



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act (Non-Intelligence National
Security Systems) Report for
Fiscal Year 2009*

September 25, 2009

Reference Number: 2009-20-145

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.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 25, 2009

MEMORANDUM FOR CHIEF INFORMATION OFFICER
DEPARTMENT OF THE TREASURY

Michael R. Phillips

FROM:

Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT:

Final Audit Report – Treasury Inspector General for Tax
Administration – Federal Information Security Management Act
(Non-Intelligence National Security Systems) Report for Fiscal
Year 2009 (Audit # 200920009)

We are pleased to submit the Treasury Inspector General for Tax Administration's Federal Information Security Management Act (FISMA)¹ Non-Intelligence National Security Systems report for Fiscal Year 2009. Appendix I presents our independent evaluation of the status of information technology security for Non-Intelligence National Security Systems at the Internal Revenue Service (IRS) for the period under review.

For Fiscal Year 2009, we based our evaluation on the Office of Management and Budget 2009 Reporting Guidelines. We evaluated the IRS' two Non-Intelligence National Security Systems to determine whether information security policies, procedures, and practices complied with FISMA requirements.

Our evaluation showed that the IRS is adequately securing its Non-Intelligence National Security Systems and data. The IRS also corrected the security weakness we identified during our Fiscal Year 2008 FISMA review.² In that review, we identified one security control area for

¹ 44 U.S.C. §§ 3541 - 3549.

² *Treasury Inspector General for Tax Administration – Federal Information Security Management Act (Non-Intelligence - National Security Systems) Report for Fiscal Year 2008* (Reference 2008-20-179, dated September 26, 2008).

*Treasury Inspector General for Tax Administration –
Federal Information Security Management Act (Non-Intelligence National
Security Systems) Report for Fiscal Year 2009*

management's attention. The FISMA requires that the annual testing of information systems include the selection of a subset of management, operational, and technical controls. While some operational and technical controls were tested, identification and authentication controls were not tested. However, the IRS' Fiscal Year 2009 annual testing has improved and did include an appropriate selection of controls.

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

Appendix I

Evaluation of the Internal Revenue Service's Non-Intelligence National Security Systems

This appendix presents our evaluation of the Internal Revenue Service's (IRS) Non-Intelligence National Security Systems, as required by the Federal Information Security Management Act (FISMA).¹ We based our evaluation on the Office of Management and Budget 2009 Reporting Guidelines. We are not providing responses for agency-wide questions, which will be addressed in the Treasury Inspector General for Tax Administration's (TIGTA) evaluation of the IRS' unclassified systems.

Annual FISMA Reporting Inspector General Questions Non-Intelligence National Security Systems

Question 1: System Inventory

Identify the number of agency and contractor systems by component and 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.

The IRS has two high-impact level Non-Intelligence National Security Systems. The IRS does not use any National Security Systems owned by another Federal agency.

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

For the Total Number of Systems identified 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.

Both of the IRS National Security Systems have a current certification and accreditation. A subset of management, technical, and operational security controls for both systems were tested within the past year. The IRS performed a Business Impact Analysis which determined that neither System requires a contingency plan.

¹ 44 U.S.C. §§ 3541 - 3549.

*Treasury Inspector General for Tax Administration –
Federal Information Security Management Act (Non-Intelligence National
Security Systems) Report for Fiscal Year 2009*

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.

Question 3 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

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

Question 3 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

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

Question 3 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

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

Question 3 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

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

Not applicable because the National Security Systems do not interface with other systems.

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

Not applicable because the National Security Systems do not interface with other systems.

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.

*Treasury Inspector General for Tax Administration –
Federal Information Security Management Act (Non-Intelligence National
Security Systems) Report for Fiscal Year 2009*

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.

[Question 4 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

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

[Question 4 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

Has the Agency fully implemented the policy? Yes/No

[Question 4 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

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

[Question 4 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

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

[Question 4 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

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

[Question 4 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

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

[Question 4 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

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.](#)

*Treasury Inspector General for Tax Administration –
Federal Information Security Management Act (Non-Intelligence National
Security Systems) Report for Fiscal Year 2009*

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

Question 4 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

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

Question 4 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

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.

Annual testing of both IRS National Security Systems was conducted within the past year as part of the certification and accreditation process. TIGTA found that the annual testing was conducted in accordance with Federal guidelines.

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

This part of Question 5 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

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

This part of Question 5 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

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

Appropriate risk categories*

Adequate risk assessments*

- Selection of appropriate controls
- Adequate testing of controls
- Regular monitoring of system risks and the adequacy of controls

* Not applicable because these areas were not part of the annual testing of security controls TIGTA evaluated this FISMA year.

*Treasury Inspector General for Tax Administration –
Federal Information Security Management Act (Non-Intelligence National
Security Systems) Report for Fiscal Year 2009*

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, the Designated Accrediting Authority was provided with the annual testing results.

Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment 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.

Question 6 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

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

Question 6 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

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

Question 6 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

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

Question 6 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

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

Question 6 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

Question 7: Configuration Management

Is there an agency-wide security configuration policy? Yes/No

Question 7 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

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

Question 7 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.

*Treasury Inspector General for Tax Administration –
Federal Information Security Management Act (Non-Intelligence National
Security Systems) Report for Fiscal Year 2009*

Indicate the status of the implementation of FDCC at your agency:

Agency has documented deviations from FDCC standard configuration? Yes/No

[Question 7 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

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.

[Question 7 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

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.

[Question 8 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

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.

[Question 8 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

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

[Question 8 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

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.

[Question 9 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

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 providing them with suitable IT security awareness training? Yes/No/Not Applicable

[Question 9 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

Report the following for your agency:

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

[Question 9 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2009 FISMA evaluation of the IRS' unclassified systems.](#)

*Treasury Inspector General for Tax Administration –
Federal Information Security Management Act (Non-Intelligence National
Security Systems) Report for Fiscal Year 2009*

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).

Question 9 is an agency-wide question that will be addressed in the TIGTA’s Fiscal Year 2009 FISMA evaluation of the IRS’ unclassified systems.

Total number of employees with significant information security responsibilities.

Question 9 is an agency-wide question that will be addressed in the TIGTA’s Fiscal Year 2009 FISMA evaluation of the IRS’ unclassified systems.

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).

Question 9 is an agency-wide question that will be addressed in the TIGTA’s Fiscal Year 2009 FISMA evaluation of the IRS’ unclassified systems.

Question 10: Peer-to-Peer File Sharing

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

Question 10 is an agency-wide question that will be addressed in the TIGTA’s Fiscal Year 2009 FISMA evaluation of the IRS’ unclassified systems.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Acting Assistant Inspector General for Audit (Security and Information Technology Services)

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)

Kent Sagara, Acting Director

Carol Taylor, Audit Manager

Joan Bonomi, Senior Auditor

Louis Lee, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief Technology Officer OS:CTO
Deputy Chief Financial Officer, Department of the Treasury