



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2007*

September 4, 2007

Reference Number: 2007-20-186

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Background

The Federal Information Security Management Act (FISMA)¹ requires each Federal Government agency to report annually to the Office of Management and Budget 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 performs the annual independent evaluation of the security program and practices of the Internal Revenue Service.

The Office of Management and Budget provides information security performance measures by which each agency is evaluated for the FISMA review. The Office of Management and Budget 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 Treasury Inspector General for Tax Administration Fiscal Year 2007 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 4, 2007

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 2007

We are pleased to submit the Treasury Inspector General for Tax Administration's Federal Information Security Management Act (FISMA)¹ report for Fiscal Year 2007. The FISMA requires the Office of Inspector General to perform an annual independent evaluation of information security policies, procedures, and practices and compliance with FISMA requirements. As such, this report presents the results of our independent evaluation of the Internal Revenue Service's (IRS) information technology security program.

We based our evaluation on the Office of Management and Budget (OMB) FISMA reporting guidelines for 2007 and the answers to the questionnaire published with the OMB guidelines (see Attachment I). During the 2007 evaluation period², we also conducted 12 audits to evaluate the adequacy of information security in the IRS (see Attachment II). We considered the results of those audits when making our assessment.

The IRS has made steady progress in complying with FISMA requirements since enactment of the FISMA in 2002, and it continues to place a high priority on efforts to improve its security program. During 2007, the IRS Modernization and Information Technology Services organization Cybersecurity office, the Security Program Management Office representatives from each IRS operating unit, and the Modernization and Information Technology Services organization Information Technology Security Council have partnered to improve the IRS'

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 1, 2006, through June 30, 2007. Hereafter, all references to 2007 refer to the FISMA evaluation period.

compliance with the FISMA. Efforts continued this year to develop an enterprise-wide approach to help employees understand their responsibilities for securing IRS systems and data. A working group³, with participation from all of 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 Treasury Inspector General for Tax Administration and the Department of the Treasury Acting Chief Information Officer to 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 20 IRS information systems to:

- Determine whether the systems are certified and accredited and to evaluate the quality of the certification and accreditation process, including annual testing of security controls.
- Determine whether security controls had been tested within the last year and to evaluate the quality of the annual testing.
- Evaluate the quality of the Plan of Action and Milestones (POA&M) process.
- Determine whether Information Technology Contingency Plans had been adequately tested within the last year.

We conducted separate tests to evaluate processes for configuration management, incident reporting, awareness training, and ensuring the privacy of sensitive information.

Our evaluation of the IRS' 2007 performance against specific OMB security measures and our audit work performed during the 2007 evaluation period show that the IRS still needs to do more to adequately secure its systems and data. The most significant areas of concern are annual testing of security controls and contingency plans, implementation of configuration management standards, and privacy requirements for protecting personally identifiable information.

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

Certification and Accreditation The quality of the certification and accreditation process is satisfactory; however, not all systems are currently certified and accredited.

The OMB guidelines for minimum security controls in Federal Government information systems require that all systems be certified and accredited every 3 years or when major system changes occur. The NIST provides guidelines for conducting the certifications and accreditations.

³ IRS Security Program Management Office Council.

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.

In 2006, we reported that the IRS had implemented a satisfactory certification and accreditation process. Because of budget constraints, the IRS planned to implement its process over 3 years. For 2007, the IRS continued to apply this process and is on track to meet its goal by the end of the 2008 FISMA reporting period.

We evaluated the quality of the certification and accreditation process for all 5 of the systems in our sample of 20 that were certified and accredited during the 2007 FISMA reporting period. We determined that all five systems were properly certified, and all but one were accredited in accordance with NIST guidelines.

The certification documentation for each system included a:

- System Security Plan that documented an appropriate set of security controls.
- Security Test and Evaluation of all applicable controls using appropriate assessment procedures to determine whether the controls were implemented and operating as intended.
- Security Assessment Report to inform the system owner of the remaining security weaknesses and risks.
- POA&M for tracking the identified security control weaknesses.

However, the NIST Guidelines for the Security Certification and Accreditation of Federal Information Systems (Special Publication 800-37) state 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. OMB guidelines state that continuous monitoring of security controls is required as part of the certification and accreditation process to ensure controls remain effective over time. The IRS did not make sufficient progress this year in properly implementing annual testing of security controls as part of its continuous monitoring efforts. Accordingly, we could rate the certification and accreditation process no higher than satisfactory.

The OMB also requires the Inspector General to report on the number of systems certified and accredited in our sample. We are reporting that 15 (75 percent) of the 20 systems in our sample were certified and accredited. One system was certified in May 2007 but was not accredited by June 30, 2007, the end of the FISMA reporting period. The other four systems were certified prior to 2006 before the IRS changed its process. These systems were certified and accredited based solely on their underlying general support systems, which does not meet the OMB requirements.

In prior years, when making our assessment of the number of systems certified and accredited, we considered any system with an authorization to operate to be certified and accredited regardless of the quality of the process. This year, to be consistent with the Department of the Treasury Inspector General methodology, we considered the number of systems with satisfactory certifications and accreditations in making our assessment. Because we changed our methodology in addressing this issue, the percentage of systems with certifications and accreditations appears to have dropped from 100 percent in the 2006 FISMA reporting period, when in fact the number of satisfactory certifications and accreditations has steadily increased since 2006.

Annual Testing of Security Controls As previously stated, the IRS did not make sufficient progress in implementing annual testing of security controls. The NIST requires system owners to select and test an appropriate and applicable set of security controls every year throughout the system life cycle but not necessarily to the same extent required for a certification. NIST and Department of the Treasury guidelines state that, for selecting a subset of controls for annual testing, the first priority should be controls for which a weakness was corrected and closed off of a POA&M. The second priority should be the selection of highly volatile controls, the effectiveness of which is most likely to change over time.

The IRS met annual testing requirements on only 5 (25 percent) of the 20 systems we reviewed. We consider these systems as having met the requirement because they were tested during the certification process. For those systems that were not certified during the year, annual testing was conducted; however, the testing was not in compliance with NIST guidelines.

For the 15 systems that did not meet the annual testing requirements, the following weaknesses in the annual testing of controls demonstrate a lack of understanding by the system owners of the purpose of the requirements:

- The system owners requested the assistance of the Cybersecurity office to help them meet their annual testing requirements. In response, the Cybersecurity office provided a standard list of controls to test for each system, based on the risk categorization of the system. Specifically, 13 high-volatility controls were preselected and required to be reviewed for moderate-impact systems, and 8 high-volatility controls were selected for the review of low-impact systems. This process is not consistent with NIST guidelines, and Department of the Treasury guidance that states system owners must select an appropriate set of controls to be tested for their systems. Many of the controls required by the Cybersecurity office were not applicable to the 15 systems; nonetheless, the system owners included them in their continuous monitoring plans and then stated in the testing documentation that they were not applicable. Controls that are not applicable to the system do not require testing and should not be included in the continuous monitoring plans.
- The requirement to include closed POA&M weaknesses in the continuous monitoring plan was not appropriately addressed by system owners. The purpose of this requirement is to verify whether the weaknesses were adequately addressed before being closed off the POA&M as completed. The continuous monitoring plans for 3 of the 15 systems included the selection of closed POA&M weaknesses for testing. However, system owners for two of the three systems included closed POA&M weaknesses that were not applicable to the system and required no testing. The continuous monitoring plan for one of the three systems included security certification and security accreditation, which had been closed off the system POA&M; however, these controls do not require testing to verify whether they are operating as intended and should not have been included in the continuous monitoring plan.
- The continuous monitoring plans for 5 of the 15 systems included controls selected by the system owners that were in addition to those required by the Cybersecurity office and any closed POA&M control weaknesses. However, some of the controls

selected were not appropriate for inclusion in a continuous monitoring plan. For example, organizational common controls were selected for one system. Common controls are not the responsibility of the system owner; therefore, these should not be included in a continuous monitoring plan. Other controls selected were known security weaknesses that had been identified when the system was certified in May 2006.

- Controls that were appropriately included in the continuous monitoring plans were not always sufficiently tested to support the “passing” test results or to identify potential security control weaknesses. For example, we identified controls with passing results; however, the assessments of the controls were based on the controls being included in the Internal Revenue Manual or in the System Security Plan rather than testing of the controls to determine whether they were operating as intended.

While system owners have documented that all 15 systems were tested and evaluated this year, the selection of the controls to be tested and the quality of the testing were insufficient to (1) apprise the system owners of the status of security controls in their systems and (2) identify controls that may not be operating as intended to protect the systems and data.

Information Technology Contingency Plan Testing The IRS made progress in 2007 in meeting the Federal Government requirement for annual testing of contingency plans. However, additional efforts are needed. The OMB requires that all information technology contingency plans be tested at least annually. The NIST requires that key aspects of contingency plans be tested for systems with moderate- and high-impact levels for the availability control objective. Guidance in the IRS FISMA Handbook states that tabletop⁵ testing can be done for low-impact systems. Department of the Treasury guidance states that tabletop testing alone is not sufficient for testing the contingency plans of moderate- and high-impact systems; functional⁶ testing is also required. The guidance states that testing of the backup process is an example of a functional test.

Based on the above guidelines and requirements, we determined contingency plans for 14 (70 percent) of the 20 IRS systems we reviewed were properly tested. The contingency plan for one of the other six systems was not tested at all. Contingency plans for two systems were evaluated inadequately because they were tested using only a tabletop exercise. In addition, contingency plans for three systems were improperly tested because the functional testing of the backup process was incomplete. Department of the Treasury guidance describes backup process testing as a multistep test beginning with confirming that backup tapes are made. To fully test the process, bureaus must also verify whether the backup tape data are valid and retrievable. The IRS performed only the first step of the backup test process for these three systems.

Security Configuration Policies The primary security goal of configuration management is ensuring changes to the system do not unintentionally or unknowingly diminish security. The OMB requires agencies to have configuration guides in place to ensure the consistent

⁵ Participants in tabletop exercises walk through the contingency plan procedures to ensure the documentation reflects the ability to adequately perform the tasks outlined without any recovery operations actually occurring. A tabletop exercise is also known as a classroom exercise.

⁶ A functional exercise is more extensive than a tabletop exercise and includes the simulation of an emergency.

implementation of software across the agency. The IRS has an agency-wide security configuration policy but needs to do more to ensure information systems apply common security configurations established by the NIST.

The IRS provided test results that demonstrated an overall rate of 71 percent to 80 percent for implementing security configurations on all of the types of software it uses for which security configurations are provided by the NIST. For the individual types of software, the implementation rates range from a high of 99 percent to a low of 12 percent.

In 2007, we evaluated configuration management controls for database software used by the IRS⁷. We found that standard database security configurations were not adequately implemented because the configurations were poorly communicated, security roles and responsibilities were not assigned or carried out, and tests to detect noncompliance with standard configurations were inadequate. Improperly configured database software could make the IRS network vulnerable to disruptions of service and theft of sensitive information by hackers, employees, and contractors.

Awareness Training The IRS provided security awareness training to over 98 percent of its employees. We also found that awareness training had been provided to more than 92 percent of its contractor staff, a significant improvement over last year when only 43 percent of contractor staff was trained. Awareness training is critical to ensuring employees understand how to properly use and protect the information technology resources entrusted to them. However, the IRS needs to improve employees' awareness of techniques hackers could use to persuade them to reveal their user names and passwords.

During the evaluation period, we conducted an audit to evaluate the susceptibility of IRS employees to social engineering⁸ attempts that could be used by hackers to gain access to IRS systems.⁹ We found the IRS needs to enhance its security awareness program to increase employees' awareness of social engineering techniques and the importance of protecting their usernames and passwords. In a March 2007 audit test, posing as help desk employees, we were able to convince 60 percent of 102 employees tested to provide us with their usernames and to temporarily change their passwords to ones we suggested.

Privacy Requirements During the past year, the IRS continued to take actions to conduct evaluations for all systems and applications that collect personal information. We determined a Privacy Impact Assessment¹⁰ was prepared for all systems in our representative sample of 20 systems. The Office of Privacy has standard operating procedures and has submitted revised guidelines for processing Privacy Impact Assessments.

⁷ See Attachment II, Report 11.

⁸ A method used to circumvent existing computer security controls by exploiting the human element to obtain sensitive information that can be used to access computer resources and data.

⁹ See Attachment II, Report 9.

¹⁰ This is an analysis of how personal information is collected, stored, shared, and managed in a Federal Government system. Specifically, a privacy impact assessment (1) ensures handling conforms to applicable legal, regulatory, and policy requirements on privacy; (2) determines the risks and effect of collecting, maintaining, and disseminating personal information; and (3) examines and evaluates protection and alternative processes for handling personal data to reduce potential privacy risks.

However, in 2007, we assessed the IRS' privacy requirements as poor due to the lack of compliance with security policies and procedures. We issued a report in 2007 summarizing the results of reviews we conducted from 2003 to 2007 that address the security of personally identifiable information¹¹. The report concludes that persistent computer security weaknesses continue to jeopardize the security of personally identifiable information, primarily because employees and managers are not held accountable for implementing and complying with applicable IRS policies and procedures.

Specifically, we reported that:

- Employees did not sufficiently safeguard laptop computers and did not encrypt data on the computers.
- Employees were susceptible to social engineering techniques that hackers could use to gain access to their systems.
- Employees continued to ignore IRS policies on the appropriate use of email, which increases potential security vulnerabilities.
- Employees with key security responsibilities continued to ignore standard security configurations for their own convenience and were not held accountable for complying with procedures.
- Managers did not consistently review audit trails to identify unauthorized accesses to taxpayer accounts.
- Managers provided employees access to systems and data they do not need for their job responsibilities. In many cases, managers were not aware of the access capabilities of their employees.
- The IRS and its contractors were not integrating security controls into modernized computer systems.

¹¹ See Attachment II, Report 10.

Details of the TIGTA Federal Information Security Management

Section C - Inspector General: Questions 1 and 2

Agency Name: Department of the Treasury - Internal Revenue Service

Submission date: August 31, 2007

Question 1: FISMA Systems Inventory

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

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

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

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

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

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

Bureau Name	FIPS 199 System Impact Level	Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems (Agency and Contractor systems)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
		Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
IRS	High	4	0	0	0	4	0						
	Moderate	179	15	6	3	185	18	15	83%	5	28%	12	67%
	Low	71	2	0	0	71	2	0	0%	0	0%	2	100%
	Not Categorized	0	0	0	0	0	0						
	Sub-total	254	17	6	3	260	20	15	75%	5	25%	14	70%

Comments: **Question 2.a.** - In prior years when making our assessment of the number of systems certified and accredited, we considered any system with an authorization to operate to be certified and accredited regardless of the quality of the process. This year, to be consistent with the Department of the Treasury Inspector General methodology, we considered the number of systems with satisfactory certifications and accreditations in making our assessment. Because we changed our methodology in addressing this issue, the percentage of systems with certifications and accreditations appears to have dropped from 100 percent for the FISMA 2006 reporting cycle, when in fact the number of satisfactory certifications and accreditations has steadily increased since 2006. Five systems are not considered to be certified and accredited. Four of the five systems reviewed were not certified following NIST guidelines and were not counted as certified and accredited. The IRS is on track to have these systems certified and accredited for the next FISMA reporting cycle. One of the five systems did not have a current accreditation.

Question 2.b. - The IRS met annual testing requirements on only 5 (25 percent) of the 20 systems we reviewed. We consider these systems as having met the requirement because they were tested during the certification process. For those systems that were not certified during the year, annual testing was conducted; however, the testing was not in compliance with NIST guidelines. See Question 5, Quality of the Certification and Accreditation process for further details. Question 2.c.-14 of 20 contingency plans were tested in accordance with NIST and OMB guidelines. Six contingency plans were not properly tested. All 6 were moderate impact for the availability control objective. One of the six was not tested at all, 2 of the 6 were tested using a tabletop exercise only, and 3 of the 6 included an insufficient functional exercise to test the backup process.

Section C - Inspector General: Questions 4 and 5

Agency Name: Internal Revenue Service

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

Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.

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

Response Categories:

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

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

POA&M process comments:

Question 5: IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate.

Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.

5.a.	<p>The IG rates the overall quality of the Agency's certification and accreditation process as:</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - Excellent - Good - Satisfactory - Poor - Failing 	Satisfactory																
5.b.	<p>The IG's quality rating included or considered the following aspects of the C&A process: (check all that apply)</p>	<table border="1" style="width: 100%;"> <tr> <td style="width: 80%;">Security plan</td> <td style="width: 20%; text-align: center;">X</td> </tr> <tr> <td>System impact level</td> <td style="text-align: center;">X</td> </tr> <tr> <td>System test and evaluation</td> <td style="text-align: center;">X</td> </tr> <tr> <td>Security control testing</td> <td style="text-align: center;">X</td> </tr> <tr> <td>Incident handling</td> <td></td> </tr> <tr> <td>Security awareness training</td> <td></td> </tr> <tr> <td>Configurations/patching</td> <td></td> </tr> <tr> <td>Other:</td> <td></td> </tr> </table>	Security plan	X	System impact level	X	System test and evaluation	X	Security control testing	X	Incident handling		Security awareness training		Configurations/patching		Other:	
Security plan	X																	
System impact level	X																	
System test and evaluation	X																	
Security control testing	X																	
Incident handling																		
Security awareness training																		
Configurations/patching																		
Other:																		

C&A process comments: We reviewed the certification and accreditation documentation for five systems certified and accredited during the 2007 FISMA cycle. The certifications and accreditations were in compliance with NIST guidelines. We also reviewed the annual security controls testing as part of continuous monitoring that was conducted during the 2007 FISMA cycle for 15 systems. Because continuous monitoring is part of the certification and accreditation process, we included the quality of the annual testing into the overall evaluation of the certification and accreditation process. The annual testing was not in compliance with NIST guidelines. The Cybersecurity office provided system owners with a standard list of controls to test for each system. This process is not consistent with NIST guidelines, or Department of the Treasury guidance that state system owners must select an appropriate set of controls to be tested for their systems. Many of the controls required by the Cybersecurity office were not applicable to the 15 systems. As a result, the Continuous Monitoring Plans for all 15 systems included controls that were not applicable to the systems. Continuous Monitoring Plans for 5 of the 15 systems

Section C - Inspector General: Questions 6 and 7

Agency Name: Internal Revenue Service

Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process

<p>6.a. Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D II.4 (SAOP reporting template), including adherence to existing policy, guidance, and standards.</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing <p>Comments: All 20 of the sample systems reviewed have a PIA. All were timely processed. The Office of Privacy (OP) has updated their standard operating procedures for processing PIA's, has submitted revised Internal Revenue Management guidelines for processing PIA's, and has updated and distributed literature on the PIA process.</p>	Satisfactory
---	--------------

<p>6.b. Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15, "Safeguarding Personally Identifiable Information" since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect personally identifiable information (PII).</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - Response Categories: - Excellent - Good - Satisfactory - Poor <p>Comments: During the past year, the IRS continued to take actions to conduct evaluations for all systems and applications that collect personal information. We determined a Privacy Impact Assessment was prepared for all systems in our representative sample of 20 systems. The Office of Privacy has standard operating procedures and has submitted revised guidelines for processing Privacy Impact Assessments. However, in 2007, we assessed the IRS' privacy requirements as poor due to the lack of compliance with security policies and procedures. We issued a report in 2007 summarizing the results of reviews we have conducted from 2003 to 2007 that address the security of personally identifiable information. The report concludes that persistent computer security weaknesses continue to jeopardize the security of personally identifiable information, primarily because employees and managers are not held accountable for implementing and complying with applicable IRS policies and procedures. Specifically:</p> <ul style="list-style-type: none"> • Employees did not sufficiently safeguard laptop computers and did not encrypt data on the computers. • Employees were susceptible to social engineering techniques that hackers could use to gain access to their systems. • Employees continue to ignore IRS policies on the appropriate use of email which increases potential security vulnerabilities. • Employees with key security responsibilities continue to ignore standard security configurations for their own convenience and were not held accountable for complying with procedures. • Managers do not consistently review audit trails to identify unauthorized access to taxpayer accounts. • Managers provide employees access to systems and data they do not need for their job responsibilities. In many cases, managers were not aware of the access capabilities of their employees. • The IRS and its contractors were not integrating security controls into modernized computer systems. 	Poor
---	------

Question 7: Configuration Management

<p>7.a. Is there an agency-wide security configuration policy? Yes or No.</p> <p>Comments:</p>	Yes
<p>7.b. Approximate the extent to which applicable information systems apply common security configurations established by NIST.</p> <p>Response categories:</p> <ul style="list-style-type: none"> - 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 	Frequently (71-80% of the time)

Section C - Inspector General: Questions 8, 9, 10 and 11

Agency Name: Internal Revenue Service

Question 8: Incident Reporting

<p>Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.</p>	
8.a. The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
8.b. The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)	Yes
8.c. The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.	Yes
Comments:	

Question 9: Security Awareness Training

<p>Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities?</p> <p>Response Categories:</p> <ul style="list-style-type: none"> - Rarely- or approximately 0-50% of employees - Sometimes- or approximately 51-70% of employees - Frequently- or approximately 71-80% of employees - Mostly- or approximately 81-95% of employees - Almost Always- or approximately 96-100% of employees 	Almost Always (96-100% of employees)
---	--------------------------------------

Question 10: Peer-to-Peer File Sharing

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
--	-----

Question 11: E-Authentication Risk Assessments

The agency has completed system e-authentication risk assessments. Yes or No.	Yes
---	-----

*Treasury Inspector General for Tax Administration
Information Technology Security Reports Issued
During the 2007 Evaluation Period*

1. *Business Cases for Information Technology Projects Remain Inaccurate* (Reference Number 2007-20-024, dated January 25, 2007).
2. *The Internal Revenue Service Adequately Protected Sensitive Data and Restored Computer Operations After the Flooding of Its Headquarters Building* (Reference Number 2007-20-023, dated January 26, 2007).
3. *The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices* (Reference Number 2007-20-048, dated March 23, 2007).
4. *The Background Investigation Process Needs Improvements to Ensure Investigations Are Completed Timely and Efficiently* (Reference Number 2007-20-059, dated March 28, 2007).
5. *Sensitive Data Remain at Risk From the Use of Unauthorized Wireless Technology* (Reference Number 2007-20-060, dated March 28, 2007).
6. *Sufficient Emphasis Was Not Placed on Resolving Security Vulnerabilities When Restoring the Electronic Fraud Detection System* (Reference Number 2007-20-108, dated June 14, 2007).
7. *Progress Has Been Slow in Meeting Homeland Security Presidential Directive-12 Requirements* (Reference Number 2007-20-110, dated June 20, 2007).
8. *Network Devices Are Running Unnecessary Communication Services Which Could Expose Sensitive Data to Unauthorized Individuals* (Reference Number 2007-20-104, dated July 9, 2007).
9. *Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers* (Reference Number 2007-20-107, dated July 20, 2007).
10. *Efforts Have Been Made, but Manager and Employee Noncompliance With Security Policies and Procedures Puts Personally Identifiable Information at Risk* (Reference Number 2007-20-117, dated August 13, 2007).
11. *Standard Database Security Configurations Are Adequate, Although Much Work Is Needed to Ensure Proper Implementation* (Reference Number 2007-20-129, dated August 22, 2007).
12. *Insufficient Attention Has Been Given to Ensure States Protect Taxpayer Information* (Reference Number 2007-20-134, dated August 31, 2007).