



*Treasury Inspector General for Tax
Administration's Federal Information
Security Management Act (Non-Intelligence
National Security Systems) Report for Fiscal
Year 2010*

September 9, 2010

Reference Number 2010-20-101

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 9, 2010

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’s Federal Information Security Management Act
(Non-Intelligence National Security Systems) Report for
Fiscal Year 2010 (Audit # 201020011)

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 2010. 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 status of information technology security for Non-Intelligence National Security Systems at the Internal Revenue Service (IRS) for the period under review.

We based our evaluation on the Office of Management and Budget’s Fiscal Year 2010 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. However, we noted one security control area for management’s attention. The FISMA requires that Federal agencies track and monitor known information security weaknesses in Plans of Action and Milestones (POA&M). POA&Ms assist in identifying, assessing, prioritizing, and monitoring the progress of corrective actions for security weaknesses found in systems or programs. However, the IRS did not include the weaknesses identified during the Fiscal Year 2010 annual testing of controls for the IRS National Security Systems in

¹ 44 U.S.C. §§ 3541–3549.



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

POA&Ms for tracking and remediation. Also, previously identified weaknesses that were tracked in the system POA&Ms and subsequently remediated were not timely closed out in the POA&Ms. This POA&M process is particularly important because the IRS decided not to perform a new certification and accreditation in Fiscal Year 2010 and to rely instead on its annual testing to ensure a subset of security controls have been implemented and are working as intended.

Appendix I presents our responses to the Office of Management and Budget's Fiscal Year 2010 FISMA evaluation checklist for Inspectors General. Major contributors to this report are listed in Appendix II.

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.



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

Appendix I

Results of the Treasury Inspector General for Tax Administration's Federal Information Security Management Act Review of the Non-Intelligence National Security Systems

The Office of Management and Budget (OMB) issued the attached checklist for the Inspectors General to assess the level of performance achieved by agencies in the specified program areas during the Fiscal Year 2010 Federal Information Security Management Act (FISMA)¹ period. This appendix presents our evaluation of the Internal Revenue Service's (IRS) two Non-Intelligence National Security Systems, as required by the FISMA. We are not providing responses for items that relate to agency-wide programs because these will be addressed in the Treasury Inspector General for Tax Administration (TIGTA) evaluation of the IRS' unclassified systems.

Section 1: System Inventory

1. Identify the number of Agency and Contractor systems by component and FIPS 199 impact level (low, moderate, high) reviewed.

The IRS has two high-impact level Non-Intelligence National Security Systems. We reviewed these two systems.

2. For the total number of reviewed 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. A current certification and accreditation.

Both systems did not have current certifications and accreditations. Certifications and accreditations for these systems were last completed on May 31 and June 1, 2007, which meant new certifications and accreditations were required during Fiscal Year 2010. However, the IRS made a business decision not to perform certifications and accreditations on both systems due to the anticipated retirement of both systems by December 31, 2010, and the high costs associated with a certification and accreditation. In lieu of certifications and accreditations for Fiscal Year 2010, the IRS performed annual testing of a subset of security

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's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

controls and the Designated Authorities have extended each system's authorization to operate for 6 months. We agree with the actions taken by the IRS as long as the IRS follows through with its intent to retire both systems as indicated.

Please refer to Section 2: Status of Certification and Accreditation Program for further details.

- b. Security controls tested and reviewed within the past year.

Both systems tested a subset of management, technical, and operational security controls within the past year.

- c. A contingency plan tested in accordance with policy.

Both systems did not have contingency plans to test during Fiscal Year 2010. The IRS completed Business Impact Analyses for these systems in April and May 2007, and determined that neither systems required a contingency plan because manual procedures existed to recover or reconstitute the systems and the information processed on the systems were maintained in hard copy at alternate locations. Although the IRS allowed the Management Certification Statements (i.e., signed waivers) supporting these decisions to expire in March 2010 in anticipation of the retirement of both systems, we agree with the IRS' original assessment that contingency plans were not required and, therefore, not tested.

Please refer to Section 10: Status of Contingency Planning Program for further details.

Section 2: Status of Certification and Accreditation Program

1. Check one:

- a. The Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. Documented policies and procedures describing the roles and responsibilities of participants in the certification and accreditation process.
2. Establishment of accreditation boundaries for agency information systems.
3. Categorizes information systems.
4. Applies applicable minimum baseline security controls.
5. Assesses risks and tailors security control baseline for each system.



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

6. Assessment of the management, operational, and technical security controls in the information system.
 7. Risks to Agency operations, assets, or individuals analyzed and documented in the system security plan, risk assessment, or an equivalent document.
 8. The accreditation official is provided (i) the security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective actions; (ii) the plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and (iii) the updated system security plan with the latest copy of the risk assessment.
- b. The Agency has established and is maintaining a certification and accreditation program. However, the Agency needs to make significant improvements as noted below.
 - c. The Agency has not established a certification and accreditation program.
2. If b. checked above, check areas that need significant improvement:
- a. Certification and accreditation policy is not fully developed.
 - b. Certification and accreditation procedures are not fully developed or consistently implemented.
 - c. Information systems are not properly categorized (FIPS 199/SP 800-60).
 - d. Accreditation boundaries for agency information systems are not adequately defined.
 - e. Minimum baseline security controls are not adequately applied to information systems (FIPS 200/SP 800-53).
 - f. Risk assessments are not adequately conducted (SP 800-30).
 - g. Security control baselines are not adequately tailored to individual information systems (SP 800-30).
 - h. Security plans do not adequately identify security requirements (SP 800-18).
 - i. Inadequate process to assess security control effectiveness (SP800-53A).
 - j. Inadequate process to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate (SP 800-37).
 - k. Inadequate process to continuously track changes to information systems that may necessitate reassessment of control effectiveness (SP 800-37).



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

1. Other.
3. Comments:

Certification and accreditation for both IRS National Security Systems was due in Fiscal Year 2010 because the last certification and accreditation was performed in Fiscal Year 2007. However, due to the anticipated retirement of both systems by December 31, 2010, and the high costs associated with a certification and accreditation, the IRS made a business decision not to recertify and reaccredit the systems, but to perform annual testing of a subset of security controls. The IRS has accepted the risk of not completing the certification and accreditation for both systems, and the Designated Approving Authorities have extended each system's Authorization to Operate for 6 months. From a business and risk mitigation perspective, we agree with the actions taken by the IRS as long as the IRS follows through with its intent to retire both systems as indicated.

Section 3: Status of Security Configuration Management

Section 3 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2010 FISMA evaluation of the IRS' unclassified systems.

4. Check one:
 - a. The Agency has established and is maintaining a security configuration management program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:
 1. Documented policies and procedures for configuration management.
 2. Standard baseline configurations.
 3. Scanning for compliance and vulnerabilities with baseline configurations.
 4. FDCC baseline settings fully implemented and/or any deviations from FDCC baseline settings fully documented.
 5. Documented proposed or actual changes to the configuration settings.
 6. Process for the timely and secure installation of software patches.
 - b. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.
 - c. The Agency has not established a security configuration management program.
5. If b. checked above, check areas that need significant improvement:



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

- a. Configuration management policy is not fully developed.
 - b. Configuration management procedures are not fully developed or consistently implemented.
 - c. Software inventory is not complete (NIST 800-53: CM-8).
 - d. Standard baseline configurations are not identified for all software components (NIST 800-53: CM-8).
 - e. Hardware inventory is not complete (NIST 800-53: CM-8).
 - f. Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).
 - g. Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).
 - h. FDCC is not fully implemented (OMB) and/or all deviations are not fully documented.
 - i. Software scanning capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).
 - j. Configuration related vulnerabilities have not been remediated in a timely manner (NIST 800-53: CM-4, CM-6, RA-5, SI-2).
 - k. Patch management process is not fully developed (NIST 800-53: CM-3, SI-2).
 - l. Other.
6. Identify baselines reviewed:
- a. Software Name.
 - b. Software Version.
7. Comments:

Section 4: Status of Incident Response & Reporting Program

Section 4 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2010 FISMA evaluation of the IRS' unclassified systems.

8. Check one:
- a. The Agency has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

1. Documented policies and procedures for responding and reporting to incidents.
 2. Comprehensive analysis, validation, and documentation of incidents.
 3. When applicable, reports to US-CERT within established timeframes.
 4. When applicable, reports to law enforcement within established timeframes.
 5. Responds to and resolves incidents in a timely manner to minimize further damage.
 - b. The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below.
 - c. The Agency has not established an incident response and reporting program.
9. If b. checked above, check areas that need significant improvement:
- a. Incident response and reporting policy is not fully developed.
 - b. Incident response and reporting procedures are not fully developed, sufficiently detailed, or consistently implemented.
 - c. Incidents were not identified in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
 - d. Incidents were not reported to US-CERT as required (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
 - e. Incidents were not reported to law enforcement as required.
 - f. Incidents were not resolved in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
 - g. Incidents were not resolved to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
 - h. There is insufficient incident monitoring and detection coverage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
 - i. Other.
10. Comments:

Section 5: Status of Security Training Program

Section 5 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2010 FISMA evaluation of the IRS' unclassified systems.



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

11. Check one:

- a. The Agency has established and is maintaining a security training program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:
 - 1. Documented policies and procedures for security awareness training.
 - 2. Documented policies and procedures for specialized training for users with significant information security responsibilities.
 - 3. Appropriate training content based on the organization and roles.
 - 4. Identification and tracking of all employees with login privileges that need security awareness training.
 - 5. Identification and tracking of employees without login privileges that require security awareness training.
 - 6. Identification and tracking of all employees with significant information security responsibilities that require specialized training.
- b. The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below.
- c. The Agency has not established a security training program.

12. If b. checked above, check areas that need significant improvement:

- a. Security awareness training policy is not fully developed.
- b. Security awareness training procedures are not fully developed, sufficiently detailed, or consistently implemented.
- c. Specialized security training policy is not fully developed.
- d. Specialized security training procedures are not fully developed or sufficiently detailed (SP 800-50, SP 800-53).
- e. Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).
- f. Identification and tracking of employees with login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).
- g. Identification and tracking of employees without login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

- h. Identification and tracking of employees with significant information security responsibilities is not adequate (SP 800-50, SP 800-53).
- i. Training content for individuals with significant information security responsibilities is not adequate (SP 800-53, SP 800-16).
- j. Less than 90% of employees with login privileges attended security awareness training in the past year.
- k. Less than 90% of employees, contractors, and other users with significant security responsibilities attended specialized security awareness training in the past year.
- l. Other.

13. Comments:

Section 6: Status of Plans of Actions & Milestones (POA&M) Program

14. Check one:

- a. The Agency has established and is maintaining a POA&M program that is generally consistent with NIST's and OMB's FISMA requirements and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:
 - 1. Documented policies and procedures for managing all known IT security weaknesses.
 - 2. Tracks, prioritizes and remediates weaknesses.
 - 3. Ensures remediation plans are effective for correcting weaknesses.
 - 4. Establishes and adheres to reasonable remediation dates.
 - 5. Ensures adequate resources are provided for correcting weaknesses.
 - 6. Program officials and contractors report progress on remediation to the CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly.
- b. The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.
- c. The Agency has not established a POA&M program.

15. If b. checked above, check areas that need significant improvement:

- a. POA&M Policy is not fully developed.



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

- b. POA&M procedures are not fully developed, sufficiently detailed, or consistently implemented.
- √ c. POA&Ms do not include all known security weaknesses (OMB M-04-25).
- d. Remediation actions do not sufficiently address weaknesses (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls).
- e. Initial date of security weaknesses are not tracked (OMB M-04-25).
- f. Security weaknesses are not appropriately prioritized (OMB M-04-25).
- g. Estimated remediation dates are not reasonable (OMB M-04-25).
- h. Initial target remediation dates are frequently missed (OMB M-04-25).
- √ i. POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).
- j. Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 & OMB M-04-25).
- k. Agency CIO does not track and review POA&Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).
- l. Other.

16. Comments:

The IRS did not include the weaknesses that were identified during the annual testing of controls for the IRS National Security Systems in its POA&Ms for tracking and remediation. Also, previously identified weaknesses that had been tracked in the system POA&Ms and subsequently remediated were not timely closed out in the POA&Ms. This POA&M process is particularly important because the IRS decided not to perform a new certification and accreditation in Fiscal Year 2010 and to rely instead on its annual testing to ensure a subset of security controls have been implemented and are working as intended.

Section 7: Status of Remote Access Program

Section 7 is not applicable because both systems are standalone laptops and do not provide remote access.

17. Check one:

- a. The Agency has established and is maintaining a remote access program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.
 2. Protects against unauthorized connections or subversion of authorized connections.
 3. Users are uniquely identified and authenticated for all access.
 4. If applicable, multi-factor authentication is required for remote access.
 5. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.
 6. Requires encrypting sensitive files transmitted across public networks or stored on mobile devices and removable media such as CDs and flash drives.
 7. Remote access sessions are timed-out after a maximum of 30 minutes of inactivity after which re-authentication is required.
- b. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.
- c. The Agency has not established a program for providing secure remote access.
18. If b. checked above, check areas that need significant improvement:
- a. Remote access policy is not fully developed.
 - b. Remote access procedures are not fully developed, sufficiently detailed, or consistently implemented.
 - c. Telecommuting policy is not fully developed (NIST 800-46, Section 5.1).
 - d. Telecommuting procedures are not fully developed or sufficiently detailed (NIST 800-46, Section 5.4).
 - e. Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, Section 5.1).
 - f. Multi-factor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).
 - g. Agency has not identified all remote devices (NIST 800-46, Section 2.1).
 - h. Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46, Section 3.1 and 4.2).
 - i. Agency does not adequately monitor remote devices when connected to the agency's networks remotely (NIST 800-46, Section 3.2).



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

- j. Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).
- k. Remote access rules of behavior are not adequate (NIST 800-53, PL-4).
- l. Remote access user agreements are not adequate (NIST 800-46, Section 5.1, NIST 800-53, PS-6).
- m. Other.

19. Comments:

Section 8: Status of Account and Identity Management Program

20. Check one:

- a. The Agency has established and is maintaining an account and identity management program that is generally consistent with NIST's and OMB's FISMA requirements and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:
 - 1. Documented policies and procedures for account and identity management.
 - 2. Identifies all users, including Federal employees, contractors, and others who access Agency systems.
 - 3. Identifies when special access requirements (e.g., multifactor authentication) are necessary.
 - 4. If multi-factor authentication is in use, it is linked to the Agency's PIV program.
 - 5. Ensures that the users are granted access based on needs and separation of duties principles.
 - 6. Identifies devices that are attached to the network and distinguishes these devices from users.
 - 7. Ensures that accounts are terminated or deactivated once access is no longer required.
- b. The Agency has established and is maintaining an account and identify management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.
- c. The Agency has not established an account and identity management program.

21. If b. checked above, check areas that need significant improvement:



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

- a. Account management policy is not fully developed.
 - b. Account management procedures are not fully developed, sufficiently detailed, or consistently implemented.
 - c. Active Directory is not properly implemented (NIST 800-53, AC-2).
 - d. Other Non-Microsoft account management software is not properly implemented (NIST 800-53, AC-2).
 - e. Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).
 - f. Accounts are not properly issued to new users (NIST 800-53, AC-2).
 - g. Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).
 - h. Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).
 - i. Agency has not adequately planned for implementation of PIV for logical access (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01).
 - j. Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).
 - k. Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).
 - l. Network devices are not properly authenticated (NIST 800-53, IA-3).
 - m. Other
22. Comments:

TIGTA found that the IRS properly managed account and identity controls for the two National Security Systems. The two systems granted access only to authorized users with a business need. Once the business need no longer existed, user accounts were disabled. Default administrative and guest accounts were disabled.

Section 9: Status of Continuous Monitoring Program

23. Check one:

- a. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

1. Documented policies and procedures for continuous monitoring.
 2. Documented strategy and plans for continuous monitoring, such as vulnerability scanning, log monitoring, notification of unauthorized devices, sensitive new accounts, etc.
 3. Ongoing assessments of selected security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.
 4. Provides system authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions.
- b. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.
 - c. The Agency has not established a continuous monitoring program.
24. If b. checked above, check areas that need significant improvement:
- a. Continuous monitoring policy is not fully developed.
 - b. Continuous monitoring procedures are not fully developed, sufficiently detailed, or consistently implemented.
 - c. Strategy or plan has not been fully developed for entity-wide continuous monitoring (NIST 800-37).
 - d. Ongoing assessments of selected security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).
 - e. The following were not provided to the system authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&Ms (NIST 800-53, NIST 800-53A).
 - f. Other.

25. Comments:

TIGTA found that the IRS conducted annual testing of controls in compliance with Federal guidelines. The IRS tested a subset of management, technical, and operational security controls for the two IRS National Security Systems within the past year in accordance with the IRS continuous monitoring program.



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

Section 10: Status of Contingency Planning Program

26. Check one:

- a. The Agency established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:
1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.
 2. The agency has performed an overall Business Impact Assessment.
 3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures.
 4. Testing of system specific contingency plans.
 5. The documented business continuity and disaster recovery plans are ready for implementation.
 6. Development of training, testing, and exercises (TT&E) approaches.
 7. Performance of regular ongoing testing or exercising of continuity/disaster recovery plans to determine effectiveness and to maintain current plans.
- b. The Agency has established and is maintaining an entity-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.
- c. The Agency has not established a business continuity/disaster recovery program.

27. If b. checked above, check areas that need significant improvement:

- a. Contingency planning policy is not fully developed.
- b. Contingency planning procedures are not fully developed, sufficiently detailed, or consistently implemented.
- c. An overall business impact assessment has not been performed (NIST SP 800-34).
- d. Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).
- e. A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34).



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

- f. A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34).
 - g. System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).
 - h. Critical systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53).
 - i. Training, testing, and exercises approaches have not been developed (FCD1, NIST SP 800-34, NIST 800-53).
 - j. Training, testing, and exercises approaches have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).
 - k. Disaster recovery exercises were not successful or revealed significant weaknesses in the contingency planning (NIST SP 800-34).
 - l. After-action plans did not address issues identified during disaster recovery exercises (FCD1, NIST SP 800-34).
 - m. Critical systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).
 - n. Alternate processing sites are subject to same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).
 - o. Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).
 - p. Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).
 - q. Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).
 - r. Other.
28. Comments:

The IRS completed Business Impact Analyses in 2007 which determined that neither of the National Security Systems required a contingency plan; therefore, there were no contingency plans to test. The decisions to not recover or reconstitute these systems were based on the existence of manual procedures and that information processed on the systems was maintained in hard copy format at alternative locations. Although the IRS allowed the Management Certification Statements (i.e., signed waivers) supporting these decisions to expire in March 2010 in anticipation of the retirement of both systems by December 31, 2010, we agree with the IRS' original assessment that contingency plans



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

were not required and, therefore, contingency plan testing is not applicable for these two systems.

Section 11: Status of Agency Program to Oversee Contractor Systems

Section 11 is an agency-wide question that will be addressed in the TIGTA's Fiscal Year 2010 FISMA evaluation of the IRS' unclassified systems.

29. Check one:

- a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:
 1. Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities and that the Agency obtains sufficient assurance that security controls of systems operated by contractors or others on its behalf are effectively implemented and complies with Federal and agency guidelines.
 2. A complete inventory of systems operated on the Agency's behalf by contractors or other entities.
 3. The inventory identifies interfaces between these systems and Agency-operated systems.
 4. The agency requires agreements (MOUs, Interconnect Service Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.
 5. The inventory, including interfaces, is updated at least annually.
 6. Systems that are owned or operated by contractors or entities are subject to and generally meet NIST's and OMB's FISMA requirements.
- b. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. However, the Agency needs to make significant improvements as noted below.
- c. The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities.

30. If b. checked above, check areas that need significant improvement:

- a. Policies to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed.



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

- b. Procedures to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed, sufficiently detailed, or consistently implemented.
- c. The inventory of systems owned or operated by contractors or other entities is not sufficiently complete.
- d. The inventory does not identify interfaces between contractor/entity-operated systems to Agency owned and operated systems.
- e. The inventory of contractor/entity operated systems, including interfaces, is not updated at least annually.
- f. Systems owned or operated by contractors and entities are not subject to NIST's and OMB's FISMA requirements (e.g., certification and accreditation requirements).
- g. Systems owned or operated by contractors and entities do not meet NIST's and OMB's FISMA requirements (e.g., certifications and accreditation requirements).
- h. Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained.
- i. Other.

31. Comments:



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

Appendix II

Major Contributors to This Report

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

Kent Sagara, Director

Jody Kitazono, Audit Manager

Joan Bonomi, Senior Auditor

George Franklin, Senior Auditor

Louis Lee, Senior Auditor



*Treasury Inspector General for Tax Administration's
Federal Information Security Management Act
(Non-Intelligence National Security Systems)
Report for Fiscal Year 2010*

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
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Liaison: Chief Technology Officer OS:CTO