Evaluation Report

OIG-CA-06-001

INFORMATION TECHNOLOGY: Evaluation of Treasury's FISMA Implementation For Fiscal Year 2005

October 7, 2005

Office of Inspector General

DEPARTMENT OF THE TREASURY

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

October 7, 2005

MEMORANDUM FOR IRA L. HOBBS
CHIEF INFORMATION OFFICER

FROM: Louis C. King
Director, Information Technology Audits

SUBJECT: Evaluation of Treasury's Federal Information Security Management Act Implementation for Fiscal Year 2005

I am pleased to transmit the attached Fiscal Year (FY) 2005 evaluation of the Department of the Treasury's (Treasury) information security program and practices, as required by the Federal Information Security Management Act (FISMA). We contracted with KPMG LLP, an independent certified public accounting firm, to perform the FISMA evaluation of Treasury's unclassified systems[1], except for those of the Internal Revenue Service (IRS). The Treasury Inspector General for Tax Administration (TIGTA) performed the FISMA evaluation for the IRS systems (see attached).

We considered the results of the evaluation performed by KPMG LLP, as well as the results of the evaluation performed by TIGTA, in assessing Treasury's overall compliance with FISMA. Based on the results of these evaluations, we believe that despite some progress, Treasury has significant deficiencies that constitute substantial noncompliance with FISMA. The most important of these deficiencies follow:

- In 2004, the Treasury Chief Information Officer's (CIO) system inventory was found to be inaccurate and incomplete. In addition, we found the CIO's office had not assessed the consistency of the methodologies used by certain bureaus to re-categorize their inventories, nor had it assessed the impact of the inventory changes on the remainder of Treasury. On

[1] We performed the FISMA evaluation for Treasury's national security systems. The results of this evaluation are contained in Report No. OIG-CA-05-003. This report is classified.

September 12, 2005, the Treasury CIO issued a memo to bureau CIOs containing guidance on developing a FISMA inventory and a data call for an updated system inventory, including national security systems. The memo required the bureaus to update their inventories by October 10, 2005. Because the results of this effort were not available as of the issuance of our report, we were unable to assess the accuracy, completeness and consistency of the Treasury system inventory.

- Treasury was not fully in compliance with OMB's current requirement to include all systems in the FISMA report and to categorize these systems by FIPS 199 impact levels. In particular, we noted that the bureaus had inconsistent treatments for non-major applications. In many cases, non-major applications were not reported, or reported as part of a general support system or a major application.
- IRS continues to have significant deficiencies in its information security program and practices. In its FY 2005 FISMA Evaluation for IRS, TIGTA reported concerns in the following areas: system inventory categorization, certification and accreditation, continuous monitoring of systems, tracking corrective actions, training employees with key security responsibilities, contractor oversight, and security configuration policies.
- Other bureaus within Treasury also have significant deficiencies in their information security program and practices. KPMG reported concerns in the following areas at various bureaus: certification and accreditation, training, plans of actions and milestones, security self-assessments, and system inventory categorization.

If you have any questions or require further information, please contact me at (202) 927-5774, or a member of your staff may contact Leslye Burgess, Audit Manager, Information Technology Audits, at (202) 927-5364.

Attachments

Evaluation Report

For the

Department of the Treasury

Information Technology: Evaluation of Federal Information Security Management Act Implementation for Fiscal Year 2005

October 7, 2005

Prepared by:
KPMG LLP
2001 M Street, N.W.
Washington, D.C. 20036

UNITED STATES DEPARTMENT OF THE TREASURY
Fiscal Year 2005 FISMA EVALUATION

Evaluation Report

Table of Contents

October 7, 2005

Louis C. King
Director, Information Technology Audits
Department of the Treasury, Office of Inspector General

To assist Federal agencies in meeting their responsibilities, the President signed into law on December 17, 2002, the Electronic Government Act. Title III of this Act, the Federal Information Security Management Act (FISMA), along with Office of Management & Budget's (OMB) policy, lays out a framework for annual Information Technology (IT) security reviews, reporting, and remediation planning. As required by FISMA, an annual independent evaluation was performed for the Department of the Treasury's (Treasury) information security program and practices to determine the effectiveness of such program and practices for Fiscal Year (FY) 2005 as they relate to the 13 bureaus and Offices listed in Appendix A. FISMA requires the Inspector General or an independent external auditor, as determined by the Inspector General, to perform this evaluation. Treasury has two Inspectors General: The Treasury Inspector General for Tax Administration (TIGTA) (which covers the Internal Revenue Service (IRS)) and the Treasury Office of Inspector General (OIG) (which covers the remainder of Treasury).

For FY 2005, the OIG awarded a contract to KPMG LLP to perform the FISMA evaluation for Treasury's unclassified systems. The Treasury OIG performed the evaluation of national security systems, and the TIGTA performed the FISMA evaluation for the IRS.

Our objective, scope, and methodology are described in Appendix C. This report contains the results in brief, background, and responses to OMB questions, which contain the detailed results of our evaluation.

Results in Brief

Treasury's information security program and practices, as they relate to non-national security systems[1], requires additional improvements to adequately protect the information and systems that support Treasury operations.

Provided below are specific areas where needed improvements were identified during the evaluation:

- Treasury's security certification and accreditation (C&A) process needs enhancement. The Department has not consistently developed C&A packages in accordance with guidance prescribed by the National Institute of Standards and Technology (NIST) Special Publications (SP) series as noted in the following examples:

[1] The evaluation of Treasury's information security program and practices for its national security systems is reported separately.

- Required components of the C&A packages have not been documented.
- C&A memos have not been authorized.

We noted the above issues at the following Treasury bureaus[2]:

- U.S. Mint (Mint)
- Financial Management Service (FMS)
- Bureau of Engraving and Printing (BEP)
- Community Development Financial Institution (CDFI) Fund
- Office of Thrift Supervision (OTS)
- Office of the Comptroller of the Currency (OCC)
- Bureau of Public Debt (BPD)
- Treasury Inspector General for Tax Administration (TIGTA)
- Departmental Offices (DO)
- Financial Crimes Enforcement Network (FinCEN)

- Treasury should continue to enforce annual security awareness efforts, specialized security training, and peer-to-peer security training requirements to ensure that all employees, contractors and personnel with significant security responsibilities receive sufficient training. Training improvements are needed for the following bureaus:

  - CDFI
  - DO
  - FinCEN
  - Mint
  - OTS
  - OCC
  - TIGTA

- Treasury should continue to track IT security weaknesses in the plan of action and milestones (POA&M) documents submitted to OMB. Additional improvements with the POA&M process are needed to consistently identify weaknesses from Treasury and OIG reports in the POA&Ms. Additionally, Treasury should ensure that weaknesses identified in the POA&Ms are prioritized to allow appropriate delegation of resources as required by FISMA. Enhancements are needed in the POA&M process at the following bureaus:

  - Alcohol and Tobacco Tax and Trade Bureau (TTB)
  - BEP
  - BPD
  - CDFI
  - DO
  - FinCEN
  - FMS

[2] Not all issues were noted at each bureau.

- OCC
- OTS
- Mint
- TIGTA

- Improvements are needed to ensure that the OCC is adequately identifying system interfaces and documenting supporting connection agreements.

- Treasury should continue to perform security self assessments in accordance with NIST SP 800-26 and 800-53. However, specific improvements are needed as several bureaus did not complete security self assessments during FY 2005. Additionally, several bureaus did not sufficiently address all of the critical elements prescribed by NIST. Improvements are needed at the following bureaus to enhance the security self assessment process:

  - BEP
  - OTS
  - TIGTA

- The OIG has not been consistently included in the development and verification of the Department's systems inventory. Without consistent participation by the OIG in the development and verification of Treasury's system inventory efforts, there is an increased risk that Treasury may not have a clear understanding of all Department systems.

- In 2004, we noted that improvements were needed in the responsibility designations of the Chief Information Officer (CIO) and his reporting structure within Treasury. At that time, there was a draft Treasury Order that placed the CIO in direct reporting line to the Deputy Secretary. We further noted that this draft order was open to interpretation as to what real authority the CIO had within the Department. Since then, Treasury has rescinded this draft Order. On September 21, 2005, Treasury reaffirmed a previous order and placed the CIO under the Assistant Secretary for Management and Chief Financial Officer (ASM/CFO). While the reporting structure of the CIO has been resolved, it still remains open to interpretation as to what real authority the CIO has within the Department. Without a clear and defined role, there is an increased risk that the Treasury CIO may not be able to effectively manage Treasury's IT security program.

- Improvements are needed to enhance Treasury's methodologies for categorizing systems in accordance with FIPS 199. Specifically, the FIPS 199 categorizations for OCC and OTS did not correspond to the confidentiality, integrity, and availability ratings documented in their system security plans.

- In 2004, the Treasury CIO system inventory was found to be inaccurate and incomplete. In addition, we found the CIO's office had not assessed the consistency of the methodologies used by three bureaus to re-categorize their inventories, nor had it assessed the impact of the inventory changes on the remainder of Treasury. On September 12, 2005, the Treasury CIO issued a memo to bureau CIOs containing

rudimentary guidance on developing a FISMA inventory and a data call for an updated system inventory, including national security systems. The memo required the bureaus to update their inventories by October 10, 2005. Because the results of this effort were not available as of the issuance of our report, we were unable to assess the accuracy, completeness and consistency of the Treasury system inventory.

In addition, we found that Treasury was not fully in compliance with OMB's current requirement to include all systems in the FISMA report and to categorize these systems by FIPS 199 impact risk impact levels. In particular, we noted that the bureaus had inconsistent treatments for minor applications. In many cases, minor applications were not reported, or reported as part of a general support system or a major application.

- Improvements are needed to enhance the configuration management process. Specifically, BEP has not developed configuration guides for each operating system used by the agency.

Despite these above identified needs for improvement, our FISMA evaluation also showed that Treasury made improvements with its information security program during FY 2005. The following summarizes these improvements:

- The Franchise Subnet and Franchise DMZ contingency plan, formerly known as the Administrative Resource Center (ARC), Bureau of the Public Debt, and the TOP contingency plan have been revised to address all requirements prescribed by NIST SP 800-34.

- TTB revised their Memorandum of Understanding (MOU) with the bureau of Alcohol, Tobacco, Firearms & Explosives (ATFE) to include the purpose and authority, background and scope, interagency communications, support agreements, party responsibilities, funding, contract claims, dispute resolution, information sharing, extension/modification/termination, and designated approving authority signature pages. The purpose of the MOU is to ensure that adequate levels of IT support for both TTB and ATFE are maintained at the current levels of service and continue to support the requirements of applicable laws/regulations.

- FMS improved its documentation for connections that exist between FMS and external agencies.

Conclusion

Based on the results of our testing, we believe non-IRS Treasury, despite improvements, remains in substantial non-compliance with FISMA. The detailed results for the IRS are contained in the TIGTA's FISMA report.

Overview of TIGTA Evaluation

The TIGTA report provides an independent evaluation of the status of IT security at IRS. The report notes that FY 2005 FISMA results and the results of audits indicate that additional improvements are needed for the IRS to adequately protect the information and systems that support its operations.

The TIGTA noted that during FY 2005 IRS made strides towards improving security; for example:

- IRS developed a corporate approach to FISMA;
- A cross-organizational FISMA working group was created;
- The FISMA working group developed a Concept of Operations, established security roles and identified budget and resource requirements;
- A Security Program Management Office was established within each business unit ;
- IRS business owners were involved in the annual self-assessments of applications; and
- IRS developed new POA&Ms.

Seven areas of concern were highlighted:

- Systems inventory

The IRS has a total of 280 systems in its inventory which the TIGTA believes should have been reported in its FY 2005 FISMA submission. However, the IRS reported 82 general support systems and major applications, which the TIGTA believes is contrary to OMB guidance. The IRS considers the remaining 198 systems to be non-major systems. The IRS assigned all of its non-major applications to a general support system with the assumption that the general support systems provide the majority of the security controls for the non-major applications.

- Certification and accreditation

The IRS reported as having the majority of its systems certified and accredited. However, this may not be the case due to the assignment of non-major applications to general support systems for C&A purposes.

- Continuous monitoring

Self-assessments conducted by the IRS using NIST SP 800-26 did not include adequate testing of application controls.

- Tracking corrective actions

The POA&Ms were not completed by the IRS until early September 2005; therefore, the TIGTA did not have an opportunity to evaluate the IRS' prioritization of weaknesses.

- Training employees with key security responsibilities

The TIGTA was unable to verify that persons with significant security responsibilities completed specialized training because the IRS still has no tracking system in place to identify persons with significant security responsibilities and the specialized training completed. The IRS advised that it plans to implement a tracking system in FY 2006.

- Contractor oversight

Controls over contractor access to IRS networks and data were inadequate. Additionally, the TIGTA noted that the IRS does not require State agencies to conduct self-assessments of its systems using NIST Special Publication 800-26 and does not require them to monitor and track corrective actions using POA&Ms.

- Security configuration policies

Detailed security testing results were not provided for the TIGTA's review for any systems. Therefore, the TIGTA could not evaluate the extent of implementation of the security configuration policies.

Background

Title III of the E-Government Act of 2002, enacted on December 17, 2002, is referred to as FISMA. FISMA permanently reauthorized the framework set forth in GISRA, including the annual Treasury security review and independent evaluations. In addition, FISMA included new provisions to further strengthen the security of the Federal government's information and information systems. We performed our FY 2005 evaluation pursuant to FISMA.

To assist agencies in implementing the requirements of FISMA, OMB issued Memorandum M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated June 13, 2005. OMB M-05-15 replaced OMB M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, dated August 23, 2004. FISMA, along with supporting OMB guidance, lays out a framework for annual IT security reviews, reporting, and remediation planning.

Responses to OMB Questions

OMB's FISMA reporting guidance includes a number of questions, and has been organized as follows:

- Question 1 – Self-Assessment of Agency Systems
- Question 2 – Compliance with C&A Requirements
- Question 3 – System Inventory and Oversight of Contractor Systems
- Question 4 – OIG Assessment of the POA&M Process
- Question 5 – OIG Assessment of the C&A Process
- Question 6 – Configuration Management

- Question 7 – Incident Detection and Handling Procedures
- Question 8 – Security Training and Awareness
- Question 9 – Peer-to-Peer File Sharing

The responses to OMB's questions are contained in the attached tables.

If you have any questions regarding the report, please call Tony Hubbard at (202) 533-4324.

Very truly yours,

KPMG LLP

Attachment

Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Department of the Treasury:

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

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.

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						Question 2					
		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
BPD	High	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Moderate	14	1	0	0	14	1	1	100%	1	100%	1	100%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**14**	**1**	**0**	**0**	**14**	**1**	**1**	**100%**	**1**	**100%**	**1**	**100%**
BEP	High	5	0	0	0	5	0	0	0%	0	0%	0	0%
	Moderate	2	1	1	0	3	1	1	100%	1	100%	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	**7**	**1**	**1**	**0**	**8**	**1**	**1**	**100%**	**1**	**100%**	**0**	**0%**
CDFI	High	1	1	1	0	2	1	1	100%	1	100%	1	100%
	Moderate	0	0	0	0	0	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**	**1**	**1**	**0**	**2**	**1**	**1**	**100%**	**1**	**100%**	**1**	**100%**

		Question 1						Question 2					
		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	**FIPS 199 Risk Impact Level**	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
DO[3]	High	19	1	1	0	20	1	0[4]	0%	1	100%	0	0%
	Moderate	5	0	0	0	5	0	0	0%	0	0%	0	0%
	Low	2	0	0	0	2	0	0	0%	0	0%	0	0%
	Not Categorized	1	0	0	0	1	0	0	0%	0	0%	0	0%
	Sub-total	**27**	**1**	**1**	**0**	**28**	**1**	**0**	**0%**	**1**	**100%**	**0**	**0%**
FINCEN	High	3	1	1	0	4	1	1	100%	1	100%	0	0%
	Moderate	0	0	0	0	0	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	**3**	**1**	**1**	**0**	**4**	**1**	**1**	**100%**	**1**	**100%**	**0**	**0%**
FMS[5]	High	7	0	2	0	9	0	0	0%	0	0%	0	0%
	Moderate	32	0	0	0	32	0	0	0%	0	0%	0	0%
	Low	9	1	1	0	10	1	1	100%	1	100%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**48**	**1**	**3**	**0**	**51**	**1**	**1**	**100%**	**1**	**100%**	**0**	**0%**

[3] Additional data was received from this bureau after the final submission deadline. This information has not been verified and was not included in the report.
[4] Bureau's certification and accreditation package was deemed failing.
[5] Additional data was received from this bureau after the final submission deadline. This information has not been verified and was not included in the report.

		Question 1						Question 2					
		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
IRS[6]	High	**2**	**2**	**0**	**0**	**2**	**2**	**2**	**100%**	**0**	**0%**	**2**	**100%**
	Moderate	**79**	**15**	**8**	**3**	**87**	**18**	**13**	**72.2%**	**9**	**50%**	**3**	**16.7%**
	Low	**1**	**0**	**3**	**0**	**4**	**0**	**0**	**0%**	**0**	**0%**	**0**	**0%**
	Not Categorized			**1[7]**	**0**	**1[8]**							
	Sub-total[9]	**82**	**17**	**12**	**3**	**94**	**20**	**15**	**75%**	**9**	**45%**	**5**	**25%**
MINT[10]	High	0	1	0	0	0	1	1	100%	1	100%	0	0%
	Moderate	13	0	0	0	13	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	**13**	**1**	**0**	**0**	**13**	**1**	**1**	**100%**	**1**	**100%**	**0**	**0%**

[6] Numbers from the TIGTA's evaluation report are reflected here.
[7] Remaining columns on this row were left blank on TIGTA's submission.
[8] The total of one not categorized system differs from the total reported by TIGTA. In its report, TIGTA did not report a total of one not categorized system; however, one not categorized contractor system was reported. To better conform to OMB's guidance, we are adding the one not categorized system to the total number of not categorized systems for the IRS.
[9] The total of 94 IRS systems reported differs from the total of 82 reported by TIGTA. In its report, TIGTA reported 82 agency systems and 12 contractor systems; however, TIGTA could not determine what part, if any, of the 12 contractor systems were already counted as agency systems by the IRS. Consequently, TIGTA reported a total of 82 systems. To better conform to OMB's guidance (which includes this template), we are adding the 12 contractor systems to the 82 agency systems and reflecting a total of 94.
[10] Additional data was received from this bureau after the final submission deadline. This information has not been verified and was not included in the report.

		Question 1						Question 2					
		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
OCC	High	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Moderate	10	0	0	0	10	0	0	0%	0	0%	0	0%
	Low	1	1	0	0	1	1	0[11]	0%	1	100%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
Sub-total		**11**	**1**	**0**	**0**	**11**	**1**	**0**	**0%**	**1**	**100%**	**0**	**0%**

[11] Bureau's certification and accreditation package was deemed failing.

		Question 1						Question 2					
		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
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[12]	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	4	1	0	0	4	1	1	100%	0	0%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**19**	**1**	**0**	**0**	**19**	**1**	**1**	**100%**	**0**	**0%**	**0**	**0%**
TIGTA[13]	High	3	1	0	0	3	1	1	100%	1	100%	0	0%
	Moderate	0	0	0	0	0	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	**3**	**1**	**0**	**0**	**3**	**1**	**1**	**100%**	**1**	**100%**	**0**	**0%**

[12] Additional data was received from this bureau after the final submission deadline. This information has not been verified and was not included in the report.
[13] Additional data was received from this bureau after the final submission deadline. This information has not been verified and was not included in the report.

		Question 1						Question 2					
		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	**FIPS 199 Risk Impact Level**	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
TTB[14]	High	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Moderate	3	1	0	0	3	1	1	100%	1	100%	1	100%
	Low	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Not Categorized	0	0	0	0	0	0	0	0%	0	0%	0	0%
	Sub-total	**3**	**1**	**0**	**0**	**3**	**1**	**1**	**100%**	**1**	**100%**	**1**	**100%**
Agency Totals	**High**	**40**	**7**	**5**	**0**	**45**	**7**	**6**	**85.7%**	**5**	**71.4%**	**3**	**42.9%**
	Moderate	**174**	**18**	**9**	**3**	**183**	**21**	**16**	**76.2%**	**12**	**57.1%**	**5**	**23.8%**
	Low	**17**	**3**	**4**	**0**	**21**	**3**	**2**	**66.7%**	**2**	**66.7%**	**0**	**0%**
	Not Categorized	**1**	**0**	**1**	**0**	**2**	**0**	**0**	**0%**	**0**	**0%**	**0**	**0%**
	Total	**232**	**28**	**19**	**3**	**251**	**31**	**24**	**77.4%**	**19**	**61.3%**	**8**	**25.8%**

[14] Additional data was received from this bureau after the final submission deadline. This information has not been verified and was not included in the report.

Question 3		
In the format below, evaluate the agency's oversight of contractor systems, and 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. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. 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	- Mostly, for example, approximately 81-95% of the time
3.b.	The agency has developed an 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: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 81-95% complete

Question 3		
In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.		
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **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
3.e.	The agency inventory is maintained and updated at least annually.	Yes
3.f.	The agency has completed system e-authentication risk assessments.	Yes

Question 4		
Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below. For items 4a.-4.f, the response categories are as follows: - 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.	- Rarely, for example, approximately 0-50% 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, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Almost Always, for example, approximately 96-100% of the time
4.d.	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

Question 4		
Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below. For items 4a.-4.f, the response categories are as follows: - 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.e.	OIG findings are incorporated into the POA&M process.	- Sometimes, for example, approximately 51-70% 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	- Rarely, for example, approximately 0-50% of the time
Comments: Question 1.a - The IRS has a total of 281 systems, 199 of which are non-major applications. IRS is reporting only its 82 major systems, which we believe is contrary to OMB guidance which requires that all systems be reported. To be consistent with other Treasury bureaus, we are including 82 in our template. However, we selected our representative subset of systems from the population of 281 systems. Questions 1.b & 1.c - IRS has 12 contractor support functions that require oversight. We have reported this in Question 1.b; however, since these are not systems, they are not reflected in the total in Question 1.c. Question 2.a - The IRS reported that it has certified and accredited 90% of its major systems. However, only 35 percent of its 281 systems have been certified and accredited. Question 2.b - Self-Assessment performance levels for Major Applications are often based on the performance level for the associated GSS rather than on application specific controls. Question 3.a - We reviewed 3 of IRS' 12 contractor systems and found IRS' reviews to be generally adequate. We conducted separate reviews this year of IRS's monitoring of contractor access to networks and data and whether State agencies adequately protect federal tax data. These reviews showed the need for significantly increased oversight by the IRS of contractors and State agencies. Question 3.c - As stated in the comments for Question 1.a, we disagree that IRS should report only its major systems in its FISMA report. Question 3.d. We believe OMB guidance requires IRS to include State agencies that receive Federal Tax Information as contractors.[15]		

[15] This comment was documented in the TIGTA report.

Question 5	
OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May, 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans .	
Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Satisfactory
Comments:[16]	

[16] Please see TIGTA report for comments.

Section B: Inspector General. Question 6, 7, 8, and 9. Department of the Treasury:				
Question 6				
6.a.	Is there an agency wide security configuration policy? Yes or No.			Yes
	Comments:			
6.b.	Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.			
Product		**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**

Section B: Inspector General. Question 6, 7, 8, and 9. Department of the Treasury:			
Question 6			
Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional[17]	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Windows NT[18]	Yes	Yes	- **Frequently, or on approximately 71-80% of the systems running this software**

[17] Additional data was received regarding this product after the final submission deadline. This information has not been verified and was not included in the report.
[18] Additional data was received regarding this product after the final submission deadline. This information has not been verified and was not included in the report.

Section B: Inspector General. Question 6, 7, 8, and 9. Department of the Treasury:			
Question 6			
Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows 2000 Professional[19]	Yes	Yes	- **Mostly, or on approximately 81-95% of the systems running this software**
Windows 2000 Server	Yes	Yes	- Frequently, or on approximately 71-80% of the systems running this software
Windows 2003 Server[20]	Yes	Yes	- **Sometimes, or on approximately 51-70% of the systems running this software**

[19] Additional data was received regarding this product after the final submission deadline. This information has not been verified and was not included in the report.

[20] Additional data was received regarding this product after the final submission deadline. This information has not been verified and was not included in the report.

Section B: Inspector General. Question 6, 7, 8, and 9. Department of the Treasury:			
Question 6			
Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Solaris[21]	Yes	Yes	**- Frequently, or on approximately 71-80% of the systems running this software**
HP-UX[22]	Yes	Yes	**- Frequently, or on approximately 71-80% of the systems running this software**

[21] Additional data was received regarding this product after the final submission deadline. This information has not been verified and was not included in the report.

[22] Additional data was received regarding this product after the final submission deadline. This information has not been verified and was not included in the report.

Section B: Inspector General. Question 6, 7, 8, and 9. Department of the Treasury:			
Question 6			
Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Linux[23]	Yes	Yes	**- Frequently, or on approximately 71-80% of the systems running this software**
Cisco Router IOS	Yes	Yes	**- Frequently, or on approximately 71-80% of the systems running this software**
Oracle[24]	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software

[23] Additional data was received regarding this product after the final submission deadline. This information has not been verified and was not included in the report.

[24] Additional data was received regarding this product after the final submission deadline. This information has not been verified and was not included in the report.

Section B: Inspector General. Question 6, 7, 8, and 9. Department of the Treasury:			
Question 6			
Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Other. Specify: z/OS, DB2, MSSQL, and IMS,	Yes	Yes	- See Comment
Other. Specify: PeopleSoft and Weblogic	Yes	Yes	- See Comment
Other. Specify: AIX	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Other. Specify: Open VMS and Microsoft SQL Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Server Other. Specify: DB2 Enterprise Server and Microsoft SQL	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software

Section B: Inspector General. Question 6, 7, 8, and 9. Department of the Treasury:			
Question 6			
Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Other. Specify: Microsoft SQL Server	Yes	Yes	- See Comment
Other. Specify: IBM eServer Z OS	Yes	Yes	- See Comment
Other. Specify: Sybase	Yes	Yes	- See Comment
Comments: Bureau did not provide the percentage of implementation for the product.[25]			

[25] Please see TIGTA report for comments.

Section B: Inspector General. Question 6, 7, 8, and 9. Department of the Treasury: Question 7		
Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.		
7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes
Comments:		

Section B: Inspector General. Question 6, 7, 8, and 9. Department of the Treasury:		
Question 8		
8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Sometimes, or approximately 51-70% of employees have sufficient training
Comments:[26]		

[26] Please see TIGTA report for comments.

Section B: Inspector General. Question 6, 7, 8, and 9. Department of the Treasury: Question 9		
9	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	Yes

Appendix A Treasury Bureaus

Treasury is comprised of the following 13 bureaus and offices for FISMA reporting purposes:

- Alcohol and Tobacco Tax and Trade Bureau (TTB);
- Bureau of Engraving and Printing (BEP);
- Bureau of Public Debt (BPD);
- Community Development Financial Institutions Fund (CDFI);
- Departmental Offices (DO);
- Financial Crimes Enforcement Network (FinCEN);
- Financial Management Service (FMS);
- Internal Revenue Service[27] (IRS);
- Office of the Comptroller of the Currency (OCC);
- Office of Inspector General (OIG);
- Office of Thrift Supervision (OTS);
- United States Mint (Mint); and,
- Treasury Inspector General for Tax Administration (TIGTA).

[27] The IRS FISMA evaluation is performed by TIGTA.

Appendix B Abbreviations

ARC	Administrative Resource Center
ATFE	Alcohol, Tobacco, Firearms & Explosives
BCP	Business Continuity Plan
BEP	Bureau of Engraving and Printing
BPD	Bureau of Public Debt
C&A	Certification & Accreditation
CDFI	Community Development Financial Institutions Fund
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COOP	Continuity of Operations Plan
COTR	Contracting Officer Technical Representative
CSIRC	Computer Security Incident Response Center
DO	Departmental Organization
DRP	Disaster Recovery Plan
FCAS	Foreign Currency Accounting System – *FMS System*
FinCEN	Federal Crimes Enforcement Network
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FMS	Financial Management Service
FY	Fiscal Year
GISRA	Government Information Security Reform Act
GSS	General Support System
IRS	Internal Revenue Service
ISA	Interconnection Security Agreements
IT	Information Technology
LAN	Local Area Network
Mint	United States Mint
MOU	Memorandum of Understanding
MWI	Microsoft Window's Infrastructure – *TIGTA System*
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General
OMB	Office of Management and Budget
OTS	Office of Thrift Supervision
POA&M	Plan of Action & Milestones
ST&E	Security Test & Evaluation
TACT	Treasury Assignment and Correspondence Tracking - *DO System*
TCS	Treasury Communications System
TCSIRC	Treasury Computer Security Incident Response Center
TIGTA	Treasury Inspector General for Tax Administration
Treasury	Department of the Treasury
TSDS	Technical Security Division Systems – *BEP System*
TOP	Treasury Offset Program – *FMS System*
TTB	Alcohol and Tobacco Tax and Trade Bureau
US-CERT	United States Computer Emergency Readiness Team

Appendix C Objective, Scope, and Methodology

The objective of our evaluation was to determine the effectiveness of Treasury's information security program and practices, as it relates to non-national security systems for the following 12 bureaus and offices: BEP, BPD, CDFI, DO, FinCEN, FMS, OCC, OIG, OTS, Mint, TIGTA, and TTB. Note that TIGTA conducts a separate FISMA evaluation for the IRS, as FISMA mandates an evaluation by both the Treasury OIG and TIGTA.

On June 13, 2005, OMB issued Memorandum M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act*. Section A of M-05-15, *Instructions for Completing the Annual FISMA Report and Privacy Management Report*, contains instructions and frequently asked questions to aid Federal CIOs, OIGs, and Senior Agency Officials for Privacy, in preparing and submitting the FY 2005 FISMA Report and the Privacy Management Report. Section C of M-05-15, *Reporting Template for Agency IGs*, contains specific instructions for IGs to complete the FY 2005 FISMA template.

In addition, OMB's FISMA guidance states that "IGs or their designee, perform an annual independent evaluation of the information security program and practices of the agency to determine the effectiveness of such program and practices." Further, it states "the evaluation shall include testing of the effectiveness of information security policies, procedures and practices, to make an assessment of the compliance with information technology security policies, procedures, standards and guidelines. The testing should include an appropriate subset of agency systems. In this regard, FISMA does not limit the subset to financial systems."

To meet the requirements of FISMA, and to conform with OMB's guidance, we performed the following evaluation procedures:

- Followed up on issues identified during the FY 2004 FISMA evaluation.
- Submitted information requests to the CIO and/or Treasury components.
- Reviewed Treasury's FY 2005 FISMA submission.
- Reviewed data and documentation provided to us by Treasury, including documentation for the following subset of systems.
  - BEP TSDS
  - BPD Oracle Federal Financial System
  - CDFI Fund LAN
  - DO TACT
  - FinCEN Server Database
  - FMS FCAS
  - Mint Documentum
  - OCC Risk Analysis
  - OTS ADM200 Payroll/Personnel
  - TIGTA MWI
  - TTB GSS
- Incorporated the IRS FISMA evaluation information provided by TIGTA.
- Reviewed other relevant material (e.g. NIST guidance and Treasury OIG reports).

- Interviewed key Treasury officials.

The evaluation was conducted in accordance with the President's Council on Integrity and Efficiency's *Quality Standards for Inspections*, issued January 2005, and subsequent revisions.

Appendix D Comments on Questionnaire Numbers

Question 1 – Self-Assessment of Agency Systems

- CIO: The CIO's office maintains an inventory of each bureau's major applications and general support systems that have obtained C&As. No exception noted.

- OIG: The OIG has not been consistently included in the development and verification of the Department's inventory. The FY 2005 Treasury OIG FISMA evaluation team (evaluation team) noted that the OIG was included in the development and verification of TTB's inventory, but only after TTB's request. Exception noted.

- The evaluation team performed a comparison of the bureau system inventories to the CIO system inventory, and found that the listing was accurate. However, the evaluation team compared the current bureau FY system inventories to the prior bureau FY inventories and noted discrepancies. Upon identification of a discrepancy, the evaluation team followed up with the appropriate bureau. Additionally, when a new system was added, the evaluation team was provided with the certification and accreditation (C&A) memos for the new systems. However, DO was unable to provide signed C&A memos for two systems added during FY 2005. The evaluation team inspected self assessments and methodologies used to conduct self assessments. The evaluation team also inspected methodologies used by BEP, FMS and DO to create their system inventories. Lastly, the evaluation team verified the bureaus' FIPS 199 systems categorization efforts. A portion of the results have been included below:

  - BEP –The evaluation team determined that a self assessment was not performed on the Technical Security Division Systems during FY 2005. Exception noted.

  - OCC – The evaluation team noted that the Risk Analysis system was documented as having a FIPS 199 rating of low. However, upon inspection of the system security plan, the evaluation team noted that the confidentiality of the system was rated as moderate, the integrity was rated as high, and the availability was rated as low. Consequently, the evaluation team determined that the FIPS 199 categorization for the Risk Analysis system was not consistent with information found in the system security plan. Exception noted.

  - OTS – The evaluation team noted that the ADM 200 Personnel/Payroll system was documented as having a FIPS 199 categorization of low. However, upon inspection of the system security plan, the evaluation team noted a confidentiality rating of high, an integrity rating of high, and an availability rating of moderate. Consequently, the evaluation team determined that the FIPS 199 categorization was not consistent with information found in the system security plan. Also, the evaluation team noted that OTS did not perform a self assessment on the ADM200 Payroll/Personnel system. Exception noted.

  - TIGTA - The evaluation team inspected that the MWI Self Assessment and noted that TIGTA did not address each critical element in its entirety. Exception noted.

Summary: Based on the scope of this review, Treasury should ensure that the OIG is included in the development and verification of the bureaus' systems inventories. In addition, C&A memos should be documented, approved by the responsible parties, and maintained for each system. Additionally, self

assessments should be performed annually. Finally, improvements should be made to ensure that Treasury is consistently assigning FIPS 199 ratings that correspond to the system's confidentiality, integrity, and availability ratings as documented in the systems' security plans and other C&A documentation.

Question 2 – Compliance with C&A Requirements

- The evaluation team reviewed C&A data provided by the bureaus. The data provided included the numbers of systems with C&As, the number of systems for which controls had been tested and evaluated within the last year, and the number of systems that had tested contingency plans. The evaluation team also inspected evidence that contingency plans had been tested. Additionally, the evaluation team inspected the bureau C&A schedules to determine if the C&As were current and had been revised as required. A portion of the results have been included below:

  - BEP – The evaluation team noted that the TSDS Continuity of Operations (COOP) had not been tested to ensure restoration of TSDS in the event of an emergency. Exception noted.

  - BPD – The evaluation team inspected the Oracle Federal Financial Systems contingency plan, which required BPD to perform a rollback of production data. The evaluation team noted that a C&A schedule was documented, and guidance was in place supporting the need to complete C&As every three years or when a system undergoes a major change. No exception noted.

  - CDFI – The evaluation team inspected the CDFI Fund Forward Challenge 2005 After-Action Report and noted that CDFI conducted a test of their CDFI Local Area Network (LAN) COOP. Additionally, a C&A schedule was documented that included a listing of C&A activities and projected dates of future activities. No exception noted.

  - DO – The evaluation team noted that a TACT contingency plan had not been documented. In addition, TACT contingency plan testing was not performed. However, a C&A schedule had been documented and included a listing of system names, descriptions, C&A status, authority to operate dates, interface listings, indications of self assessments, contingency plan testing and other C&A activities. Exception noted.

  - FinCEN – The evaluation team noted that the Server Database system contingency plan had not been tested. The C&A schedule noted that the system had received a C&A in May 2003, and is scheduled for an updated C&A in May 2006. This schedule also noted the C&A status for other FinCEN systems. Exception noted.

  - FMS – The evaluation team inspected the FCAS Business Continuity Plan (BCP) testing results, and determined that a test plan, expected results, and actual results had not been documented. The evaluation team also inspected the FMS C&A schedule, and noted that the schedule documented a listing of the systems, the C&A level, and a target C&A completion date. Exception noted.

  - Mint – The evaluation team was informed that a contingency plan had not been developed for the Documentum system, and that contingency plan testing did not occur. The evaluation team also inspected the system's C&A schedule and noted that it included C&A activities for all of Mint's FISMA systems. Exception noted.

- OCC – The evaluation team was informed that a contingency plan was not developed for the Risk Analysis system, and testing did not occur. The evaluation team inspected the C&A schedule and noted that it included a list of OCC systems, system descriptions, C&A status, and C&A date. However, the schedule did not project future C&A activities. Exception noted.

- OTS – The evaluation team noted that the ADM200 Personnel/Payroll system contingency plan did not address all requirements prescribed by NIST SP 800-34. Specifically, the contingency plan did not address how often the contingency plan should be tested, and the types of activities that would be performed during the test. Additionally, the evaluation team inspected the C&A schedule and noted that it contained a FY 2005, FY 2006, and FY 2007 schedule of activities. Exception noted.

- TIGTA – The evaluation team was informed that the MWI contingency plan was not tested to ensure restoration of the infrastructure in the event of an emergency. Additionally, a C&A schedule was not documented. However, the evaluation team was informed that the C&A is complete for all TIGTA systems. Additionally, TIGTA determines which C&A activities are going to be performed based on the budget allocated. Exception noted.

- TTB – The evaluation team inspected the GSS contingency plan tabletop exercise and determined the testing was sufficient. Additionally, the evaluation team inspected the system inventory, which documented the status of each component of the C&A package. The evaluation team was notified that every system must obtain a C&A every three years or when a major change occurs. No exception noted.

Summary: Based on the scope of the review, Treasury should continue to test capabilities to restore operations following a disaster, and continue to make sure there is adequate supporting documentation for such efforts. Additionally, Treasury should ensure that C&A schedules are documented to ensure that the system C&As are current and have been updated as required.

Question 3 – System Inventory and Oversight of Contractor Systems

- The evaluation team inspected bureau FISMA submissions to determine which Treasury bureaus reported having contractor systems. Based on this review, the evaluation team noted that BEP, CDFI, and FinCEN reported one contractor system each, and that FMS reported three contractor systems. No other bureaus reported contractor systems. Thus, the evaluation team inspected the contracts for BEP, CDFI, FinCEN, and FMS, and performed inquiry and document inspection to determine whether contractor oversight was adequately performed. The results for testing at BEP, CDFI, FinCEN and FMS have been included below:

  - BEP – The evaluation team noted that BEP reported one contractor system. The evaluation team inspected the C&A package for this system and noted that it included security control testing performed by independent contractors. No exception noted.

  - CDFI – The evaluation team noted that CDFI reported one contractor system. The evaluation team inspected the C&A package for this system and noted that it included security control testing performed by independent contractors. No exception noted.

- FinCEN – The evaluation team noted that FinCEN reported one contractor system. The evaluation team inspected the NIST SP 800-26 self-assessment performed by independent contractors for this system, and noted no issues. No exception noted.

- FMS – The evaluation team noted that FMS reported three contractor systems. The evaluation team inspected the C&A packages for these systems and noted that they included security control testing performed by independent contractors. No exception noted.

- The evaluation team selected one system per bureau for interface testing. We inspected system security plans to determine whether a system interface had been documented for each system. For any interfaces documented in the system security plans, the evaluation team requested the supporting interface connection agreements. The evaluation team also inspected the bureaus' quarterly FY 2005 system inventory submissions to the Department CIO, and noted that the system inventories were adequately maintained and updated. Additionally, the evaluation team inspected e-authentication risk assessments as required. The specific results of the test work, by bureau, follow:

  - BEP – Upon inspecting the BEP TSD systems security plan, the evaluation team noted that all five TSD systems components were stand-alone systems that did not connect to any outside networks or the Internet. Thus, the evaluation team determined that the TSD systems do not have any interfaces. No exception noted.

  - BPD – Upon inspecting the BPD Oracle Federal Financials system security plan, the evaluation team noted that the system interfaces with the FMS Intragovernmental Payment and Accounting Collection System (IPAC). The evaluation team then inspected the BPD ISA with FMS and noted that this document had been signed by both designated approving authorities. The evaluation team further noted that FMS had identified this connection with BPD. No exception noted.

  - CDFI – Upon inspecting the CDFI LAN system security plan, the evaluation team noted that the system is connected to the Internet through the Treasury Communications System (TCS). The evaluation team then inspected the CDFI MOU with TCS and noted that this document had been signed by both designated approving authorities. The evaluation team determined that that TCS had identified this connection. No exception noted.

  - DO – Upon inspecting the TACT C&A package supplemental document, the evaluation team noted that TACT is connected to the DO LAN and Alpha Cluster. Thus, the evaluation team noted that TACT does not interface with any other Treasury bureaus outside DO. No exception noted.

  - FinCEN – The evaluation team noted that the FinCEN IT security policy does not document system interconnections or information sharing. Thus, the evaluation team noted that the FinCEN IT security policy was not developed in accordance with NIST SP 800-18 guidance. Exception noted.

  - FMS – Upon inspecting the FCAS system security plan, the evaluation team noted that FCAS receives data from the Department of State and interfaces with another FMS system, and these arrangements were documented. No exception noted.

- OCC – Upon inspecting the Risk Analysis system security plan, the evaluation team noted that the Risk Analysis system did not connect or interface with other systems. However, the evaluation team noted that OCC does have connections between other OCC systems, and agency connection agreements have not been documented. Exception noted.

- OTS – Upon inspecting the ADM200 Payroll/Personnel system security plan, the evaluation team noted that this system does not interface with any other Treasury bureau. No exception noted.

- Mint – Upon inspecting the Documentum System Security Plan, it was noted that Documentum does not interface with any other Treasury bureau. No exception noted.

- TIGTA – Upon inspecting the MWI system security plan, the evaluation team noted that MWI interfaces with three other TIGTA systems. Thus, it was noted that the MWI system does not interface with any other Treasury bureau outside of TIGTA. No exception noted.

- TTB – Upon inspecting the TTB Network Infrastructure GSS security plan, the evaluation team noted that the TTB GSS interfaces with the DO TCS. Thus, the evaluation team inspected the MOA between TTB and DO, and determined that it was signed by both designated approving authorities. Additionally, the evaluation team noted that TCS' interface documentation also references TTB. No exception noted.

Summary: Based on the scope of this review, the evaluation team noted that improvement is needed in regards to documenting connection agreements between all bureaus and agencies. In addition, Treasury should continue to perform contractor oversight to ensure contractors fulfill agreement terms. Finally, Treasury should continue to ensure that each bureau updates and maintains system inventories on a quarterly basis.

Question 4 – OIG Assessment of the POA&M Process

- CIO: The evaluation team was informed that the CIO is responsible for centrally tracking, maintaining, and reviewing bureau POA&M activities on a quarterly basis. No exception noted.

- The evaluation team performed a review of bureau POA&Ms. The evaluation team inspected the POA&Ms to determine if known IT security weaknesses had been incorporated and prioritized. Additionally, the evaluation team inspected security program review and assistance reports and OIG reports to determine if the weaknesses identified in the reports were documented in the POA&Ms. Results of this review have been included below:

  - All bureaus – IT security weaknesses identified in the POA&Ms had not been prioritized to ensure appropriate delegation of resources. Exception noted.

  - BEP, BPD, CDFI, DO, FinCEN, FMS, Mint, OCC, and TIGTA did not document weaknesses identified in the Security Program Review and Assistance Reports in the POA&Ms. Exception noted.

  - DO, FMS and Mint did not include weaknesses identified in the OIG reports (OIG-05-040, OIG-05-041 and OIG-05-043) in the POA&Ms. Exception noted.

Summary: Based on the scope of this review, the evaluation team found that the Treasury POA&Ms did not always accurately reflect identified security weaknesses. In addition, weaknesses identified in the security program review and assistance reports and OIG reports did not always agree to the POA&Ms. Consequently, Treasury needs to work to improve the POA&M process.

Question 5 – OIG Assessment of the C&A Process

- The evaluation team performed a review of one C&A package for each bureau. All components of the C&A packages were inspected, including: C&A methodology, risk assessment, system security plan, contingency plan, configuration management guide, incident response procedures, security awareness training and security, testing and evaluation (ST&E) reports. Results of this review have been included below:

  - BEP – The evaluation team inspected the TSDS C&A package and noted that all but one component was adequately documented in accordance with NIST. Specifically, the TSD COOP did not adequately address all requirements prescribed by NIST SP 800-34. Exception noted.

  - BPD – The evaluation team inspected the Oracle Federal Financial system C&A package and noted that the risk assessment and the contingency plan did not adequately address all requirements prescribed by NIST SP 800-30 and NIST SP 800-34. Exception noted.

  - CDFI – The evaluation team inspected the CDFI LAN C&A package, and noted that several key components had not been adequately addressed. Specifically, a C&A methodology had not been documented, the security plan did not include information regarding data integrity/validity controls, the Disaster Recovery Plan (DRP) did not address all requirements prescribed by NIST SP 800-34, and the risk assessment did not address all requirements as prescribed by NIST SP 800-30. Exception noted.

  - DO – The evaluation team inspected the TACT C&A package, and noted that a TACT system security plan, configuration guide, and contingency plan had not been documented. In addition, the DO building of major applications policy did not adequately address requirements prescribed by NIST SP 800-50, incident response procedures did not address requirements prescribed by NIST SP 800-61, and the risk assessment did not address all requirements as prescribed by NIST SP 800-30. Exception noted.

  - FinCEN – The evaluation team inspected the Server Database C&A package, and noted that the system security plan, contingency plan, incident response procedures, and risk assessment did not address all requirements prescribed by NIST guidance. Exception noted.

  - FMS – The evaluation team inspected the FCAS C&A package and noted that one component had not been adequately documented in accordance with NIST. It was determined that the FCAS BCP did not adequately address all requirements prescribed by NIST SP 800-34. Exception noted.

  - Mint – The evaluation team inspected the Documentum C&A package and noted that all but one component was adequately documented in accordance with NIST. However, the Documentum contingency plan had not been documented. Exception noted.

- OCC – The evaluation team inspected the Risk Analysis C&A package and noted many exceptions. Specifically, the security awareness training element did not sufficiently address all requirements prescribed by NIST SP 800-50, the C&A methodology had not been documented in accordance with NIST 800-37, the risk assessment did not address all requirements as prescribed by NIST SP 800-30, a contingency plan that documents restoration efforts for the Risk Analysis system had not been completed, and the system security plan was not completed in accordance with NIST SP 800-18. Exception noted.

- OTS – The evaluation team noted several exceptions upon inspection of the ADM200 Personnel/Payroll C&A package. Specifically, the C&A methodology had not been documented in accordance with NIST SP 800-37, the contingency plan did not address requirements prescribed by NIST SP 800-34, the security awareness training element did not contain all of the requirements prescribed by NIST SP 800-50, and a ST&E had not been performed for the system. Exception noted.

- TIGTA – The evaluation team inspected the MWI C&A package and noted that all documents inspected adequately addressed guidance prescribed by NIST, with the exception of the incident response procedures, the risk assessment, and the contingency plan. The evaluation team noted that the incident response procedures did not fully address all areas of NIST SP 800-61, the risk assessment did not adequately address all areas of NIST SP 800-30, and the contingency plan did not adequately address all areas of NIST SP 800-34. Exceptions noted.

- TTB – The evaluation team inspected the C&A package for the GSS and noted that all components adequately addressed NIST requirements. No exception noted.

Summary: The evaluation team reviewed 12 C&A packages and noted that 11 needed improvement. Treasury should work to improve the C&A process and enforce the use of NIST guidance when developing C&A documentation.

Question 6 – Configuration Management

- The evaluation team inspected data submitted by the bureaus regarding configuration management. The evaluation team assessed whether configuration guides were documented, and also determined whether an agency configuration management policy existed. Additionally, the evaluation team reviewed data supporting the implementation of the security configuration policy on the applicable systems. Additional procedures were performed at DO and BEP. The results of DO and BEP's reviews have been included below:

  - DO – The evaluation team inspected the configuration guide for the Windows operating system, which hosts the TACT system. The evaluation team documented the Windows configuration guide, inspected DO's configuration management implementation percentage responses, and performed inquiries to determine how the percentages were calculated. The evaluation team was informed that: 1) DO runs an automated tool to scan its operating systems in search of configuration management vulnerabilities, and 2) configuration management percentages for each operating system were calculated based on the results of the automated scanning tool. Lastly, the evaluation team followed up on a configuration management finding in the August 2005 OIG Report (OIG-05-043) to determine whether configuration management findings have been appropriately documented and implemented. The evaluation team noted that the OIG finding had been addressed. No exception noted.

- BEP – The evaluation team determined that the TSD system consists of four components: 1) Access Control Alarm Monitoring (ACAMS) system, 2) Configuration Management Systems Aperture (CMS) system, 3) Digital Video Recording (DVRS) system, and 4) Video Badging System (VBS). The ACAMS resides on the OS2 Operating System. CMS resides on the Microsoft Windows 2000 Server Operating System. DVRS resides partially on Microsoft Windows NT 4.0, and partially on Microsoft Windows Server 2000. VBS resides on a Microsoft Windows NT 4.0 platform. The evaluation team noted that the Windows 2000 Server Configuration Guide served as the guide for CMS, DVRS and VMS. However, the evaluation team was informed that a configuration guide has not been developed for ACAMS. Additionally, the evaluation team inquired as to BEP's methodology supporting the implementation of the security configuration policy and determined that a process was in place. Lastly, the evaluation team followed up on a configuration management finding in the March 2005 OIG Report (OIG-05-024) to determine whether configuration management findings have been appropriately documented and implemented. The evaluation team noted that the OIG finding had been addressed. Exception noted.

Summary: The evaluation team noted that improvements are needed for the configuration management process. Specifically, configuration guides need to be developed for each operating system, and an approved process should be used to support the implementation percentage for each security configuration policy.

Question 7 – Incident Detection and Handling Procedures

- The evaluation team inspected bureau and Treasury-wide incident response procedures and determined that the bureaus were responsible for reporting incidents internally to the Treasury Computer Security Incident Response Center (TCSIRC), and that Treasury is responsible for reporting incidents externally. Additionally, the evaluation team inspected OIG Incident Response Reports (OIG-05-041, OIG-05-040, and OIG-05-039), and determined that corrective actions had been taken to address the identified report weaknesses. Finally, the evaluation team inspected bureau monthly incident response reports submitted to TCSIRC to assess whether the bureaus followed the incident response procedures. The evaluation team inspected monthly incident response reports for all bureaus, with the exception of CDFI, and noted that the following information was captured on each report: misuse of resources, loss or theft of equipment with unclassified information, probes and reconnaissance scans, unsuccessful access or penetration attempts and malicious code detections. No exception noted.

Summary: The evaluation team reviewed bureau and Treasury wide incident response procedures and determined that the bureaus were following the guidance. However, improvements are still needed to ensure that the incident response procedures have been documented in accordance with NIST guidance (see Question 5 for further discussion regarding incident response).

Question 8 – Security Training and Awareness

- The evaluation team inspected the Treasury IT security awareness training program for each bureau, and also inspected FY 2005 listings of employees and contractors who had completed the training. Additionally, the evaluation team selected three bureaus (FMS, OTS, and BEP) to perform detailed testing. The evaluation team judgmentally selected 30 individuals each from FMS, OTS, and BEP that had completed the IT security awareness training, and requested evidence that the training had

been completed. Additionally, the evaluation team inspected evidence that the CIO, Deputy CIO and CISO received specialized training during the fiscal year. Results of this review follow:

- BEP, BPD, CDFI, FMS and TTB – No exceptions were noted upon inspection of each bureau's IT security awareness training program.

- DO – The evaluation team noted several exceptions related to DO's IT security awareness training program. Specifically, DO was not able to provide the evaluation team with the number of contractors that required training. Additionally, the evaluation team was informed that many records supporting security awareness training were lost when the database holding the records crashed and backup data was not available. Finally, only 40 percent of DO employees have completed the training. Exceptions noted.

- FinCEN – The evaluation team noted that the CIO, Deputy CIO, and CISO did not receive specialized training during FY 2005. No other weaknesses were noted regarding FinCEN's IT security awareness training program. Exception noted.

- Mint – The evaluation team noted that the CIO, Deputy CIO, and CISO did not receive specialized training during FY 2005. No other weaknesses were noted regarding the Mint's IT security awareness training program. Exception noted.

- OCC – The evaluation team noted that the CIO, Deputy CIO, and CISO did not receive specialized training during FY 2005. No other weaknesses were noted regarding OCC's IT security awareness training program. Exception noted.

- OTS – The evaluation team noted that the CIO did not receive specialized training during FY 2005. Additionally, although OTS was able to provide the evaluation team with evidence that 29 out of 30 employees selected for testing had completed the security awareness training, evidence for one employee could not be provided. Exception noted.

- TIGTA – The evaluation team noted that the Deputy CIO did not receive specialized training during FY 2005. No other weaknesses were noted regarding TIGTA's IT security awareness training program. Exception noted.

Summary: Based on the scope of the review, the evaluation team determined that enhancements are needed over the Treasury's IT security awareness training program. Treasury should work to improve the IT security awareness training program by enforcing specialized training for personnel with significant security responsibilities, and by ensuring that all employees and contractors receive the annual security awareness training (see Question 5 for further discussion regarding IT security awareness training programs).

Question 9 – Peer-to-Peer File Sharing

- The evaluation team inspected documentation to assess whether bureaus addressed peer-to-peer file sharing in their IT security awareness training, ethics training, or any other agency wide training. The evaluation team also assessed whether employees and contractors received the training. Results of this review follow:

- BEP – The evaluation team inspected BEP's IT security awareness course and noted that it addressed peer-to-peer file sharing restrictions. The evaluation team determined that BEP employees and contractors received the IT security awareness course and thus had received training regarding peer-to-peer file sharing restrictions. No exception noted.

- BPD – The evaluation team inspected BPD's end user security awareness training and noted that it addressed peer-to-peer file sharing restrictions. The evaluation team determined that BPD employees and contractors had received the end user security awareness training. Therefore, the evaluation team determined that BPD employees and contractors received training regarding peer-to-peer file sharing restrictions. No exception noted.

- CDFI – The evaluation team inspected CDFI's peer-to-peer file sharing policy, and noted that it addressed peer-to-peer file sharing restrictions. The evaluation team noted that all CDFI employees and contractors were required to review and sign the policy. Therefore, the evaluation team determined that CDFI employees received training regarding peer-to-peer file sharing. No exception noted.

- DO – The evaluation team noted that DO addressed peer-to-peer file sharing restrictions by utilizing Treasury's IT security awareness training course. However, the evaluation team noted several weaknesses surrounding DO's IT security awareness training program (as noted above in Question 8). Therefore, the evaluation team determined that not all DO employees and contractors had received the Treasury IT security awareness training course. Therefore, not all employees and contractors received training regarding peer-to-peer file sharing restrictions. Exception noted.

- FinCEN – The evaluation team noted that FinCEN addressed peer-to-peer file sharing restrictions by utilizing Treasury's IT security awareness training course. The evaluation team determined that FinCEN employees and contractors had received the Treasury IT security awareness training course. Therefore, the evaluation team determined that FinCEN employees and contractors received training regarding peer-to-peer file sharing restrictions. No exception noted.

- FMS – FMS provided the evaluation team with their security awareness training program. Upon inspection of the training, the evaluation team noted that it addressed peer-to-peer file restrictions. The evaluation team determined that FMS employees and contractors had received the security awareness training. Therefore, the evaluation team determined that FMS employees and contractors received training regarding peer-to-peer file sharing restrictions. No exception noted.

- Mint – The evaluation team inspected the Mint information security awareness briefing and determined that the Mint included peer-to-peer file sharing training within the content of the security awareness training presentation given to all employees and contractors. Therefore, the evaluation team determined that Mint employees and contractors received training regarding peer-to-peer file sharing restrictions. No exception noted.

- OCC – The evaluation team inspected the IT security awareness training program and noted that the content did not sufficiently address peer-to-peer file sharing training. However, the evaluation team also inspected the OCC newsletter and determined that it addressed peer-to-peer file restrictions. However, the evaluation team was informed that OCC has no mechanism in place to track whether or not individuals received the OCC newsletter. Therefore, the evaluation

team was not able to determine that not all employees and contractors were aware of peer-to-peer file sharing restrictions. Exception noted.

- OTS – The evaluation team inspected OTS's technology security awareness user guide and noted that it addressed peer-to-peer file sharing restrictions. As noted in Question 8 above, the evaluation team judgmentally selected 30 employees for testing and verified whether or not they had completed the training. OTS provided the evaluation team with evidence for 29 out of 30 individuals selected. However, evidence could not be provided for one individual. Therefore, the evaluation team determined that not all employees and contractors received the information regarding peer-to-peer file sharing restrictions. Exception noted.

- TIGTA – The evaluation team noted that TIGTA addressed peer-to-peer file sharing restrictions by utilizing Treasury's IT security awareness training course. The evaluation team determined that TIGTA employees and contractors had received the Treasury IT security awareness training course. Therefore, the evaluation team determined that TIGTA employees and contractors received training regarding peer-to-peer file sharing restrictions. No exception noted.

- TTB – The evaluation team noted that TTB addressed peer-to-peer file sharing restrictions by utilizing Treasury's IT security awareness training course. The evaluation team determined that TTB employees and contractors received the Treasury IT security awareness training course. Therefore, the evaluation team determined that TTB employees and contractors received training regarding peer-to-peer file sharing restrictions. No exception noted.

Summary: Based on the scope of the review, the evaluation team determined that improvements are needed for training related to peer-to-peer file sharing. Treasury should improve the IT security awareness training program by including peer-to-peer information in the annual security awareness training and ensuring that all employees and contractors receive the training.

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 07, 2005

MEMORANDUM FOR Louis King
Director, Information Technology Audits
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 2005

We are pleased to submit the Treasury Inspector General for Tax Administration's (TIGTA) Federal Information Security Management Act (FISMA)[1] report for Fiscal Year (FY) 2005. The attached spreadsheet presents our independent evaluation of the status of information technology security at the Internal Revenue Service (IRS). Our evaluation was based on Office of Management and Budget (OMB) reporting guidelines.

During FY 2005, the IRS made strides toward improving security in the bureau. Most significantly, the IRS developed a corporate approach to FISMA by elevating its FISMA processes and procedures into an enterprise-wide program. A cross-organizational FISMA working group was created, reporting to an Executive Steering Committee for the development and effective collaboration of FISMA activities. The FISMA working group developed a Concept of Operations, established security roles and responsibilities, and identified budget and resource requirements. Executive position descriptions now reflect security responsibilities. Additionally, a Security Program Management Office was established within each business unit to provide guidance and consistency across the IRS business units in implementing FISMA requirements. IRS business unit owners were more involved in the annual self-assessments of applications. In addition, the IRS developed new Plans Of Action and Milestones (POA&M) and discarded those used in prior years. The new POA&M process should enable the IRS to make risk-based, cost effective decisions to correct security weaknesses.

[1] The FISMA is part of the E Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301, 2002.

Recognizing that it will take time to achieve long-term improvements, we found that the process changes taken by the IRS have not yet had a positive effect on some measurements requested by the OMB. Specifically, we noted concerns with the IRS' system inventory categorization, certification and accreditation, continuous monitoring, tracking corrective actions, training employees with key security responsibilities, contractor oversight, and security configuration policies.

As a result, we believe that sufficient attention is not yet being given to the security of all sensitive systems and to contractor activities. The IRS continues to use a large number of systems containing sensitive taxpayer data that have been ranked as low risk, most of which have not been certified and accredited, and have not been adequately tested on an annual basis.

To complete our review, we chose a representative subset of 17 systems including 7 general support systems[2] and 10 major applications.[3] We also evaluated certifications and accreditations for 10 systems, assessed whether employees with significant security responsibilities were identified and sufficiently trained, and determined the extent of the IRS' oversight of contractors who have access to Federal tax data. Our concerns are outlined below.

Systems Inventory OMB guidance for the FY 2005 FISMA reporting states, "FISMA applies to information systems used or operated by an agency or a contractor of an agency or other organization on behalf of an agency. All systems meeting this definition shall be included in the report."

The IRS has a total of 280 systems in its inventory which we believe should have been reported in its FY 2005 FISMA submission. However, the IRS reported 82 general support systems and major applications, which we believe is contrary to OMB guidance. The IRS considers the remaining 198 systems to be non-major systems. The IRS assigned all of its non-major applications to a general support system with the assumption that the general support systems provide the majority of the security controls for the non-major applications. For its approach to be effective, the IRS must assess the risk of all systems, document the controls for each system, and assign accountability for the specific controls.

Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, requires that the risk of all systems must be categorized as high, moderate, or low considering the confidentiality, integrity, and availability requirements of the information processed by the systems. National Institute of Standards and Technology (NIST) Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, must be used in categorizing the risk for the information systems. The IRS applied the FIPS 199 security categorization to all of its systems, however, the IRS did

[2] A general support system is an interconnected set of information resources under the same direct management control that shares common functionality.

[3] A major application requires special management oversight because of the information it contains, processes, or transmits, or because of its criticality to the organization's mission.

not use the guidance provided in NIST SP 800-60 in performing the risk categorization of its non-major systems. All non-major applications were ranked as low risk for confidentiality, integrity, and availability even though several contained sensitive taxpayer and employee information. NIST SP 800-60 states that taxpayer information should be considered at least a moderate risk. The risk categorization is important because it helps determine the level of security controls needed for each system. By not applying the NIST standards to the non-major applications, sufficient security controls may not be identified and implemented. The Chief, Mission Assurance and Security Services (MA&SS) advised that a priority for Fiscal Year 2006 will be to more thoroughly review and re-validate the currently assigned risk impact levels of its non-major applications, using the guidance provided in NIST SP 800-60.

National Institute of Standards and Technology (NIST) Special Publication 800-18, Guide for Developing Security Plans for Federal Information Systems, states that when non-major applications are bundled with a general support system, the security requirements for each of the non-major applications be included in the general support system's security plan. None of the general support system security plans we reviewed addressed specific controls for non-major applications nor assigned specific accountability for those controls.

While the IRS' general support systems provide security controls to prevent hackers from entering the network, application-level controls are also critical to prevent unauthorized accesses to sensitive data by employees and contractors who already have access to the IRS network. Since risk categorizations have not been applied using NIST guidelines and because specific controls have not been documented and accountability for those controls has not been assigned, we are concerned that business unit owners of non-major applications are relying too heavily on the general support system controls to protect sensitive data. Results of our review of certifications and accreditations and annual self-assessments described below add to our concerns.

Certification and Accreditation NIST Special Publication 800-37, Guide for the Security and Accreditation of Federal Information Systems, requires that all systems must be certified and accredited every three years or when major changes to systems occur. In the IRS, the Chief, MA&SS is the certifying authority for all systems. The Chief, MA&SS must test the systems and provide the results to the business unit owner along with the systems' security plans, and POA&Ms to correct weaknesses. Business unit owners must then evaluate the information and determine whether to accredit the system, thereby giving it an authority to operate. By accrediting the system, the business unit owner accepts responsibility for the security of the system and is fully accountable for any adverse impacts if security breaches occur.

The IRS reported that 90 percent of its 82 general support systems and major applications were certified and accredited. However, if all systems were reported as we believe OMB requires, only 35 percent of its 280 systems should have been reported as certified and accredited.

We conducted a more thorough review of 10 systems that had been certified and accredited to evaluate the IRS process. Our review included documentation for 6 general support systems and 4 major applications. During FY 2005, the IRS prioritized its efforts by focusing attention first on its general support systems. The IRS certified and accredited the general support systems in compliance with NIST standards, except security plans did not include controls for the bundled non-major applications as we discussed earlier.

The IRS has recently begun to focus attention on improving the certification and accreditation process for its major applications. In our review of 4 major applications, System Security Plans and Security Test and Evaluation documents for major applications did not comply with NIST standards. Controls presented in the plans were not sufficiently detailed and were not based on risk levels established by FIPS Publication 199. Tests did not include all system components such as encryption, telecommunication links, and user account management. Only 16 percent of the systems we reviewed showed that contingency plans had been tested. The IRS has not yet focused attention on the certification and accreditation process for its non-major applications.

Continuous Monitoring In addition to certifying and accrediting systems every three years, NIST 800-37 requires that a system of continuous monitoring of systems be in place. System owners must complete a self-assessment required by NIST at least annually.

In our opinion, self-assessments conducted by the IRS using NIST SP 800-26 did not include adequate testing of application controls. System owners often referred only to the general support system controls to address security elements that should have been reviewed at the application level. For example, a question on the self-assessment for a major application, the Tax Return Data Base asks, “Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access?” The response stated that controls are implemented and the scoring is based on a composite score of several general support systems. The IRS responded similarly to questions regarding password controls and audit trails for the Combined Annual Wage Reporting, a major application that allows the IRS and the Social Security Administration (SSA) to improve the accuracy of annual wage data reported by comparing tax payments on IRS and SSA forms. In each of these examples, no references were made in the self-assessment document to the application controls, only to the controls of the general support system.

We found in our representative subset of 17 systems, that 9 systems (53 percent) had been certified during FY 2005. We considered these systems to have been tested and evaluated in FY 2005.

Tracking Corrective Actions As previously mentioned, during FY 2005 the IRS revised its POA&M process and we are hopeful that the changes will be effective. The IRS advised that it is tracking all security weaknesses in a database and developing POA&Ms for the high priority weaknesses that they can address with available

resources. Since the POA&Ms were not completed by the IRS until early September 2005, we did not have an opportunity to evaluate the IRS' prioritization of weaknesses. We were able to determine that the POA&Ms:

- include weaknesses from IRS internal reviews, as well as most TIGTA and Government Accountability Office reviews.
- are tailored to specific applications and no longer capture standard, repetitive wording as they did in past years.
- indicate that the IRS appears to have analyzed and prioritized weaknesses and have included corrective actions in the POA&Ms.

While additional refinements will be made during the coming year, we find the progress made in this area noteworthy.

Training Employees with Key Security Responsibilities The OMB requires that all employees with key security responsibilities be given security-related training at least annually. In FY 2004, we reported that the Office of Mission Assurance and Security Services did not have an adequate tracking process in place to ensure all employees with significant security responsibilities were identified and trained. As a result, the IRS did not accurately identify the number of employees with significant security responsibilities or the number of employees trained.

In FY 2005, security awareness training was provided to all of its employees and contractors. In its FY 2005 FISMA submission, the IRS reported it has 2,737 employees with significant information technology security responsibilities and that 300 (11 percent) of those employees received specialized training. We could not verify this information since the IRS still has no tracking system in place to identify persons with significant security responsibilities and the specialized training completed. The IRS advised that it plans to implement a tracking system in FY 2006.

In prior audits, we have attributed several security weaknesses to a lack of adequate training for system administrators. Since only 11 percent of these employees have been trained this year according to the IRS, we expect these weaknesses to persist.

Oversight of Contractors FY 2005 OMB guidance for completing the agency and Inspector General FISMA reports states that agency IT security programs apply to all organizations which possess or use Federal information, or which operate, use, or have access to Federal information systems on behalf of a Federal agency. Such other organizations may include contractors, grantees, State and local governments, industry partners, etc. FISMA guidelines emphasize OMB longstanding policy concerning sharing government information and interconnecting systems. Therefore, Federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls. Agencies must develop policies for information security oversight of contractors and other users with privileged access to Federal data. We believe the following conditions indicate a need for significantly increased IRS oversight of contractors and state agencies that have access to Federal tax data.

We conducted a separate review this year of the monitoring of contractor access to networks and data.[4] The overall objective of this review was to determine whether IRS management implemented adequate controls over the PRIME contractor's[5] access to IRS networks and data. We found the IRS gave the PRIME contractor the authority to add, delete, and modify its own employees' user accounts on IRS systems. Our review showed that the PRIME contractor added user accounts without any oversight by the IRS during at least a 1-year period.

We also conducted a separate review to determine whether State tax agencies were protecting Federal tax information provided by the IRS from unauthorized use and disclosure.[6] Internal Revenue Code (I.R.C.) 6103 requires the IRS to disclose Federal tax information to various state and Federal agencies. State tax agencies can use this information to identify non-filers of State tax returns, determine discrepancies in the reporting of income, locate delinquent taxpayers, and determine whether IRS adjustments have State tax consequences. The IRS is responsible for ensuring that State tax agencies properly safeguard federal tax information. To do this, the IRS' Safeguard Program encompasses reviewing and approving Safeguard Procedures and Safeguard Activity Reports submitted by State tax agencies and conducting on-site Safeguard Reviews of each state tax agency at least once every 3 years. Based on the instructions published by the OMB, it is our opinion that, as users of vast amounts of Federal tax data, the States should be required to protect that data in accordance with FISMA requirements. Accordingly, State agencies should be required to conduct annual self-assessments using NIST Special Publication 800-26 and to track and monitor corrective actions using POA&Ms.

However, the IRS does not require State agencies to conduct self-assessments of its systems using NIST Special Publication 800-26 and does not require them to monitor and track corrective actions using POA&Ms. In addition, the IRS has not provided sufficient and timely reviews over the security of Federal tax information maintained by the States. The IRS believes that States are not required to comply with FISMA requirements because they do not use the Federal tax data they receive *on behalf* of the IRS.

Security Configuration Policies Detailed security testing results were not provided for our review for any systems. Therefore, we could not evaluate the extent of implementation of the security configuration policies.

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

---

[4] *Monitoring of PRIME Contractor Access to Networks and Data Needs to Be Improved* (Reference Number 2005-20-185, dated September 2005).

[5] The PRIME contractor is the Computer Sciences Corporation, which heads an alliance of leading technology companies brought together to assist with the IRS' efforts to modernize its computer systems and related information technology.

[6] *Increased IRS Oversight of State agencies Is Needed to Ensure Federal Tax Information Is Protected* (Reference Number 2005-20-184, dated September 2005).

Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name:

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

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.

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation , a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						Question 2					
		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Bureau	High	2	2	0	0	2	2	2	100.0%	0	0.0%	2	100.0%
	Moderate	79	15	8	3	79	15	13	86.6%	9	60.0%	3	20.0%
	Low	1	0	3	0	1	0	0	0.0%	0	0.0%	0	0.0%
	Not Categorized			1	0								
	Sub-total	**82**	**17**	**12**	**3**	**82**	**17**	**15**	**88.2%**	**9**	**52.9%**	**5**	**29.4%**
Agency Totals	**High**	**2**	**2**	**0**	**0**	**2**	**2**	**2**	100.0%	**0**	0.0%	**2**	100.0%
	Moderate	**79**	**15**	**8**	**3**	**79**	**15**	**13**	86.6%	**9**	60.0%	**3**	20.0%
	Low	**1**	**0**	**3**	**0**	**1**	**0**	**0**	0.0%	**0**	0.0%	**0**	0.0%
	Not Categorized	**0**	**0**	**1**	**0**								
	Total	**82**	**17**	**12**	**3**	**82**	**17**	**15**	88.2%	**9**	52.9%	**5**	29.4%

Question 3

In the format below, evaluate the agency's oversight of contractor systems, and 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. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. 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	- Rarely, for example, approximately 0-50% of the time"
3.b.	The agency has developed an 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: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 96-100% complete
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	No
3.d.	The OIG **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.	No
3.e.	The agency inventory is maintained and updated at least annually.	Yes

3.f.	The agency has completed system e-authentication risk assessments.	Yes

Question 4

Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below.

For items 4a.-4.f, the response categories are as follows:

- 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, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Almost Always, for example, approximately 96-100% of the time
4.d.	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.	OIG findings are incorporated into the POA&M process.	- Frequently, for example, approximately 71-80% 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

Comments: Question 1.a - The IRS has a total of 280 systems, 199 of which are non-major applications. IRS is reporting only its 82 major systems, which we believe is contrary to OMB guidance which requires that all systems be reported. To be consistent with other Treasury bureaus, we are including 82 in our template. However, we selected our representative subset of systems from the population of 280 systems. **Questions 1.b & 1.c -** IRS has 12 contractor support functions that require oversight. We have reported these in Question 1.b; however, since these are not systems, they are not reflected in the total in Question 1.c. **Question 2.a -** The IRS reported that it has certified and accredited 90% of its major systems. However, only 35 percent of its 280 systems have been certified and accredited. **Question 2.b -** Self-Assessment performance levels for Major Applications are often based on the performance level for the associated GSS rather than on application specific controls. **Question 3.a -** We reviewed 3 of IRS' 12 contractor systems and found IRS' reviews to be generally adequate. We conducted separate reviews this year of IRS's monitoring of contractor access to networks and data and whether State agencies adequately protect federal tax data. These reviews showed the need for significantly increased oversight by the IRS of contractors and State agencies. **Qu**

Question 5

OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May, 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.

	Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Satisfactory

Comments: Question 5 - IRS prioritized its C&A efforts by focusing attention first on its General Support Systems (GSS) during FY 2005 and has recently begun to focus attention on improvement of the C&A process for its MAs. We found the C&A documentation for the GSSs was generally in compliance with NIST standards; however, application controls for non-major systems were not sufficiently addressed in the GSS security plans. C&A documentation for the MAs needs improvement. System Security Plans and Security Test and Evaluation documents for MAs generally did not comply with NIST standards. Controls presented in the plans were not sufficiently detailed and were not based on FIPS 199 security impact levels. Tests did not include all system components such as encryption, datacom links and user account management.

Section B: Inspector General. Question 6, 7, 8, and 9.

Agency Name:

Question 6

6.a.	Is there an agency wide security configuration policy? Yes or No.	Yes
	Comments:	

6.b. Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows NT	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows 2000 Professional	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows 2000 Server	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows 2003 Server	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Solaris	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
HP-UX	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Linux	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Cisco Router IOS	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Oracle	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Other. Specify:			

Comments: Detailed security testing results were not provided for our review for any systems. Therefore, we rated the extent of implementation of the security configuration policy as Rarely, or, on approximately 0-50% o f the systems running each software product.

Question 7

Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes

Comments:

Question 8

8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Rarely, or, approximately 0-50% of employees have sufficient training
Comments: IRS has provided security awareness training to all of its employees and contractors. IRS reported it has 2737 employees with significant IT security responsibilities and that 300 of those received specialized training. We could not verify this information because IRS currently has no tracking mechanisms to identify persons with significant security responsibilities and the specialized training they received. IRS expects to have these controls implemented during FY 2006.		
Question 9		
9	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	Yes