Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2006

September 19, 2006

Reference Number: 2006-20-179

Phone Number | 202-927-7037
Email Address | Bonnie.Heald@tigta.treas.gov
Web Site | http://www.tigta.gov

Background

The Federal Information Security Management Act (FISMA)[1] requires each Federal Government agency to report annually to the Office of Management and Budget (OMB) on the effectiveness of its security programs. In addition, the FISMA requires that each agency shall have performed an annual independent evaluation of the information security program and practices of that agency. In compliance with the FISMA requirements, the Treasury Inspector General for Tax Administration (TIGTA) performs the annual independent evaluation of the security program and practices of the Internal Revenue Service.

The OMB provides information security performance measures by which each agency is evaluated for the FISMA review. The OMB uses the information from the agencies and independent evaluations to help assess agency-specific and Federal Government-wide security performance, develop its annual security report to Congress, assist in improving and maintaining adequate agency security performance, and assist in the development of the E-Government Scorecard under the President's Management Agenda.

Attached is the TIGTA's Fiscal Year 2006 FISMA report. The report was forwarded to the Treasury Inspector General for consolidation into a report issued to the Department of the Treasury's Chief Information Officer.

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

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 19, 2006

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

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2006

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 2006. Attachment I presents our independent evaluation of the status of information technology security at the Internal Revenue Service (IRS). We based our evaluation on the Office of Management and Budget (OMB) reporting guidelines.

During the 2006 evaluation period,[2] we also conducted 14 audits to evaluate the adequacy of information security in the IRS. We considered results from these audits when making our assessment. Attachment II is a list of these specific audits.

The IRS has made steady progress in complying with FISMA requirements since the enactment of the FISMA in 2002. During 2006, the IRS reassessed the security risks of each of its systems. We are now confident that the inventory of IRS systems is substantially complete and the risk categorizations are accurate. The IRS also made significant improvements in the security certification and accreditation process. A working group,[3] with participation from all the IRS business units, continued its weekly meetings to plan and refine processes for FISMA compliance. The IRS also continued to work closely in seeking guidance and concurrence on FISMA issues with the TIGTA and the Department of the Treasury Chief Information Officer to

[1] Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).
[2] The FISMA reporting period for the Department of the Treasury is July 2005 through June 2006.
[3] IRS Security Program Management Office Council.

improve compliance with the National Institute of Standards and Technology (NIST)[4] and FISMA requirements.

To complete our review we evaluated a representative sample of 15 IRS information systems to determine whether they had been certified and accredited and whether security controls had been tested within the last year. We reviewed 10 IRS information systems to evaluate the adequacy of the certification and accreditation process and conducted separate tests to evaluate processes for Plans of Action and Milestones (POA&M), configuration management, incident reporting, awareness training, training for employees with significant security responsibilities, and ensuring privacy of sensitive information. Our evaluation of the IRS' 2006 performance against specific OMB security measures, as well as our audit work performed during the 2006 evaluation period, show that the IRS still needs to do more to adequately secure its systems and data. Provided in this document are security performance improvements as well as areas that require additional attention.

Systems Inventory An accurate systems inventory is one of the cornerstones of an effective security program. The IRS updates its inventory on an ongoing basis and reviews the system inventory monthly and annually for accuracy and completeness. In this year's FISMA evaluation, the IRS reported on its total inventory of 264 systems. In addition, during the 2006 review period, the Office of Mission Assurance and Security Services, in coordination with each of the business units, reevaluated the risk of all 264 systems. The risk categorization forms the basis for selecting an appropriate set of security controls to protect the confidentiality, integrity, and availability of systems and data. We are confident that the systems inventory is substantially complete and the risk categorizations for IRS systems are accurate.

Certification and Accreditation OMB guidelines for minimum security controls in Federal Government information systems require that all systems be certified and accredited every 3 years or when major system changes occur. In the IRS, the Chief, Mission Assurance and Security Services, is the certifying authority for all systems. The Chief, Mission Assurance and Security Services, must test[5] the security controls in the information system and provide the results to the business unit owners. 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 95.5 percent of it systems had current certifications and accreditations in Fiscal Year 2006. From our review of a sample (15 systems), we reported 100 percent had current certifications and accreditations. We attribute the difference to the limited number of systems we reviewed in our sample.

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

[5] In testing the security controls, the certification agent determines the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the information system.

In 2006, the IRS developed a repeatable, NIST-compliant process designed to ensure a thorough assessment of system risk and security from which the system owner can make an appropriate accreditation decision. The IRS used this approach to evaluate its systems inventory. However, during our review, we noted problems with the execution of this process. For example, we found that application-specific controls were sometimes erroneously described as common controls and, as a result, they were not tested.

We also found examples of controls that were accepted without adequate testing. For example, tests of the account management controls for a moderate risk system were based on interviews only. Appropriate testing procedures should have included examinations of organizational records, user accounts, and configuration settings. Additionally, the business units did not always track weaknesses identified during the certification process for remediation.

Continuous Monitoring The NIST Special Publication 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Systems*, states that a critical aspect of the security certification and accreditation process is the post-accreditation period involving the oversight and monitoring of the information system's security controls. The NIST requires the testing of an appropriate set of security controls every year throughout the system life cycle but not necessarily to the same extent required for a certification.

In 2006, the IRS did not make progress in implementing annual testing requirements. From our sample of 15 systems, we determined that the IRS met annual testing requirements on only 7 of 15 (46.6 percent) systems we reviewed because they were tested during the certification process. On those systems that were not certified during the year, self-assessments were conducted but were generally based on tests of the operating systems only. We recognize these tests are useful; however, by not testing application-specific controls, business units cannot be confident that the privacy of sensitive taxpayer information is adequately protected.

The Department of the Treasury's Chief Information Officer recognizes that all bureaus need to improve compliance with the NIST annual testing requirements and recently issued draft guidance on the subject. The IRS agrees that this is an area for improvement and plans to have an improved process in place in Fiscal Year 2007.

Tracking Corrective Actions All Federal Government agencies are required to use the POA&M process to prioritize, track, and resolve security weaknesses. The IRS has developed, implemented, and is currently managing a POA&M process; however, the process needs improvement to ensure that all weaknesses from audit reports and vulnerability scans are tracked in POA&Ms.

From 9 TIGTA security reports issued during the 2006 FISMA reporting period, we could locate POA&Ms addressing only 11 of 41 (26.8 percent) recommendations and 11 of 47 (23.4 percent) proposed corrective actions. Also, in September 2005, the TIGTA issued an audit report[6] in which we noted that problems identified during vulnerability scans and penetration tests were not formally provided to the business units, and corrective actions were not documented in POA&Ms.

[6] *The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made* (Reference Number 2005-20-143, dated September 2005).

Security Configuration Policies The OMB requires that agencies have configuration guides in place for software to ensure consistent implementation across the agency. During 2006, the IRS provided configuration guides for all eight types of operating system, database, and router software running on IRS systems.

The IRS provided test results that demonstrated implementation for configuration policies for 6 of the 8 software types on at least 81 percent - 95 percent of the systems running the software. However, it could not provide documentation of testing done to demonstrate the extent to which security configuration guides were implemented for the other two software products. These software products, if improperly configured, could make the IRS' network vulnerable to disruptions of service and thefts of sensitive information by hackers, employees, and contractors.

Incident Reporting Procedures The IRS Computer Security Incident Response Center (CSIRC) in the Mission Assurance and Security Services organization provides IRS-wide assistance and guidance for incident handling. The CSIRC defines a security incident as ". . . any adverse event whereby some aspect of computer security could be threatened."

The loss or theft of an information technology asset, including laptop computers and other portable devices, is a type of incident that could result in unauthorized access to systems and information. The IRS' incident reporting procedures require reporting this type of incident to an employee's first-line manager immediately upon detection, who should then notify the CSIRC and the TIGTA.

For 2006, we believe the IRS has not complied with CSIRC incident reporting policies and procedures. Employees' managers did not follow procedures for reporting the loss or theft of laptops and other portable devices to the IRS and the TIGTA. In a separate, ongoing audit,[7] we found the CSIRC and the TIGTA were not notified of incidents involving lost or stolen computer devices (e.g., laptops, Blackberries).

We recognize that incidents regarding lost or stolen portable devices are not the only type of incidents that require reporting to the CSIRC and the TIGTA. However, due to the significance of this type of incident and the risk of loss and misuse of personal information that these incidents pose, it appears the IRS is not in compliance with incident reporting policies and procedures.

Awareness Training The NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, states that an awareness training program is crucial for all users since it is the vehicle for disseminating information that users need to do their jobs. The IRS provided security awareness training to all of its employees but did not ensure all of its contractors received security awareness training. The IRS records showed that 998 contractors received security awareness training. Based on the 2,323 contractors reported by the IRS for 2006, we determined that 1,325 (57 percent) did not receive security awareness training. To ensure that all contractors receive security awareness training, further improvements are needed.

[7] Protection of Sensitive Data on Electronic Media (Audit Number 200620001, report due in November 2006).

Training Employees With Key Security Responsibilities The OMB requires that all employees with key security responsibilities be given security-related training at least annually. The IRS has improved its performance in this area in 2006 and now has a process in place for identifying employees with significant security responsibilities. The IRS has also implemented the Electronic Learning Management System to centrally track specialized security training provided. However, further improvements are needed to ensure that employees with significant security responsibilities receive sufficient security training.

The IRS reported that 2,447 of 2,476 (99 percent) employees with significant security responsibilities received specialized security training during the reporting period. Since the OMB and NIST have not provided minimum training requirements for employees with key security responsibilities, the IRS considered an employee trained if he or she received any training during the reporting period. We determined, however, that only 1,712 (69 percent) employees received 8 hours or more of training (an amount we arbitrarily selected) during the entire reporting period. The Department of the Treasury has indicated it will provide more specific training requirements for the 2007 reporting period.

Training employees with key security responsibilities requires more emphasis. We have attributed several weaknesses in past audit reports to the lack of training provided to these employees. Without sufficient training, these weaknesses will continue.

Privacy Requirements In March 2006, the TIGTA completed field work on an audit[8] to determine whether the Office of Privacy has effective controls and procedures to ensure IRS computer systems and employees adhere to privacy regulations. We determined that the IRS did not comply with Section 208 of the E-Government Act[9] on privacy requirements. Specifically, the IRS needs to take further actions to conduct evaluations for all systems and applications which collect personal information and to enhance its processes to better monitor compliance with privacy policy and procedures. Since we completed the fieldwork on this audit, the IRS has made several improvements to better comply with privacy regulations by conducting privacy impact assessments for most of its systems and applications and developing an agency-wide privacy training program. Corrective actions are in process to complete assessments for the remainder of its applications, provide job-specific privacy training, and improve continuous monitoring capabilities.

[8] *The Monitoring of Privacy Over Taxpayer Data Is Improving Although Enhancements Can Be Made to Ensure Compliance with Privacy Requirements* (Reference Number 2006-20-166, dated September 2006).
[9] E-Government Act of 2002, Pub. L. No. 107-347, Sec. 208 (2002).

Attachment I

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

Details of the Treasury Inspector General for Tax Administration Federal Information Security Mangement Actual Analysis

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 over the past fiscal year 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. Agency Systems		b. Contractor Systems		c. 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
Internal Revenu	High	4	2	0	0	4	2	2	100.0%	0	0.0%	0	0.0%
	Moderate	180	9	6	1	186	10	10	100.0%	5	50.0%	3	30.0%
	Low	73	3	1	0	74	3	3	100.0%	2	66.7%	1	33.3%
	Not Categorized	0	0	0	0	0	0	0	0.0%	0	0.0%	0	0.0%
Sub-total		**257**	**14**	**7**	**1**	**264**	**15**	**15**	**100.0%**	**7**	**46.7%**	**4**	**26.7%**
Agency Totals	**High**	**4**	**2**	**0**	**0**	**4**	**2**	**2**	100.0%	**0**	0.0%	**0**	0.0%
	Moderate	**180**	**9**	**6**	**1**	**186**	**10**	**10**	100.0%	**5**	50.0%	**3**	30.0%
	Low	**73**	**3**	**1**	**0**	**74**	**3**	**3**	100.0%	**2**	66.7%	**1**	33.3%
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**	0.0%	**0**	0.0%	**0**	0.0%
Total		**257**	**14**	**7**	**1**	**264**	**15**	**15**	100.0%	**7**	46.7%	**4**	26.7%

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 and/or NIST 800-53 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	- Sometimes, for example, approximately 51-70% of the time
3.b.1.	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.b.2.	If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the systems that are missing from the inventory.	Missing Agency Systems: Missing Contractor Systems:
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.	- Frequently, for example, approximately 71-80% 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).	- Frequently, for example, approximately 71-80% 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 2.b. **-** The IRS reported 61 percent of its systems were tested and evaluated in 2006. The IRS considered systems that had been certified and accredited within the reporting period as having been tested and evaluated. Using the same criteria we are reporting that 46.7 percent (7 of the 15 systems we reviewed) were tested and evaluated. We attribute the difference to the limited number of systems we reviewed in our sample. We did note that the IRS completed self-assessments during the review period for the remaining 8 systems; however, we are not recognizing self-assessments as a method of testing and evaluation. As we reported for FISMA 2005, self-assessment performance levels for applications are often based on tests of the General Support Systems which are usually conducted by the office of the CIO. We recognize these tests are useful. However, application-specific controls have not yet been selected and tested for each application as part of annual testing requirements, and business units have not been adequately involved in the testing. The IRS expects to have annual testing procedures in place in 2007.

In our 2005 FISMA assessment, we reported our concern that the IRS and State agencies do not use NIST guidelines, to monitor the security of Federal tax information provided to State agencies. We did not follow up on this concern during this 2006 assessment; however, we have an audit planned for FY 2007 to further address this issue. Question 3.a. - In 2006, the IRS certified 4 of 7 (57.14 percent) of its contractor systems and performed self-assessments for the other 3 contractor systems. As explained in the comments for Question 2.b. we do not recognize self-assessments as meeting the annual testing requirement. Therefore, we replied that the IRS provides oversight and evaluation of its contractor systems only Sometimes (51-70 percent of the time). Question 4.a. - e. - The IRS has developed, implemented, and is managing an agency-wide POA&M process; however, the process needs improvement to ensure that all weaknesses are tracked in the repository the IRS uses to generate POA&Ms.

From 9 TIGTA security reports issued during the 2006 FISMA reporting period, we could locate only 11 of 41 (26.8 percent) recommendations and 11 of 47 (23.4 percent) proposed corrective actions in the weakness repository. The repository also contained no weaknesses for 2 applications of a sample of 10 certified and accredited in 2006 even though control weaknesses were identified during the certification Security Test & Evaluation.

We located a POA&M for one of the two systems, indicating that the POA&M was not generated from the weakness repository contrary to IRS POA&M procedures. In addition, in September 2005, the TIGTA issued audit report 2005-20-143, titled, The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made, in which we reported that problems identified during vulnerability scans and penetration tests were not formally provided to the business owners, and corrective actions were not documented in POA&Ms. If all weaknesses are not entered into the weakness repository, the IRS cannot ensure that POA&Ms are developed and corrective actions are taken to address security weaknesses.

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: We reviewed a sample of 10 applications that were certified and accredited during 2006. The IRS made substantial improvements to the C&A process during the 2006 FISMA reporting period. They have implemented a repeatable, NIST-compliant process designed to ensure a thorough assessment of system risk and security from which the system owner can make an appropriate accreditation decision. While we recognize and commend the IRS on this significant progress, the process needs further improvement to support an assessment level exceeding satisfactory. As we reported in Question 2, the IRS has not implemented procedures to ensure the continuous monitoring of security controls, a key requirement of the C&A process. Such procedures would require system owners to select a subset of controls for each system they own, to be tested in the interim years when a system is not scheduled for certification. The selection of controls is a system owner decision and should consider risk as well as the degree to which a control might degrade between certification cycles.

The IRS recognizes the need to improve compliance with continuous monitoring requirements and has committed to developing a process and guidelines to better implement this control during 2007. In addition, our review of the System Security Plans (SSP) showed application-specific controls that were sometimes erroneously described as common controls resulting in the controls not being tested. We also found examples of tested controls with "PASS" ratings that were not clearly supported. For example, some tests were based on interviews only when appropriate testing procedures should have included examinations of organizational records, user accounts, and configuration settings. Additionally, weaknesses identified during the certification process were not always tracked by the business units for remediation.

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

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	- Almost Always, or on approximately 96-100% of the systems running this software
Windows NT	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Windows 2000 Professional	N/A	No	
Windows 2000 Server	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Windows 2003 Server	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Solaris	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
HP-UX	N/A	No	
Linux	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Cisco Router IOS	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Oracle	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Other. Specify:			

Comments: Our assessment differs from IRS' assessment for systems running Linux and Oracle software. For each of these, IRS reported an implementation rate of, "Mostly, or on approximately 81-95 percent of the systems running this software", while we rated the two as, "Rarely, or, on approximately 0-50 percent of the systems running this software". Our ratings reflect that IRS could not provide documentation of testing done to support the extent to which the security configuration policy has been implemented on the systems running Linux or Oracle.

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

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.	No
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities.	No
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

Comments: Questions 7.a. & b. - The IRS has not followed policies and procedures for reporting incidents internally or to law enforcement authorities. The IRS responded that they have followed incident reporting policies and procedures. Our response is based on a separate, on-going audit, in which we found that incidents involving lost or stolen computer devices (e.g., laptops, blackberries) were not reported to the CSIRC or the TIGTA. Results are still being compiled and will be reported in a separate report. We recognize that incidents regarding lost or stolen portable devices are not the only type of incident required to be reported to the CSIRC and the TIGTA. However, due to the significance of this type of incident and the risk of loss and misuse of personal information that these incidents pose, it appears that the IRS is not in compliance with incident reporting policies and procedures.

Question 8

8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?	- Sometimes, or approximately 51-70% of employees have sufficient training

Comments: We are supplementing this response with comments because a single response choice cannot be applied to the two separate performance measures addressed in Question 8; namely, awareness training for all employees (including contractors) as well as specialized security training for employees with significant security responsibilities. Awareness training - The IRS provided security awareness training to all of its employees, but did not ensure awareness training was provided to all contractors. The IRS records showed that 998 contractors received awareness training. Based on the 2,323 contractors reported by the IRS for 2006, we determined that 1,325 (57 percent) did not receive security awareness training. Further improvements are needed to ensure that all contractors receive awareness training. Specialized security training - we disagree with the IRS' response that 99 percent (2,447 of 2,476) of employees with significant security responsibilities received specialized security training. We determined only 1,712 (69 percent) of these employees received 8 hours or more of training (an amount we arbitrarily selected) during the entire reporting period. We do not agree that training of less than 8 hours meets this security requirement.

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

Attachment II

Treasury Inspector General For Tax Administration Information Technology Security Reports Issued During the 2006 Evaluation Period

1. *Security Controls for the Taxpayer Advocate Management Information System Could Be Improved* (Reference Number 2005-20-100, dated July 2005)
2. *Managers and System Administrators Need to Limit Employees' Access to Computer Systems* (Reference Number 2005-20-097, dated July 2005)
3. *More Management Attention Is Needed to Protect Critical Assets* (Reference Number 2005-20-108, dated July 2005)
4. *Security Controls Were Not Adequately Considered in the Development and Integration Phases of Modernized Systems* (Reference Number 2005-20-128, dated August 2005)
5. *Monitoring Prime Contractor Access to Networks and Data Needs to Be Improved* (Reference Number 2005-20-185, dated September 2005)
6. *Increased Internal Revenue Service Oversight of State Agencies Is Needed to Ensure Federal Tax Information Is Protected* (Reference Number 2005-20-184, dated September 2005)
7. *Internal Penetration Test of the Internal Revenue Service's Networked Computer Systems* (Reference Number 2005-20-144, dated September 2005)
8. *The Computer Security Incident Response Center Is Operating As Intended, Although Some Enhancements Can Be Made* (Reference Number 2005-20-143, dated September 2005)
9. *Contracting for Information Technology Goods and Service Generally Provided Intended Benefits; However, Maintenance Contracts Were Not Always Supported* (Reference Number 2005-20-187, dated September 2005)
10. *Federal Information Security Management Act Report for Fiscal Year 2005* (Reference Number 2006-20-071, dated October 2005)
11. *Progress Has Been Made in Using the Tivoli Software Suite, Although Enhancements Are Needed to Better Distribute Software Updates and Reconcile Computer Inventories* (Reference Number 2006-20-021, dated December 2005)
12. *Secure Configurations Are Initially Established on Employees Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation* (Reference Number 2006-20-031, dated February 2006)
13. *The Internal Revenue Service Successfully Accounted for Employees and Restored Computer Operations After Hurricanes Katrina and Rita* (Reference Number 2006-20-068, dated March 2006)
14. *The Enterprise-Wide Implementation of Active Directory Needs Increased Oversight* (Reference Number 2006-20-080,dated May 2006)