adequacy of the computer incident response training programs at each non-IRS bureau.

Late or mis-categorized computer security incidents could limit Treasury's ability to timely and accurately report computer security incidents according to policies and procedures.

---

[9] Source: Treasury CIO Memorandum 06-02 *Cyber Security Incident Response (Non-National Security Systems)*

We recommend that the ACIOCS:

9. Evaluate viable alternatives to improve bureau level awareness capabilities by providing and/or assisting bureaus with the development and implementation of incident response awareness programs.

3. Common Security Configuration Baselines Were Not Fully Compliant

Treasury has established a Department-wide configuration management policy requiring all information systems to implement NIST SP 800-70 common security configuration baselines. However, we noted one (1) system at BPD and one (1) system at OTS (or 17% of the representative subset of Treasury information systems) had not utilized NIST SP 800-70 common security configurations. Common security configuration baselines were not developed for the one (1) system at BPD at time of fieldwork. In addition, competing resource requirements at OTS have prevented NIST SP 800-70 common security configuration baselines from being fully utilized to-date.

By not having a NIST SP 800-70 compliant secure configuration baseline documented and implemented, the ability of these bureaus to apply a consistent security configuration across platforms and operating systems may be impaired. This could lead to the increased risk of exposure relative to the confidentiality, integrity, and availability of sensitive information and information systems controlled by these operating systems.

We recommended that:

10. Both BPD and OTS utilize NIST SP 800-70 common security configurations on the two (2) systems reported.

4. Federal Desktop Core Configurations Were Not Fully Implemented

Treasury has made substantial progress in the implementation of FDCC secure configuration baselines since the issuance of OMB Memorandum 07-11. However, we noted that DO, FinCEN, the OIG, and OTS had not completed the implementation and validation of FDCC secure baseline configurations. First, at DO and the OIG, current network technology limitations have prevented them from implementing FDCC secure configuration baselines on all instances of the Microsoft Windows XP operating system. Second, at FinCEN, a lack of technical knowledge has prevented the bureau from fully implementing FDCC secure configuration baselines across all instances of the Microsoft Windows XP operating system. Third, OTS management indicated that unclear guidance from NIST and a constantly changing FDCC baseline has resulted in OTS being unable to fully test and implement all FDCC baseline configurations. However, OTS management also stated that several controls have been implemented to mitigate the potential risk posed by not implementing all FDCC secure configurations.

By not applying the FDCC secure baseline configuration requirements for Windows XP, Treasury 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:

11. DO, FinCEN, the OIG, and OTS work to implement FDCC secure configuration baselines on all Microsoft Windows XP workstations.

CONCLUSIONS

As part of the FISMA audit 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. Overall, we determined that an information security program is in place and is generally consistent with FISMA; however, Treasury did not fully comply with the requirements of NIST SP 800-53, as of June 30, 2008. Specifically, we determined from a sample of systems reviewed that 35% of Treasury non-IRS systems did not fully comply with NIST SP 800-53 minimum security control catalog requirements. We are reporting exceptions with the extent NIST 800-53 minimum security control catalogs were documented, implemented or tested. All of our findings are included in the results section of this report, which warrants management attention and corrective action.

Additionally, we obtained evidence to assess Treasury's compliance with HSPD-7 paragraphs 1-11 and related OMB guidance. We determined that Treasury had implemented all provisions of HSPD-7 paragraphs 1-11 and related OMB guidance, and included the development of critical infrastructure plans in identifying, prioritizing, protecting, and planning for contingencies related to IT-related CI/KR of Treasury bureaus and those under direction and control of the OCIO.

MANAGEMENT RESPONSE TO DRAFT REPORT

The following is the OCIO's response to the draft FISMA FY 2008 Performance Audit report dated, September 15, 2008.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 26, 2008

MEMORANDUM FOR JOEL GROVER
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
FINANCIAL MANAGEMENT AND IT AUDITS

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

SUBJECT: CIO Response to Draft FISMA Report

Thank you for the opportunity to review and comment on the draft report entitled: "INFORMATION TECHNOLOGY: Federal Information Security Management Act Fiscal Year 2008 Performance Audit." We are pleased that the audit recognized Treasury's progress in Federal Information Security Management Act (FISMA) implementation, particularly with regard to our system inventory, Plans of Action and Milestones process, and Security Configuration Management and determined Treasury's information security program is in place and consistent with FISMA. We agree with the findings and recommendations.

The OCIO continuously strives to improve the Department's information technology (IT) security program. We have a comprehensive program in place to monitor and review performance metrics, and assess Bureau compliance with Department and Government-wide policy and standards. The continued improvement shown by the Department and Bureaus is evidence of the effectiveness of this program. In addition, I recently added formal, quarterly progress reports to Bureau CIOs to augment my executive-level oversight of outstanding action items.

We remain committed to sustaining a mature IT security program and providing the appropriate protection of personal information throughout the Department. I believe we are on a course of continued progress, and I look forward to continuing to partner with the Treasury Office of the Inspector General towards this objective.

Should you have any questions pertaining to this response, please do not hesitate to contact me at (202) 622-1200.

Attachment

ATTACHMENT

MANAGEMENT RESPONSE TO TREASURY OIG DRAFT
RECOMMENDATIONS

**OIG Finding 1: NIST FIPS 200 Minimum Security Control Baselines Were Not
Sufficiently Documented, Tested, and/or Implemented.**

OIG Recommendation 1: For BEP, we recommend the System Security Plan (SSP) be
updated to include all baseline security controls for a system with a FIPS 199 system
impact level of Moderate.

Treasury Response: Treasury concurs with this recommendation.
In the FY 2009 FISMA reporting period, BEP will execute their C&A activities and
continue to update SSPs to include all baseline security controls for a system with a FIPS
199 system impact level of Moderate in their SSP as required by NIST, Treasury, and
Bureau policy in effect at the time of the C&A.

OIG Recommendation 2: For BEP, we recommend all security controls be tested
within the NIST FIPS 200 minimum security control baseline, based on the system's
FIPS 199 system impact level during the systems recertification and accreditation in the
FY 2009 FISMA reporting period, or during the next three-year certification and
accreditation period through continuous monitoring.

Treasury Response: Treasury concurs with this recommendation.
For the FY 2009 FISMA reporting period, BEP will execute their C&A and continuous
monitoring activities, and continue to test the NIST FIPS 200 minimum security control
baseline based on the system's FIPS 199 system impact level.

OIG Recommendation 3: For TTB, we recommend that management implement,
document, and test management, operational, and technical security controls across each
of the 17 security control families of NIST SP 800-53 Rev. 2.

Treasury Response: Treasury concurs with this recommendation.
In the FY 2009 FISMA reporting period, TTB will execute security control activities in
compliance with policy.

OIG Recommendation 4: For TTB, re-consider the decision to issue a full authority to
operate based on the assessment of the implementation of the management, operational,
and technical security controls across all 17 security controls families of NIST SP 800-53
Rev. 2.

Treasury Response: Treasury concurs with this recommendation.
In the FY 2009 FISMA reporting period, TTB will execute C&A related testing consistent with the revised NIST standards and provide authorizing officials with the appropriate information to make sound accreditation decisions in compliance with policy.

OIG Recommendation 5: For TTB, review its certification and accreditation process to prevent other systems from being granted full authority to operate when NIST FIPS 200 minimum security standards are not met.

Treasury Response: Treasury concurs with this recommendation.
In the FY 2009 FISMA reporting period, TTB will execute C&A activities to provide authorizing officials with the necessary information to make sound accreditation decisions in compliance with policy.

OIG Recommendation 6: For OTS, we recommend that management continue with bureau plans to resolve the security weaknesses identified during the certification and accreditation process by the end of the interim authorization period, December 31, 2008, and achieve a full authority to operate during the FY 2009 FISMA reporting period

Treasury Response: Treasury concurs with this recommendation.
In the FY 2008 FISMA reporting period, OTS complied with existing NIST, Treasury, and Bureau policy in granting an interim authority to operate. An interim authorization to operate is rendered when the identified security vulnerabilities in the information system resulting from deficiencies in the planned or implemented security controls are significant but can be addressed in a timely manner.

In FY 2009 FISMA reporting period, OTS will aggressively pursue their C&A plans for systems to achieve full authority to operate.

OIG Recommendation 7: The one CDFI system contingency plan be updated to include a business impact analysis and equipment replacement strategy in accordance with NIST SP 800-34.

Treasury Response: Treasury concurs with this recommendation.
CDFI will update their Contingency Plan to include a business impact analysis and equipment replacement strategy in accordance with NIST SP 800-34 by June 30, 2009.

OIG Recommendation 8: Additional oversight by the Treasury OCIO Cyber Security program to enforce and monitor compliance with Treasury OCIO policies, as well as OMB and NIST laws, policies, and guidance, with respect to the documentation, implementation, and testing of the minimum security control baselines required by NIST FIPS 200.

Treasury Response: Treasury concurs with this recommendation.
Treasury has an extensive oversight and compliance program in place that includes program and technical reviews as well as weekly, monthly, and quarterly Bureau reporting and Treasury review. Both the OIG and TIGTA FISMA evaluations from 2005-2008 clearly demonstrate Treasury's progress and effectiveness of OCIO oversight. Nonetheless, Treasury recognizes the need to continuously improve its IT security program. During the FY 2009 FISMA reporting period, the OCIO will work with Bureaus to address issues identified in the 2008 FISMA audit report.

OIG Finding 2 - Computer Security Incidents were not Consistently Reported Timely or Correctly Categorized.

OIG Recommendation 9: Evaluate viable alternatives to improve bureau level awareness capabilities by providing and/or assisting bureaus with the development and implementation of incident response awareness programs.

Treasury Response: Treasury concurs with the recommendation.
We recognize that some administrative reporting errors were identified through the FISMA FY-2008 audit. Treasury OCIO will provide additional training, guidance and assistance to the Bureaus to address this issue.

OIG Finding 3: Configuration Baselines Were Not Fully Compliant.

OIG Recommendation 10: Both BPD and OTS utilize NIST SP 800-70 common security configurations on the two systems reported.

Treasury Response: Treasury concurs with the recommendation.
In the FY-2009 FISMA reporting period, these Treasury Bureaus will identify and implement appropriate baselines for the systems noted in the audit report.

OIG Finding 4: Federal Desktop Core Configurations Were Not Fully Implemented

OIG Recommendation 11: DO, FinCEN, the OIG, and OTS work to implement FDCC secure configuration baselines on all Microsoft Windows XP workstations.

Treasury Response: Treasury concurs with this recommendation.
DO, FinCEN, the OIG, and OTS are executing detailed project plans to implement FDCC secure configuration baselines on all Microsoft Windows XP workstations by December 31, 2009. All are in compliance with OMB/NIST guidance on FDCC implementation.

APPENDIX I - OIG RESPONSE TO THE FY 2008 OMB FISMA REPORTING QUESTIONS

OMB's FY2008 FISMA Reporting Template for IGs includes the following questions, which are to be addressed by the Treasury OIG and TIGTA:[10]

- Question 1 – FISMA 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 Impact Assessment (PIA) Process[11]
- Question 7 – IG Assessment of the Agency Privacy Program[12]
- Question 8 – Configuration Management
- Question 9 – Incident Reporting
- Question 10 – Security Awareness Training
- Question 11 – Collaborative Web Technologies and Peer-to-peer File Sharing
- Question 12 – E-Authentication Risk Assessments

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 2008 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 2008 Reporting Template for IGs. The Treasury's responses to the FY 2008 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 developed by KPMG, under contract with the Treasury OIG. KPMG does not take responsibility for the evaluation performed by TIGTA over the IRS.

Detailed Description of the Responses to the FY 2008 Reporting Template for IGs[13]

FISMA System Inventory/Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory (Questions 1&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 Department'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

---

[10] The Treasury's IGs include both the Treasury OIG and TIGTA.

[11] A separate performance audit report on the Treasury's compliance with Section 522, Division H of the Consolidated Appropriations Act, 2005, and the provisions of OMB Memorandum 07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* will be issued.

[12] A separate performance audit report on the Treasury's compliance with Section 522, Division H of the Consolidated Appropriations Act, 2005, and the provisions of OMB Memorandum 07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* will be issued.

[13] Individual non-IRS bureaus have been notified of the detail observations identified during fieldwork separately.

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 noted 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.

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 within our representative subset of information systems is operating with an IATO. Per NIST SP 800-37, an IATO does not represent a full system accreditation. Lastly, 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 2008 FISMA reporting period.

Evaluation of Agency POA&M Process (Question 4)

Treasury has implemented policies for the creation and maintenance of POA&Ms and has implemented the TAF system to serve as the centralized, Department-wide system for tracking IT security weaknesses. Treasury CIO Memorandum, 06-01 *Improving the Department's Security Plan of Action and Milestone (POA&M) Process* provides guidance for the inclusion of IT security weaknesses in POA&Ms and for the prioritization of POA&Ms weaknesses. The Treasury OCIO Cyber Security program also requires bureaus to follow OMB Memorandum 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* as guidance for properly document and reporting POA&Ms weaknesses.

Treasury is using the TAF system to track all known weaknesses from all sources, including IG reports, on a continuous basis. Each weakness has been documented in accordance with OMB Memorandum 04-25 and has been prioritized. For weaknesses that were not uploaded into TAF, we noted that a bureau system-level POA&M for each of those weaknesses existed. TAF also allows for the continuous updating bureau-level POA&Ms with newly identified weaknesses and the status of exist weaknesses. Individual bureaus are permitted to have internal POA&M weakness tracking mechanisms, however quarterly updates must be made to TAF.

IG Assessment of the Certification and Accreditation (C&A) Process/Implementation of the Security Control Catalog Contained in NIST SP 800-53 Rev.2 (Question 5)

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

Configuration Management (Question 8)

Refer to Finding No. 3 and No. 4 in the Results section of this report on page 17.

Incident Reporting (Question 9)

Refer to Finding No. 2 in the Results section of this report on page 15.

Security Awareness Training (Question 10)

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 improved its security awareness training program since the FY 2007 FISMA reporting period. Out of a sample of 360 employees and contractors across the Department, only five (5) did not attend IT security awareness training within the FY 2008 FISMA reporting period. Of these five (5), two (2) were outside visitors who require periodic network access for training and meetings. However, the network accounts belonging to these individuals were disabled at the time of fieldwork. We noted that these deviations represented only a minimal rate of control failure, based on the total sample size of 360 employees and contractors across all 12 non-IRS bureaus, and did not represent a control weakness.

Collaborative Web Technologies and Peer-to-Peer File Sharing (Question 11)

Treasury has established a Department-wide policy in TD P 85-01 for the inclusion of collaborative web technologies and 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 have incorporated collaborative web technologies and peer-to-peer file sharing within their IT security awareness training programs.

E-Authentication Risk Assessments (Question 12)

Treasury has established a Department-wide policy in TD P 85-01, which requires bureaus to conduct an e-authentication risk analysis in accordance with OMB Memorandum 04-04 *E-Authentication Guidance for Federal Agencies*. Bureaus have either validated that an E-authentication risk assessment was not required by completing a questionnaire to determine the types of information the system is processing or by identifying the type of transactions the system is processing in the security plan. Three (3) of twenty-three (23) systems selected in our representative subset of Treasury information systems required an E-Authentication Risk Assessment. Each had an E-Authentication Risk Assessment in accordance with OMB Memorandum 04-04.

OMB FY 2008 Reporting Template for IGs

Question 1: FISMA Systems Inventory

1. **As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.**

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by Component/Bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self-reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

2.   **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.**

		Question 1						Question 2					
		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	2	0	0	0	2	0	0	0	0	0	0	0
	Moderate	39	3	2	0	41	3	3	100%	3	100%	3	100%
	Low	9	1	0	0	9	1	1	100%	1	100%	1	100%
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0

Bureau Name	FIPS 199 System Impact Level	Question 1						Question 2					
		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	
		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
	Sub-total	**50**	**4**	**2**	**0**	**52**	**4**	**4**	100%	**4**	100%	**4**	100%
BPD	High	2	0	0	0	2	0	0	0	0	0	0	0
	Moderate	12	2	0	0	12	2	2	100%	2	100%	2	100%
	Low	6	1	0	0	6	1	1	100%	1	100%	1	100%
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Sub-total	**20**	**3**	**0**	**0**	**20**	**3**	**3**	100%	**3**	100%	**3**	100%
CDFI	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	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
	Sub-total	**3**	**0**	**0**	**0**	**3**	**0**	**0**	0	**0**	0	**0**	0
DO	High	11	1	3	1	14	2	2	100%	2	100%	2	100%
	Moderate	22	2	6	1	28	3	3	100%	3	100%	3	100%
	Low	13	3	2	0	15	3	3	100%	3	100%	3	100%
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Sub-total	**46**	**6**	**11**	**2**	**57**	**8**	**8**	100%	**8**	100%	**8**	100%
FinCEN	High	5	0	0	0	5	0	0	0	0	0	0	0
	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
	Sub-total	**8**	**0**	**0**	**0**	**8**	**0**	**0**	0	**0**	0	**0**	0
FMS	High	8	0	3	0	11	0	0	0	0	0	0	0
	Moderate	32	3	2	0	34	3	3	100%	3	100%	3	100%
	Low	9	1	0	0	9	1	1	100%	1	100%	1	100%

	FIPS 199 System Impact Level	Question 1						Question 2					
		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	
		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
	Sub-total	49	4	5	0	54	4	4	100%	4	100%	4	100%
IRS	High	4	0	0	0	4	0	0	0	0	0	0	0
	Moderate	184	14	6	1	190	15	15	100%	15	100%	15	100%
	Low	53	7	0	0	53	7	7	100%	7	100%	7	100%
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Sub-total	241	21	6	1	247	22	22	100%	22	100%	22	100%
Mint	High	0	0	0	0	0	0	0	0	0	0	0	0
	Moderate	15	0	1	0	16	0	0	0	0	0	0	0
	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
	Sub-total	18	0	1	0	19	0	0	0	0	0	0	0
OCC	High	0	0	0	0	0	0	0	0	0	0	0	0
	Moderate	15	0	0	0	15	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
	Sub-total	16	0	0	0	16	0	0	0	0	0	0	0
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
	Sub-total	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

Bureau Name	FIPS 199 System Impact Level	Question 1						Question 2					
		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	
		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
	Moderate	8	1[14]	0	0	8	1	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
	Sub-total	8	1	0	0	8	1	0	0%	0	0%	0	0%
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
	Not Categorized	0	0	0	0	0	0	0	0	0	0	0	0
	Sub-total	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	3	0	0	17	3	3	100%	3	100%	3	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
	Sub-total	18	3	0	0	18	3	3	100%	3	100%	3	100%
Agency Totals	High	32	1	6	1	38	2	2		2		2	
	Moderate	351	28	17	2	368	30	29		29		29	
	Low	97	13	2	0	99	13	13		13		13	
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Total	480	42	25	3	505	45	44		44		44	

[14] One OTS system selected in our representative subset of Treasury information system was identified as operating with an IATO.

	Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory	
3.a.	**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.** **Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.** Response Categories: - Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	Almost Always- for example, approximately 96-100% of the time
3.b.	**The agency has developed a complete inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.** Response Categories: - The inventory is approximately 0-50% complete - The inventory is approximately 51-70% complete - The inventory is approximately 71-80% complete - The inventory is approximately 81-95% complete - The inventory is approximately 96-100% complete	The inventory is approximately 96-100% complete
3.c.	**The IG generally agrees with the Chief Information Officer (CIO) on the number of agency-owned systems. Yes or No.**	Yes

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory	
3.d. **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 or No.**	Yes
3.e. **The agency inventory is maintained and updated at least annually. Yes or No.**	Yes
3..f. **If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.**	

Component/Bureau	System Name	Exhibit 53 Unique Project Identifier (UPI)	Agency or Contractor system?
N/A	N/A	N/A	N/A
Number of known systems missing from inventory:	0		

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. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.

For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.

Response Categories:
 - Rarely- for example, approximately 0-50% of the time
 - Sometimes- for example, approximately 51-70% of the time
 - Frequently- for example, approximately 71-80% of the time
 - Mostly- for example, approximately 81-95% of the time
 - Almost Always- for example, approximately 96-100% of the time

4.a.	The POA&M is an agency-wide process, incorporating all known IT security weaknesses 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.	Almost Always- for example, approximately 96-100% of the time
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	Almost Always- for example, approximately 96-100% of the time
4.c.	Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).	Almost Always- for example, approximately 96-100% of the time
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always- for example, approximately 96-100% of the time
4.e.	IG findings are incorporated into the POA&M process.	Mostly- for example, approximately 81-95% of the time
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Almost Always- for example, approximately 96-100% of the time

	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. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.
	
	For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.
	
	Response Categories:
	  - Rarely- for example, approximately 0-50% of the time
	  - Sometimes- for example, approximately 51-70% of the time
	  - Frequently- for example, approximately 71-80% of the time
	  - Mostly- for example, approximately 81-95% of the time
	  - Almost Always- for example, approximately 96-100% of the time

POA&M process comments:	**Treasury OIG Comment:** Overall, our audit of the non-IRS bureaus of the Treasury displayed a consistent approach to the development, implementation and management of a Treasury-wide POA&M process. The Treasury has developed policy and guidance and implemented a POA&M process that is followed by each Treasury bureau. In addition, the Treasury OCIO has implemented TAF to serve as a Treasury-wide system of record for all FISMA related artifacts, including IT security weaknesses. In instances were detailed IT security weaknesses and corrective actions were not incorporated into TAF, we noted that bureaus maintained system-level POA&Ms to track the status of security weaknesses and related corrective action. **TIGTA Comment:** The IRS has an agency-wide process for managing POA&Ms, which generally includes incorporating findings from our audit reports. However, TIGTA findings reported in 2008 were not included in the IRS POA&M process as they had been in prior years.

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. Provide narrative comments as appropriate.

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, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.

5.a.	**The IG rates the overall quality of the Agency's certification and accreditation process as:** **Response Categories:** - **Excellent** - **Good** - **Satisfactory** - **Poor** - **Failing**		Satisfactory
5.b.	**The IG's quality rating included or considered the following aspects of the C&A process:** (check all that apply)	**Security plan**	X
		System impact level	X
		System test and evaluation	X
		Security control testing	X
		Incident handling	X
		Security awareness training	X
		Configurations/patching	X
		Other:	
C&A process comments:	**Treasury OIG Comment:** The assessment of the quality of the certification and accreditation process involved the inspection of the documentation used to certify and accredit a representative subset of 23 major application, minor application, and general support systems across six (6) of the 12 non-IRS Treasury bureaus. Test work involved an inspection of system security plan, NIST FIPS 199 system impact level documentation, security test and evaluation reports, continuous monitoring documentation, incident handling documentation, security awareness documentation, and configuration management documentation. Test work identified inconsistencies in the processes used to design, implement, and/or test the NIST SP 800-53 minimum security control baseline at three (3) bureaus. Specifically,		

seven (7) of the 23 systems selected across two (2) bureaus in the representative statistical sample of Treasury systems did not have all of the minimum baseline security controls tested and evaluated prior to the decision to issue an authorization operate. In addition, the specific NIST SP 800-53 minimum baseline controls required by NIST FIPS 200 were not documented within the system security plans of these systems. Lastly, one (1) system within our representative subset has yet to have the NIST SP 800-53 minimum security control baseline fully implemented. This system is currently operating with an IATO.

Treasury OIG Comment: In the FY 2007 FISMA reporting period, it was identified that several elements required by NIST SP 800-34 were missing from a CDFI Fund contingency plan. As of the close of the FY 2008 FISMA reporting period, these elements were still missing.

TIGTA Comment: The IRS has made significant progress in its certification and accreditation process. We evaluated the quality of the certification and accreditation process for all 11 of the systems in our sample of 22 that were certified and accredited in 2008. We determined that all 11 systems were properly certified and accredited in accordance with NIST guidelines.

For the remaining systems in our sample, we reviewed the adequacy of annual testing of security controls. The IRS made significant progress this year in this area. An appropriate subset of management, operational, and technical controls was selected, documented, and approved for each of the 11 systems we reviewed. However, the testing of operational and technical controls needs improvement to meet NIST and IRS guidelines. Thirty-seven percent of the operational controls were not adequately tested, and 67 % of the technical controls were not adequately tested.

We also examined Information Technology Contingency Plan testing for all 22 systems in our sample, which has improved in the past year. This year the IRS implemented a revised testing program and improved its testing guidance. Adequate tabletop testing was performed for all systems and functional testing was performed for 10 systems in our sample that required this testing. However, improvements are needed to ensure that functional testing meets Department of the Treasury and IRS guidelines.

Question 6-7: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process		
6	**Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D Question #5 (SAOP reporting template), including adherence to existing policy, guidance, and standards.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Satisfactory
Comments:	**Treasury OIG Comment:** The Senior Agency Official for Privacy (SAOP) and the Treasury Office of Privacy and Treasury Records have issued Treasury Directive (TD) 25-07 *Privacy Impact Assessment (PIA)* on August 6, 2008 and drafted TD P 25-07 *Privacy Impact Assessment Manual.* This directive and related procedures manual are being followed by all bureaus for the performance of a PIA. However, these documents were in draft during the FY 2008 FISMA reporting period. Non-IRS Treasury bureaus have been using the draft directive and related procedures manual to perform PIAs. We noted that all systems within the representative subset of 23 non-IRS Treasury systems had a PIA performed that met the guidance outlined in this draft directive and procedures manual.[15] **TIGTA Comment:** During the past year, the IRS has continued to take steps to better protect the privacy of taxpayers. We determined that a PIA was prepared according to IRS guidelines for each of the 22 systems in our representative sample.	

---

[15] A separate performance audit report on the Treasury's compliance with Section 522, Division H of the Consolidated Appropriations Act, 2005, and the provisions of OMB Memorandum 07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* will be issued.

Question 6-7: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process		
7	**Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Poor
Comments:	**Treasury OIG Comment:** The purpose of OMB Memorandum 07-16 is to instruct agencies to develop breach notification policies based on the guidance contained with the memorandum no later then September 19, 2007. The SAOP and the Treasury Office of Privacy and Treasury Records have developed TD 25-08 *Personally Identifiable Information (PII) Protection, Breach Response, and Notification*. While this TD was still under review by the SAOP at the conclusion of fieldwork, the policies outlined within were being followed by each of the 12 non-IRS bureaus. **TIGTA Comment:** The IRS has also taken steps to implement OMB Memorandum 07-16 requirements for safeguarding against and responding to the breach of PII. The IRS has developed plans to respond to PII breaches and to reduce the use of Social Security Numbers. In 2008, the IRS also conducted a program to refresh employee awareness of existing policies and procedures about encrypting, safeguarding, and protecting sensitive information.	

Question 8: Configuration Management		
8.a.	**Is there an agency-wide security configuration policy? Yes or No.**	Yes
Comments:	**Treasury OIG Comment:** Treasury OCIO TCIO Memorandum 07-01 *Security Configuration and Vulnerability Management Policy,* which became effective on April 1, 2007, requires all Treasury bureaus to develop and/or implement configuration baselines that are compliant with NIST SP 800-70 on all operating systems and platforms. In addition, the Treasury OCIO released TCIO Memorandum 07-04 *Implementation of Common Security Configuration for IT Systems Using Windows XP or Vista* on April 17, 2007, which requires all Bureaus to implement common security configurations for Windows XP and Vista systems (i.e. FDCC) no later then February 1, 2008.	
8.b.	**Approximate the extent to which applicable systems implement common security configurations, including use of common security configurations available from the National Institute of Standards and Technology's website at** http://checklists.nist.gov**.** **Response categories:**	Frequently- for example, approximately 71-80% of the time

	- Rarely- for example, approximately 0-50% of the time
	  - Sometimes- for example, approximately 51-70% of the time
	  - Frequently- for example, approximately 71-80% of the time
	  - Mostly- for example, approximately 81-95% of the time
	  - Almost Always- for example, approximately 96-100% of the time	

8.c.	**Indicate which aspects of Federal Desktop Core Configuration (FDCC) have been implemented as of this report:**	
	c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations. Yes or No.	Yes
	c.2 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 or No.	Yes
	c.3 All Windows XP and VISTA computing systems have implemented the FDCC security settings. Yes or No.	No
Comments:	**Treasury OIG Comment:** Question 8.b – From our representative statistical sample of 23 non-IRS information systems, we determined that one (1) system at each of two (2) bureaus were not using NIST SP 800-70 common security configuration baselines during the FY 2008 FISMA reporting period. As a result, we determined that NIST SP 800-70 common security configurations are applied to 94% of the systems within our representative subset of non-IRS systems. When combined with the total percentage of instances of the Microsoft Windows XP operating systems running the FDCC secure baseline configurations, with	

Question 8: Configuration Management
deviations, the total percentage of implementation of NIST SP 800-70 common security configurations becomes 83%. **Treasury OIG Comment:** Question 8.c.2 – Our response is based on the review of a selection of contracts at BEP, BPD, DO, and FMS. **Treasury OIG Comment:** Question 8.c.3 – As noted in 8.a. above, Treasury required the adoption of FDCC standard configurations. To date, four (4) have not implemented the FDCC secure baseline configuration across all workstations. In total, we determined that non-IRS Treasury is approximately 82% complete in implementing FDCC secure configuration baselines on all instances of the Microsoft Windows XP platform. **TIGTA Comment:** Question 8.b – The IRS provided test results that demonstrated an overall rate of 71% to 80% for implementing security configurations. In general, we agreed with the IRS' compliance assessment, with one exception. The IRS used external scanning software to assess compliance for one of its most heavily used database products instead of using a scanner that can authenticate to the database and assess internal database configurations. **TIGTA Comment:** Question 8.c.3 – The IRS has adopted the FDCC standard configurations in its workstation security policies and compliance assessment tools. It has documented 11 deviations from the FDCC and the business reasons why the settings cannot be implemented, which have been reported along with other noncompliant settings to the Department of the Treasury. The IRS continues to test FDCC standard configurations and therefore has only partially implemented the FDCC. The IRS is currently testing settings to determine whether they can be implemented; it has confirmed compliance with 89 FDCC settings in its test environment. However, the IRS has not yet validated that these settings are implemented on IRS workstations. The IRS compliance assessment tool, recently configured to assess compliance with some FDCC settings, is in the initial stages of assessing IRS workstations.

Question 9: Incident Reporting		
Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.		
9.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	No
9.b.	The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)	No
9.c.	The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.	Yes
Comments:	**Treasury OIG Comment:** The Treasury OCIO Cyber Security program and the TCSIRC have developed policies, guidance, and procedures for reporting computer security incidents internally, as well as for the reporting computer security incidents to the US-CERT and to law enforcement. However, nine (9) out of 38 computer security incidents sampled (or 24%) from the total population of US-CERT Category 1 through Category 4 computer security incidents across the 12 non-IRS bureaus (147) in the FY 2008 FISMA reporting period were incorrectly categorized. In addition, three (3) category 1 computer security incidents out of 38 computer security incidents sampled (or 8%) from the total population of US-CERT Category 1 through Category 4 computer security incidents across the 12 non-IRS bureaus (147) in the FY 2008 FISMA reporting period were not reported based on the timeframes established by the US-CERT and Treasury OCIO policy. **TIGTA Comment for IRS:** IRS reports directly to the TCSIRC, not US-CERT.	

Question 10: Security Awareness Training	

Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities?
 	
Response Categories:
  - Rarely- or approximately 0-50% of employees
  - Sometimes- or approximately 51-70% of employees
  - Frequently- or approximately 71-80% of employees
  - Mostly- or approximately 81-95% of employees
  - Almost Always- or approximately 96-100% of employees
	Almost Always- or approximately 96-100% of employees

Question 11: Collaborative Web Technologies and Peer-to-Peer File Sharing	
Does the agency explain policies regarding the use of collaborative web technologies and peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes or No.	Yes
Question 12: E-Authentication Risk Assessments	
12.a. Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST Special Publication 800-63, "Electronic Authentication Guidelines"? Yes or No.	No
12.b. If the response is "No", then please identify the systems in which the agency has not implemented the e-authentication guidance and indicate if the agency has a planned date of remediation.	While the Treasury OIG answered "Yes" to this question for the representative subset of Treasury systems selected at the non-IRS bureaus, TIGTA reported that for IRS three of the five e-authentication applications were not validated to determine whether the applications operationally achieved the required assurance level. The IRS plans to revise its process for validating e-authentication assurance levels during the FY 2009 FISMA reporting period.

APPENDIX II – APPROACH TO THE SELECTION OF THE SUBSET OF SYSTEMS

KPMG's approach for the selection of a representative subset of Treasury systems was based on applying an attribute random sampling formula per GAO/President's Council on Integrity and Efficiency *Financial Audit Manual* guidance for tests of controls. A standard sample size of 45 items is generally recommended for test of controls based on a 90% confidence level and a 10% precision level or error rate that the results will not be representative of the population. This confidence level is generally appropriate for test of controls because the auditor obtains additional satisfaction regarding controls through other tests such as substantive tests, inquiry, observation, and walkthroughs.[16]

The following table shows the approach taken for sampling 45 Treasury systems that included a breakout between Treasury IRS[17] and non-IRS systems, per OIG scope requirements:

Component	Time period	Low Risk (90% confidence level and 10% precision)
IRS	As of June 10	20
	From June 10 to June 30	2
Non-IRS	As of June 10	21
	From June 10 to June 30	2
Total		**45**

A sample of 41 systems was initially selected using the June 10, 2008 universe and four (4) systems were selected from the June 30, 2008 universe. The allocation of selections in the sample was proportional to the number of systems in the population, therefore, out of the sample of 45, 22 selected were IRS systems and 23 were Non-IRS systems. The first sample of 41 systems included 20 systems of the IRS sub-population and 21 for the Non-IRS population. The final four (4) samples contained two (2) selections for each group.

---

[16] GAO/President's Council on Integrity and Efficiency *Financial Audit Manual*, Section 450 – Sampling Control Tests, July 2001.
[17] Test work performed over Treasury IRS system was performed by TIGTA; not by KPMG.

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
C&A	Certification and Accreditation
CDFI	Community Development Financial Institution
CI/KR	Critical Infrastructure/Key Resources
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CSIRC	Computer Security Incident Response Capability
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
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
IATO	Interim Authority to Operate
IG	Inspector General
IRS	Internal Revenue Service

Acronym	Definition
IT	Information Technology
Mint	United States Mint
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of Currency
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
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
Revision	Rev
SAOP	Senior Agency Official for Privacy
SP	Special Publication
TAF	Trusted Agent FISMA
TCIO	Treasury Chief Information Officer
TCSIRC	Treasury Computer Security Incident Response Capability
TD	Treasury Directive
TD P	Treasury Directive Publication
TIGTA	Treasury Inspector General for Tax Administration
TTB	Alcohol and Tobacco Tax and Trade Bureau
US-CERT	United States Computer Emergency Readiness Team

ATTACHMENT 2

Treasury Inspector General for Tax
Administration–Federal Information Security
Management Act Report for Fiscal Year 2008,
September 10, 2008

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

September 10, 2008

MEMORANDUM FOR DEPUTY 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 2008 (Audit #200820024)

We are pleased to submit the Treasury Inspector General for Tax Administration's Federal Information Security Management Act (FISMA)[1] report for Fiscal Year 2008. The FISMA requires the Office of Inspector General to perform an annual independent evaluation of information security policies, procedures, and practices and compliance with FISMA requirements. As such, this report presents the results of our independent evaluation of the Internal Revenue Service's (IRS) information technology security program.

We based our evaluation on the Office of Management and Budget (OMB) FISMA reporting guidelines for 2008 and the answers to the questionnaire published with the OMB guidelines (see Attachment I). During the 2008 evaluation period,[2] we also conducted nine audits to evaluate the adequacy of information security in the IRS (see Attachment II). We considered the results of those audits when making our assessment. Major contributors to this report are listed in Attachment III.

To complete our review, we evaluated a representative sample of 22 IRS information systems to assess the quality of the certification and accreditation process. For these systems, we also assessed the annual testing of controls for continuous monitoring, testing of Information Technology Contingency Plans, and quality of the Plan of Action and Milestones process. We conducted separate tests to evaluate processes for inventory accuracy, configuration management, incident reporting, awareness training, and information privacy.

Overall, the IRS has made steady progress in complying with FISMA requirements since enactment of the FISMA in 2002, and it continues to place a high priority on efforts to improve

---

[1] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[2] The FISMA evaluation period for the Department of the Treasury is July 1, 2007, through June 30, 2008. Hereafter, all references to 2008 refer to the FISMA evaluation period.

its security program. We observed significant improvements in the areas of security that we had identified as needing improvement in our 2007 FISMA evaluation.[3] In addition, during 2008, the IRS Modernization and Information Technology Services organization Cybersecurity office took steps to achieve efficiencies in the certification and accreditation process. It realigned its general support system structure by functional rather than physical boundaries, which reduced the number of general support systems and improved mapping to applications. It also streamlined the certification and accreditation process for low-impact systems to reduce costs and improve scheduling capabilities. During 2008, the IRS certified and accredited the last of its systems that had not previously been assessed through a National Institute of Standards and Technology (NIST)[4]-compliant certification and accreditation process. The IRS also continued to work closely in seeking guidance and concurrence on FISMA issues with the Treasury Inspector General for Tax Administration and the Department of the Treasury Chief Information Officer to improve compliance with the NIST and FISMA requirements.

Our evaluation of the IRS' 2008 performance against specific OMB security measures and our audit work performed during 2008 show that while the IRS improved its certification and accreditation process, more needs to be done to adequately secure its systems and data. The most significant area of concern is implementation of configuration management standards.

Attachment I provides our responses to the OMB FISMA questions for the Inspector General. We are confident that the IRS systems inventory is substantially complete, the Plan of Action and Milestones process is adequate to ensure the remediation of security weaknesses, and policies and procedures are followed for reporting computer security incidents. Provided in this document are security performance improvements as well as areas that require additional attention.

Certification and Accreditation Process The IRS has made significant progress in its certification and accreditation process. Therefore, this year we evaluate this process as *good*. However, the IRS needs to continue to improve the process to ensure that the level of annual security controls and contingency plan testing is sufficient.

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 certifications and accreditations. In our 2007 FISMA evaluation, we reported that the IRS had implemented a *satisfactory* certification and accreditation process. This year the IRS completed this implementation, and it has now subjected all systems to the process. We evaluated the quality of the certification and accreditation process for all 11 of the systems in our sample of 22 that were certified and accredited in 2008. We determined that all 11 systems were properly certified and accredited in accordance with NIST guidelines.

For the remaining systems in our sample, we reviewed the adequacy of annual testing of security controls for continuous monitoring. The IRS made significant progress this year in this area. An

---

[3] *Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2007* (Reference Number 2007-20-186, dated September 4, 2007).

[4] The NIST, under the Department of Commerce, is responsible for developing standards and guidelines, including minimum requirements for providing adequate information security for all Federal Government agency operations and assets.

appropriate subset of management, operational, and technical controls was selected, documented, and approved for each of the 11 systems we reviewed. However, the testing of operational and technical controls needs improvement and does not meet NIST and IRS guidelines. Overall, 28 percent of the controls were not sufficiently tested for the 11 systems from our sample. Thirty-seven percent of the operational controls were not adequately tested, and 67 percent of the technical controls were not adequately tested. These tests were limited to examining certification and accreditation documentation without securing evidence from the system. As a result, some tests were insufficient to identify controls that might not be operating as intended to protect the systems and data.

We also examined the IRS' testing of Information Technology Contingency Plans, which has improved in the past year. This year, the IRS implemented a revised testing program and improved its testing guidance. Our review of the 22 systems in our sample determined that adequate tabletop[5] testing was performed for all systems. In addition, the IRS performed functional testing for the 10 systems in our sample for which this testing was required. However, improvements are needed to ensure that testing meets Department of the Treasury and IRS guidelines:

- Supporting documentation for 4 of the 10 functional tests did not adequately support testing results for verifying readability of backup tapes retrieved during the tests.

- The IRS has not developed criteria to assess the timeliness of retrieving backup tapes from offsite locations. In addition, the IRS did not compute the time for retrieving backup tapes in any of the 10 functional tests.

- The IRS performed only a limited test of timeliness for offsite retrieval of backup tapes, including those from offsite vendors, during other than normal working hours. The IRS conducted this test for only one system and did not document the results. IRS management informed us that this was a cost-based decision due to the limited funding for these tests.

- Testing plans and results did not include a description of the sampling methodology used for retrieving and validating the readability of backup files. IRS procedures recommend that a sample of files, rather than the entire population, be selected for testing and that the sample be selected at random.

Plan of Action and Milestones Process The IRS has an agency-wide process for managing Plans of Action and Milestones, which generally includes incorporating findings from our audit reports. However, our findings reported in 2008 were not included in the IRS Plan of Action and Milestones process as they had been in prior years. Based on our discussions with IRS management, we determined that responsibilities for this part of the Plan of Action and Milestones process were inadequately transferred between employees.

Privacy Requirements During the past year, the IRS has continued to take steps to better protect the privacy of taxpayers. We determined that a Privacy Impact Assessment[6] was

---

[5] Participants in tabletop exercises walk through the contingency plan procedures to ensure that the documentation reflects the ability to adequately perform the tasks outlined without any recovery operations actually occurring.
[6] This is an analysis of how personal information is collected, stored, shared, and managed in a Federal Government system.

prepared according to IRS guidelines for each of the 22 systems in our representative sample. The IRS has also taken steps to implement OMB requirements for safeguarding against and responding to the breach of personally identifiable information (PII). The IRS has developed plans to respond to PII breaches and to reduce the use of Social Security Numbers. In 2008, the IRS also conducted a program to refresh employee awareness of existing policies and procedures about encrypting, safeguarding, and protecting sensitive information. As a result, we are evaluating the IRS' progress in implementing OMB requirements for safeguarding against and responding to breaches of PII as *good*.

However, we continue to have concerns about the IRS' overall ability to adequately protect PII. In particular, weaknesses in access controls, audit trails, and system configuration settings directly affect the IRS' ability to protect PII. In 2008, our audits continued to identify weaknesses in the IRS' ability to adequately secure its systems and protect PII. Attachment II presents a list of these reports.

Security Configurations The OMB requires agencies to have configuration guides in place to ensure consistent implementation of software across the agency. The IRS has an agency-wide security configuration policy but needs to do more to ensure that information systems apply common security configurations established by the NIST.

The IRS provided test results that demonstrated an overall rate of 71 percent to 80 percent for implementing security configurations. In general, we agreed with the IRS' compliance assessment, with one exception. The IRS used external scanning software to assess compliance for one of its most heavily used database products instead of using a scanner that can authenticate to the database and assess internal database configurations.

During our evaluation, we also identified software used by the IRS for which compliance with NIST or IRS standard configurations was not reported. The software includes firewalls, systems management computers, web servers, handheld device servers, and mainframes. The software should be included in the IRS' 2009 FISMA assessment.

In this year's assessment, the OMB also requires an evaluation of agency progress in implementing the Federal Desktop Core Configuration (FDCC) standard configurations. We are currently conducting an audit in this area and will further evaluate the IRS' progress in implementing these configurations. Our evaluation below is based on the IRS' progress as of June 30, 2008.

The IRS has adopted the FDCC standard configurations in its workstation security policies and compliance assessment tools. It has documented 11 deviations from the FDCC and the business reasons why the settings cannot be implemented, which have been reported along with other noncompliant settings to the Department of the Treasury. The IRS continues to test FDCC standard configurations and therefore has only partially implemented the FDCC. Based on guidance from the OMB that partial implementation is acceptable, and because the IRS followed the Department of the Treasury process for reporting deviations, we determined that the agency has adopted and implemented FDCC standard configurations and has documented deviations. The IRS has also included new Federal Acquisition Regulation[7] language in three contracts that we were able to review and has issued guidance on this requirement.

---

[7] 48 C.F.R. ch. 1 (2006).

However, we were unable to confirm that the IRS has implemented FDCC standard configurations on all Windows workstations. The OMB permits implementation to include those settings for which deviations have been documented. The IRS is currently testing settings to determine whether they can be implemented; it has confirmed compliance with 89 FDCC settings in its test environment. However, the IRS has not yet validated that these settings are implemented on IRS workstations. The IRS compliance assessment tool, recently configured to assess compliance with some FDCC settings, is in the initial stages of assessing IRS workstations. Therefore, we cannot validate that FDCC settings are implemented on all IRS workstations.

<u>Electronic Authentication Risk Assessments</u> Last year, we reported that the IRS completed electronic authentication (e-authentication) risk assessments for its systems. While our review this year continued to find that e-authentication risk assessments are completed, we do not have confidence that applications have operationally achieved the required assurance level in accordance with NIST *Electronic Authentication Guidelines* (Special Publication 800-63).

We agree with the IRS' inventory of e-authentication applications and did not identify any additional applications that should be included. However, the IRS has not consistently validated the operation of e-authentication controls. The OMB requires Federal Government agencies to conduct a final validation confirming that systems achieve the required e-authentication assurance level. This validation should be performed as part of required security procedures, such as certification and accreditation or annual testing. We determined that three of the five e-authentication applications did not include e-authentication validation tests during certification and accreditation. The IRS has acknowledged the need to improve its e-authentication process and plans to revise its process for validating e-authentication assurance levels during the 2009 FISMA reporting period.

Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Details of the Treasury Inspector General for Tax Administration Federal Information Security Management Act Analysis

Section C - Inspector General: Questions 1 and 2												

Agency Name:	**Department of Treasury**							**Submission date:**		**August 28, 2008**		

Question 1: FISMA Systems Inventory												

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing												

2. 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.

		Question 1						Question 2					
		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
Internal Revenue Servi	High	4	0	0	0	4	0	0		0			
	Moderate	184	14	6	1	190	15	15	100%	15	100%	15	100%
	Low	53	7	0	0	53	7	7	100%	7	100%	7	100%
	Not Categorized	0	0	0	0	0	0	0		0			
	Sub-total	241	21	6	1	247	22	22	100%	22	100%	22	100%
Agency Totals	High	4	0	0	0	4	0	0		0		0	
	Moderate	184	14	6	1	190	15	15	100%	15	100%	15	100%
	Low	53	7	0	0	53	7	7	100%	7	100%	7	100%
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Total	241	21	6	1	247	22	22	100%	22	100%	22	100%

= Data Entry Cells
= Editable Calculations (no Data Entry-ONLY edit Formulas when necessary)

Section C - Inspector General: Question 3		
Agency Name:	**Department of Treasury**	
	Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory	
3.a.	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. Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance. Response Categories: - Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	Almost Always (96-100% of the time)
3.b.	The agency has developed a complete inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. Response Categories: - The inventory is approximately 0-50% complete - The inventory is approximately 51-70% complete - The inventory is approximately 71-80% complete - The inventory is approximately 81-95% complete - The inventory is approximately 96-100% complete	Inventory is 96-100% complete
3.c.	The IG generally agrees with the CIO on the number of agency-owned systems. Yes or No.	Yes
3.d.	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 or No.	Yes
3.e.	The agency inventory is maintained and updated at least annually. Yes or No.	Yes
3.f.	If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.	

Component/Bureau	System Name	Exhibit 53 Unique Project Identifier (UPI) {must be 23-digits}	Agency or Contractor system?
Number of known systems missing from inventory:			

= Data Entry Cells

Section C - Inspector General: Questions 4 and 5

Agency Name:	Department of Treasury

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. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.

For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.

Response Categories:
 - Rarely- for example, approximately 0-50% of the time
 - Sometimes- for example, approximately 51-70% of the time
 - Frequently- for example, approximately 71-80% of the time
 - Mostly- for example, approximately 81-95% of the time
 - Almost Always- for example, approximately 96-100% of the time

4.a.	The POA&M is an agency-wide process, incorporating all known IT security weaknesses 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.	Almost Always (96-100% of the time)
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	Almost Always (96-100% of the time)
4.c.	Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).	Almost Always (96-100% of the time)
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always (96-100% of the time)
4.e.	IG findings are incorporated into the POA&M process.	Mostly (81-95% of the time)
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Almost Always (96-100% of the time)
POA&M process comments:		

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. Provide narrative comments as appropriate.

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, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.

5.a.	The IG rates the overall quality of the Agency's certification and accreditation process as: Response Categories: - Excellent - Good - Satisfactory - Poor - Failing		Good
5.b.	The IG's quality rating included or considered the following aspects of the C&A process: (check all that apply)	Security plan	X
		System impact level	X
		System test and evaluation	X
		Security control testing	X
		Incident handling	X
		Security awareness training	X
		Configurations/patching	X
		Other:	
C&A process comments:			

Section C - Inspector General: Questions 6, 7, and 8		
Agency Name:	**Department of Treasury**	
Question 6-7: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process		
6	Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D Question #5 (SAOP reporting template), including adherence to existing policy, guidance, and standards. Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Good
Comments:		
7	Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information. Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Good
Comments:		
Question 8: Configuration Management		
8.a.	Is there an agency-wide security configuration policy? Yes or No.	Yes
Comments:		
8.b.	Approximate the extent to which applicable systems implement common security configurations, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov. **Response categories:**	Frequently (71-80% of the time)
	- Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	
8.c.	Indicate which aspects of Federal Desktop Core Configuration (FDCC) have been implemented as of this report:	
	c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations. Yes or No.	Yes
	c.2 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 or No.	Yes
	c.3 All Windows XP and VISTA computing systems have implemented the FDCC security settings. Yes or No.	No

Section C - Inspector General: Questions 9, 10 and 11		
Agency Name:	**Department of Treasury**	
Question 9: Incident Reporting		
Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.		
9.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
9.b.	The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)	
9.c.	The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.	Yes
Comments:	IRS reports directly to the Treasury Computer Security Incident Response Center, not US-CERT.	
Question 10: Security Awareness Training		
Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities? Response Categories: - Rarely- or approximately 0-50% of employees - Sometimes- or approximately 51-70% of employees - Frequently- or approximately 71-80% of employees - Mostly- or approximately 81-95% of employees - Almost Always- or approximately 96-100% of employees		Almost Always (96-100% of employees)
Question 11: Collaborative Web Technologies and Peer-to-Peer File Sharing		
Does the agency explain policies regarding the use of collaborative web technologies and peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes or No.		Yes
Question 12: E-Authentication Risk Assessments		
12.a. Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST Special Publication 800-63, "Electronic Authentication Guidelines"? Yes or No.		No
12.b. If the response is "No", then please identify the systems in which the agency has not implemented the e-authentication guidance and indicate if the agency has a planned date of remediation.		Three of the five e-authentication applications were not validated to determine whether the applications operationally achieved the required assurance level. The IRS plans to revise its process for validating e-authentication assurance levels during the FISMA 2009 reporting period.

Treasury Inspector General for Tax Administration Information Technology Security Reports Issued During the 2008 Evaluation Period

1. *Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved* (Reference Number 2007-20-161, dated September 19, 2007).

2. *Lack of Proper IRS Oversight of the Department of the Treasury HSPD-12 Initiative Resulted in Misuse of Federal Government Resources* (Reference Number 2008-20-030, dated December 14, 2007).

3. *Internal Revenue Service Databases Continue to Be Susceptible to Penetration Attacks* (Reference Number 2008-20-029, dated December 14, 2007).

4. *Improvements Are Needed to the Information Security Program Governance Process* (Reference Number 2008-20-076, dated March 11, 2008).

5. *Actions Are Needed to Improve the Effectiveness of the Physical Security Program* (Reference Number 2008-20-077, dated March 13, 2008).

6. *Inadequate Security Controls Over Routers and Switches Jeopardize Sensitive Taxpayer Information* (Reference Number 2008-20-071, dated March 26, 2008).

7. *Private Collection Agencies Adequately Protected Taxpayer Data* (Reference Number 2008-20-078, dated March 26, 2008).

8. *Control Weaknesses at Internal Revenue Service Internet Connections Increase Security Risks* (Reference Number 2008-20-143, dated July 17, 2008).

9. *Unauthorized and Insecure Internal Web Servers Are Connected to the Internal Revenue Service Network* (Reference Number 2008-20-159, dated August 26, 2008).

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Michael Howard, Audit Manager
Alan Beber, Senior Auditor
Richard Borst, Senior Auditor
Charles Ekunwe, Senior Auditor
Myron Gulley, Senior Auditor
Jody Kitazono, Senior Auditor
Thomas Nacinovich, Senior Auditor
Midori Ohno, Senior Auditor
Joan Raniolo, Senior Auditor
Jefferson Lee, Program Analyst