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

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 199 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).

Details of the TIGTA's FISMA 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 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	- 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	- Almost Always, for example, approximately 96-
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Almost Always, for example, approximately 96-
4.e.	OIG findings are incorporated into the POA&M process.	- Frequently, for example, approximately 71-80% of
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

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.

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