Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2009

October 27, 2009

Reference Number: 2010-20-004

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.

Phone Number | 202-622-6500
Email Address | inquiries@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 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 information 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 2009 FISMA report. The report was forwarded to the Treasury Inspector General for consolidation into a report issued to the Department of the Treasury Chief Information Officer.

[1] 44 U.S.C. §§ 3541 - 3549.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

October 27, 2009

MEMORANDUM FOR ASSISTANT 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 2009 (Audit # 200920010)

We are pleased to submit the Treasury Inspector General for Tax Administration's Federal Information Security Management Act (FISMA)[1] report for Fiscal Year 2009. The FISMA requires the Office of Inspector General to perform an annual independent evaluation of information security policies, procedures, and practices as well as evaluate compliance with FISMA requirements. This report reflects our independent evaluation of the Internal Revenue Service's (IRS) information technology security program for the period under review.

We based our evaluation on the Office of Management and Budget (OMB) FISMA 2009 Reporting Guidelines. During the 2009 evaluation period,[2] we conducted eight audits, as shown in Attachment I, to evaluate the adequacy of information security in the IRS. We considered the results of these audits in our evaluation. In addition, we evaluated a representative sample of 12 major IRS information systems for our FISMA work. For each system in the sample, we assessed the quality of the certification and accreditation process, the annual testing of controls for continuous monitoring, the testing of information technology contingency plans, and the quality of the Plan of Action and Milestones process. We also conducted tests to evaluate processes over inventory accuracy, configuration management, incident reporting, security awareness and specialized security training, and the information privacy program.

---

[1] 44 U.S.C. §§ 3541 - 3549.
[2] The FISMA evaluation period for the Department of the Treasury is July 1, 2008, through June 30, 2009. All subsequent references to 2009 refer to the FISMA evaluation period.

Included in Attachment II are our responses to the OMB Fiscal Year 2009 FISMA questions for the Inspector General. Major contributors to this report are listed in Attachment III.

We are confident that the IRS has:

- Established a materially correct inventory.
- Implemented a certification and accreditation process that follows the National Institute for Standards and Technology (NIST) framework.
- Sufficiently tested its information technology contingency plans.
- Implemented an adequate Plan of Action and Milestones process to ensure that security weaknesses are remediated.
- Followed policies and procedures for reporting computer security incidents.
- Provided employees security awareness and specialized security training.
- Implemented adequate policies to protect privacy-related information.

Since the enactment of the FISMA in Calendar Year 2002, overall, the IRS has made steady progress in complying with FISMA requirements. In addition, the IRS continues to place a high priority on efforts to improve its security program. We observed significant improvements in information technology contingency plan testing and additional improvements in annual security controls testing, two security areas we identified as needing improvement in our 2008 FISMA evaluation.[3] However, based on our 2009 evaluation, we believe the IRS still needs to take additional actions in the areas of certification and accreditation and configuration management to better secure its systems and data.

Certification and Accreditation Process 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 system certifications and accreditations. Five of the 12 systems in our sample were certified and accredited in 2009. We evaluated the quality of the certification and accreditation process for these five systems and determined that all of them were properly certified and accredited in accordance with NIST guidelines.

The OMB also requires that system security controls be tested for every system at least annually. In years when a system will not be certified and accredited, a subset of security controls must be tested. The NIST provides guidelines for annual testing of security controls. We reviewed the adequacy of annual testing of security controls for 7 of the 12 systems in our sample that were

[3] *Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2008* (Reference Number 2008-20-173, dated September 10, 2008).

not certified and accredited in 2009. We found that an appropriate subset of management, operational, and technical controls was selected, documented, and approved for each of the seven systems. However, tests of the operational and technical controls for three of the seven systems were not sufficient to determine if the controls were in place and operating as intended. Specifically, 11 (31 percent) of 35 operational controls and 15 (27 percent) of 56 technical controls selected for the 3 systems, collectively, were not adequately tested. The tests were limited to examining certification and accreditation documentation or conducting interviews without examining system evidence. For example, configuration change control is an operational control that ensures changes to the information system are authorized, documented, and controlled. For one of the systems, the IRS evaluated this control by examining the test results from the system's last certification and accreditation in 2007. For another system, the IRS evaluated the control by referring to a description of the control in the system's System Security Plan. In both examples, the IRS did not actually test the control. As a result, these tests were insufficient to determine whether the security controls were operating as intended.

Configuration Management The OMB required Federal Government agencies that use the Windows XP or VISTA operating systems to adopt a standard set of configuration settings by February 1, 2008. These configuration settings are referred to as the Federal Desktop Core Configuration (FDCC). The IRS has made significant progress in implementing FDCC standard settings. As of the end of the 2009 evaluation period, the IRS had implemented or had deviations approved by the Department of the Treasury for 265 (94 percent) of 282 FDCC settings. The IRS continues to test the remaining FDCC configurations and has a plan in place to reach full implementation by February 2010. The IRS has not, however, modified its software contracts to ensure purchased software will operate properly with the FDCC settings. In March 2009, we issued a report[4] in which we identified that 27 of 30 software contracts that we examined did not include the required FDCC contract language. The IRS has not yet developed a policy that would require the inclusion of the FDCC language in contracts for new software products. The IRS responded to the report that it planned to issue an agency-wide policy that will incorporate the FDCC contract language in information technology acquisitions.

Please contact me at (202) 622-6510 if you have questions or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-8510.

---

[4] *Progress Has Been Slow in Implementing Federal Security Configurations on Employee Computers* (Reference Number 2009-20-055, dated March 27, 2009).

Attachment I

Treasury Inspector General for Tax Administration Information Technology Security Reports Issued During the 2009 Evaluation Period

1. *The Office of Research, Analysis, and Statistics Needs to Address Computer Security Weaknesses* (Reference Number 2008-20-176, dated September 17, 2008).
2. *Weaknesses in Business Resumption Plans Could Delay Recovery From a Disaster* (Reference Number 2008-20-178, dated September 17, 2008).
3. *The Internal Revenue Service Deployed Two of Its Most Important Modernized Systems With Known Security Vulnerabilities* (Reference Number 2008-20-163, dated September 24, 2008).
4. *The Internal Revenue Service Deployed the Modernized e-File System With Known Security Vulnerabilities* (Reference Number 2009-20-026, dated December 30, 2008).
5. *Better Emergency Preparedness Planning Could Improve Business Continuity Efforts* (Reference Number 2009-20-038, dated February 13, 2009).
6. *While Controls Have Been Implemented to Address Malware, Continued Attention Is Needed to Address This Growing Threat* (Reference Number 2009-20-045, dated March 10, 2009).
7. *Progress Has Been Slow in Implementing Federal Security Configurations on Employee Computers* (Reference Number 2009-20-055, dated March 27, 2009).
8. *The Homeland Security Presidential Directive 12 Program Office Has Addressed Prior Weaknesses, but Progress Is Slower Than What Has Been Reported* (Reference Number 2009-20-084, dated June 25, 2009).

Attachment II

Treasury Inspector General for Tax Administration Responses to the 2009 Office of Management and Budget Federal Information Security Management Act Inspector General Questions

Question 1: System Inventory
Identify the number of agency and contractor systems by component and Federal Information Processing Standard (FIPS) 199 impact level (low, moderate, high). Please also identify the number of systems that are used by your agency but owned by another Federal agency (i.e., ePayroll, etc.) by component and FIPS 199 impact level.

Internal Revenue Service (IRS)				
FIPS 199 System Impact Level	Agency Systems	Contractor Systems	Total Systems (Agency and Contractor Systems)	Systems Owned by Another Federal Agency
High	4	0	4	*
Moderate	181	6	187	*
Low	44	0	44	*
Total	**229**	**6**	**235**	*

* This information will be provided by the Department of the Treasury for all agency components.

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

FIPS 199 System Impact Level	Systems Reviewed	Number of systems with a current certification and accreditation	% of Total	Systems with security controls tested and reviewed within the past year	% of Total	Systems with contingency plans tested in accordance with policy	% of Total
High	0						
Moderate	12	12	100%	12	100%	12	100%
Low	0						
Total	**12**	**12**	**100%**	**12**	**100%**	**12**	**100%**

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory

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.

Does the agency have policies for oversight of contractors? Yes/No

Yes.

If the answer above is yes, is the policy implemented?

Yes. The response to this question is based on our evaluation of the annual testing of 1 contractor system in the sample of 12 systems reviewed. The Treasury Inspector General for Tax Administration (TIGTA) is currently conducting an audit of the effectiveness of contractor managed systems, the results of which will be reflected in future FISMA evaluation results.

The agency has a materially correct inventory of major information systems (including national security systems) operated by or under the control of such agency. Yes/No

Yes.

Does the agency maintain an inventory of interfaces between the agency systems and all other systems, such as those not operated by or under the control of the agency? Yes/No

Yes.

Does the agency require agreements for interfaces between systems it owns or operates and other systems not operated by or under the control of the agency? Yes/No

Yes.

The IG generally agrees with the CIO on the number of agency-owned systems. Yes/No

Yes.

The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes/No

Yes.

The agency inventory is maintained and updated at least annually. Yes/No

Yes.

If the IG does not indicate that the agency has a materially correct inventory, please identify any known missing major systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the systems as presented in the FY 2009 Exhibit 300 (if known), and indicate if the system is an agency or contractor system.

Not applicable as the TIGTA agrees that the IRS has a materially correct inventory.

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 POA&M process, providing explanatory detail in the area provided.

Has the agency developed and documented an adequate policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts? Yes/No

Yes.

Has the agency fully implemented the policy? Yes/No

Yes.

Is the agency currently managing and operating a POA&M process?

Yes.

Is the agency's POA&M process an agency-wide process, incorporating all known IT security weaknesses, including IG/external audit findings 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? Yes/No

Yes.

Does the POA&M process prioritize IT security weaknesses to help ensure significant IT security weaknesses are corrected in a timely manner and receive appropriate resources? Yes/No

Yes.

When an IT security weakness is identified, do program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)? Yes/No

Yes.

For Systems Reviewed:
a. Are deficiencies tracked and remediated in a timely manner? Yes/No

Yes.

b. Are the remediation plans effective for correcting the security weakness? Yes/No

Yes.

c. Are the estimated dates for remediation reasonable and adhered to? Yes/No

Yes.

Do Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly)? Yes/No

Yes.

Does the Agency CIO centrally track, maintain, and independently review/validate POA&M activities on at least a quarterly basis? Yes/No

Yes.

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. 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 a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Provide explanatory detail in the area provided.

Five of the 12 systems reviewed were certified and accredited during the past year. Security controls were selected and tested for the remaining seven systems as part of the continuous monitoring of security controls.

Has the agency developed and documented an adequate policy for establishing a certification and accreditation process that follows the NIST framework? Yes/No

Yes.

Is the agency currently managing and operating a C&A process in compliance with its policies? Yes/No

Yes.

For systems reviewed, does the C&A process adequately provide: (check all that apply)

- ✓ Appropriate risk categories
- ✓ Adequate risk assessments
- ✓ Selection of appropriate controls
- X Adequate testing of controls
- ✓ Regular monitoring of system risks and the adequacy of controls

Controls were not adequately tested for 3 of the 12 sampled systems reviewed. For each of the three systems, controls were selected and tested during 2009 for continuous monitoring of security. However, tests of the operational and technical controls for the three systems were not sufficient to determine if the controls were in place and operating as intended. Specifically, 11 (31 percent) of 35 operational controls and 15 (27 percent) of 56 technical controls selected for the 3 systems, collectively, were not adequately tested. The tests were limited to examining certification and accreditation documentation or conducting interviews without examining system evidence. For example, configuration change control is an operational control that ensures changes to the information system are authorized, documented, and controlled. For one of the systems, the IRS evaluated this control by examining the test results from the system's last certification and accreditation in 2007. For another system, the IRS evaluated the control by referring to a description of the control in the system's System Security Plan. In both examples, the IRS did not actually test the control.

For systems reviewed, is the Authorizing Official presented with complete and reliable C&A information to facilitate an informed system Authorization to Operate decision based on risks and controls implemented? Yes/No

Yes.

Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process
Provide a qualitative assessment of the agency's process, as discussed in Section D, for protecting privacy-related information, including adherence to existing policy, guidance, and standards. Provide explanatory information in the area provided.

Has the Agency developed and documented adequate policies that comply with OMB guidance in M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information? Yes/No

Yes.

Is the Agency currently managing and operating a privacy program with appropriate controls in compliance with its policies? Yes/No

Yes.

Has the Agency developed and documented an adequate policy for Privacy Impact Assessments? Yes/No/Not Applicable

Yes.

Has the Agency fully implemented the policy and is the Agency currently managing and operating a process for performing adequate privacy impact assessments? Yes/No/Not Applicable

Yes.

Question 7: Configuration Management
Is there an agency-wide security configuration policy? Yes/No

Yes.

What tools, techniques is your agency using for monitoring compliance?

The IRS uses the following tools and techniques for monitoring compliance with configuration policy:

- Windows Policy Checker for Windows XP, Windows NT, Windows 2000 Professional, Windows 2000 Server, and Windows 2003 Server.
- Security Compliance Checker for Windows XP.
- Unix Policy Checker for Unix, Solaris, and HP-UX.
- Mainframe Policy Checker for Mainframes.
- OPNET Doctor for Cisco Router and Switches.
- Checklists for Linux, Oracle, SQL, DB2, and AIX.

Indicate the status of the implementation of FDCC at your agency:
Agency has documented deviations from FDCC standard configuration. Yes/No

Yes.

New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology," is included in all contracts related to common security settings. Yes/No

No. In March 2009, we issued a report[1] in which we identified 27 of 30 contracts for new software products that we reviewed did not include the required FDCC contract language. The IRS has not yet implemented policy that would require the inclusion of the FDCC language in contracts for new software products. The IRS responded to the report that it planned to issue an agency-wide policy that will incorporate the FDCC contract language in information technology acquisitions.

Question 8: Incident Reporting

How often does the agency comply with documented policies and procedures for identifying and reporting incidents internally? Answer will be a percentage range.

90 percent– 100 percent. This percentage rate is based on an August 2009 TIGTA audit report[2] which showed that IRS employees reported 96 percent of all incidents involving the loss of information technology assets to the IRS Computer Security Incident Response Center, whose mission is to be proactive in preventing, detecting, and responding to computer security incidents targeting IRS enterprise information technology assets.

How often does the agency comply with documented policies and procedures for timely reporting of incidents to US CERT? Answer will be a percentage range.

Not applicable. The IRS does not report incidents directly to US-CERT. The IRS reports incidents to the Department of the Treasury. The Department of the Treasury serves as the central point for reporting Treasury bureau incidents to the US-CERT.

How often does the agency comply with documented policy and procedures for reporting to law enforcement? Answer will be a percentage range.

90 percent– 100 percent. This percentage rate is based on an August 2009 TIGTA audit report[3] that showed that the IRS reported 96 percent of all incidents involving the loss of information technology assets to the TIGTA Office of Investigations, the law enforcement agency for the IRS.

---

[1] *Progress Has Been Slow in Implementing Federal Security Configurations on Employee Computers* (Reference Number 2009-20-055, dated March 27, 2009).

[2] *Significant Improvements Have Been Made to Protect Sensitive Data on Laptop Computers and Other Portable Electronic Media Devices* (Reference Number 2009-20-120, dated August 31, 2009).

[3] *Significant Improvements Have Been Made to Protect Sensitive Data on Laptop Computers and Other Portable Electronic Media Devices* (Reference Number 2009-20-120, dated August 31, 2009).

Question 9: Security Awareness Training

Has the agency ensured IT security awareness training of all users with log in privileges, including contractors and those employees with significant IT security responsibilities? Provide explanatory detail in the space provided.

Has the agency developed and documented an adequate policy for identifying all general users, contractors, and system owners/employees who have log in privileges, and provided them with suitable IT security awareness training? Yes/No/Not Applicable

Yes. The IRS identifies all employees and contractors including those with log in privileges as well as those without system access.

Report the following for your agency:

Total number of people with log in privileges to agency systems.

86,535.

Number of people with log in privileges to agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" (October 2003).

107,568 people received information security awareness training. This included individuals with log in privileges as well as those without system access.

Total number of employees with significant information security responsibilities.

5,919.

Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (April 1998).

5,913.

Question 10: Peer-to-Peer File Sharing

Does the agency explain policies regarding the use of peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes/No

Yes.

Attachment III

Major Contributors to This Report

Margaret E. Begg, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Acting Director
Carol Taylor, Audit Manager
Joan Bonomi, Lead Auditor
Richard Borst, Senior Auditor
Myron Gulley, Senior Auditor
Midori Ohno, Senior Auditor
Larry Reimer, Senior Auditor
Kasey Koontz, Auditor
Elton Jewell, Information Technology Specialist
Monique Queen, Information Technology Specialist