Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2010

November 10, 2010

Reference Number: 2011-20-003

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.

Redaction Legend:
2(f) = Risk Circumvention of Agency Regulation or Statute

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

November 10, 2010

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDIT
OFFICE OF THE INSPECTOR GENERAL
DEPARTMENT OF THE TREASURY

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 2010 (Audit # 201020010)

We are pleased to submit the Treasury Inspector General for Tax Administration's Federal Information Security Management Act (FISMA)[1] report for the Fiscal Year 2010 FISMA evaluation period.[2] The FISMA requires the Office of Inspector General to perform an annual independent evaluation of each Federal agency's information security policies, procedures, and practices, as well as evaluate its 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 of the IRS on the Office of Management and Budget's (OMB) FISMA 2010 Reporting Guidelines. During the 2010 evaluation period, we conducted 10 audits, as shown in Appendix II, 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 10 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 configuration management, incident response and

[1] 44 U.S.C. §§ 3541–3549.
[2] The Fiscal Year 2010 FISMA evaluation period for the Department of the Treasury is July 1, 2009, through June 30, 2010. All subsequent references to 2010 refer to the FISMA evaluation period.

reporting, security training, remote access, account and identity management, and contractor oversight.

Included in Appendix I are our responses to the OMB's 2010 FISMA checklist for the Inspectors General. Major contributors to this report are listed in Appendix III.

Based on our 2010 evaluation, we determined that the IRS's information security program was generally compliant with the FISMA legislation, OMB information security requirements, and related information security standards published by the National Institute of Standards and Technology. We determined that the following program areas met the level of performance specified by the OMB's 2010 FISMA checklist.

- Certification and accreditation program.
- Incident response and reporting program.
- Remote access management.

While the information security program was generally compliant with the FISMA legislation, the program was not fully effective as a result of the conditions identified in the following areas.

- Configuration management.
- Security training.
- Plans of action and milestones.
- Identity and access management.
- Continuous monitoring management.
- Contingency planning.
- Contractor systems/financial audit.

Specific to the financial audit area, the Government Accountability Office (GAO) reported[3] newly identified and unresolved information security control weaknesses in key financial and tax processing systems continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information. Until these control weaknesses are corrected, the IRS remains unnecessarily vulnerable to insider threats related to the unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as the disruption of system operations and services. These conditions were the basis for GAO's determination that the IRS had a material weakness in internal controls over financial reporting related to information security in Fiscal Year 2009.

[3] *INFORMATION SECURITY: IRS Needs to Continue to Address Significant Weaknesses* (GAO-10-355, dated March 2010).

Copies of this report are also being sent to the IRS managers affected by the report results. 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) 622-5894.

Table of Contents

Abbreviations

CIO	Chief Information Officer
FCD1	Federal Continuity Directive 1
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Directive
IRS	Internal Revenue Service
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
TIGTA	Treasury Inspector General for Tax Administration
TT&E	Training, Testing, and Exercises
US-CERT	United States Computer Emergency Response Team

Background

The Internal Revenue Service (IRS) collects and maintains a significant amount of personal and financial information on each taxpayer. The IRS also relies extensively on computerized systems to support its responsibilities in collecting taxes, processing tax returns, and enforcing the Federal tax laws. As custodians of taxpayer information, the IRS has an obligation to protect the confidentiality of this sensitive information against unauthorized access or loss. Otherwise, taxpayers could be exposed to invasion of privacy and financial loss or damage from identity theft or other financial crimes.

The Federal Information Security Management Act (FISMA)[1] was enacted to strengthen the security of information and systems within Federal agencies. As part of this legislation, each Federal Government agency is required to report annually to the Office of Management and Budget (OMB) on the effectiveness of its security programs. In addition, the FISMA requires the Offices of Inspector General to perform an annual independent evaluation of each Federal agency's information security policies and procedures, as well as evaluate its compliance with FISMA requirements. In compliance with the FISMA requirements, the Treasury Inspector General for Tax Administration (TIGTA) performs the annual independent evaluation of the information security program and practices of the IRS.

The OMB provides information security performance measures by which each agency is evaluated for the FISMA review. The OMB uses the information from the agencies and independent evaluations to help assess agency-specific and Federal Governmentwide security performance, develop its annual security report to Congress, and assist in improving and maintaining adequate agency security performance.

Attached is the TIGTA's Fiscal Year 2010 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.

Appendix I

Results of the Treasury Inspector General for Tax Administration's Federal Information Security Management Act Review[1]

The OMB issued a checklist for use by Offices of Inspectors General to assess the level of performance achieved by agencies in the specified program areas during the 2010 FISMA evaluation period. This appendix presents our completed OMB checklist for the IRS.

We determined the level of performance (a, b, or c) that the IRS had achieved for each of the program areas listed. As defined by the OMB, agencies achieve an "a" status for the program area if they have met all the attributes specified by OMB in the "a" section. Agencies achieve a "b" status if they have established the program area, but significant improvements were needed. The OMB listed conditions in the "b" section that, if in need of significant improvement, would prevent agencies from achieving an "a" status. Agencies achieve a "c" status if they have not yet established the program area.

We checked IRS program areas as an "a" status where we determined that the IRS met all the program attributes specified by the OMB. We checked IRS program areas as a "b" status where we determined that one or more conditions listed by the OMB needed significant improvement at the IRS. Due to time and resource constraints, we were not able to test all conditions listed by the OMB in the "b" sections. Therefore, it is possible that more of these conditions exist at the IRS than those we have checked. We did not check any program areas as a "c" status because the IRS has established all program areas listed by the OMB.

For our FISMA work, we evaluated a representative sample of 10 major IRS information systems, which included 9 IRS systems and 1 contractor-managed system. Of these 10 systems, 1 system had a Federal Information Processing Standards (FIPS) 199 impact level of high, and 9 systems were of a moderate impact level. All 10 systems had a current certification and accreditation, had security controls tested within the past year, and had contingency plans tested in accordance with policy.

[1] Due to the nature of the listing that follows, abbreviations are used exactly as presented in the original document reproduced and are not defined therein. Please see the Abbreviations page after the Table of Contents of this report for a listing of abbreviations.

RESPONSES TO FISCAL YEAR 2010 OMB QUESTIONS FOR INSPECTOR GENERALS

S1: Certification and Accreditation

Status of Certification and Accreditation Program [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. 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.
1a. If b. checked above, check areas that need significant improvement:		1a(1) Certification and accreditation policy is not fully developed.
		1a(2) Certification and accreditation procedures are not fully developed, sufficiently detailed, or consistently implemented.
		1a(3) Information systems are not properly categorized (FIPS 199/SP 800-60).
		1a(4) Accreditation boundaries for Agency information systems are not adequately defined.
		1a(5) Minimum baseline security controls are not adequately applied to information systems (FIPS 200/SP 800-53).
		1a(6) Risk assessments are not adequately conducted (SP 800-30).
		1a(7) Security control baselines are not adequately tailored to individual information systems (SP 800-30).

		1a(8) Security plans do not adequately identify security requirements (SP 800-18).
		1a(9) Inadequate process to assess security control effectiveness (SP 800-53A).
		1a(10) Inadequate process to determine risk to Agency operations, Agency assets, or individuals or to authorize information systems to operate (SP 800-37).
		1a(11) Inadequate process to continuously track changes to information systems that may necessitate reassessment of control effectiveness (SP 800-37).
		1a(12) Other.
		Explanation for Other:
Comments:		

S2: Configuration Management

Status of Security Configuration Management Program [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.
2a. If b. checked above, check areas that need significant improvement:		2a(1) Configuration management policy is not fully developed.
	✓	2a(2) Configuration management procedures are not fully developed or consistently implemented.
		2a(3) Software inventory is not complete (NIST 800-53: CM-8).
		2a(4) Standard baseline configurations are not identified for all software components (NIST 800-53: CM-8).
		2a(5) Hardware inventory is not complete (NIST 800-53: CM-8).
		2a(6) Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).
		2a(7) Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).
		2a(8) FDCC is not fully implemented (OMB) and/or all deviations are not fully documented.
		2a(9) Software scanning capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).

	✓	2a(10) Configuration-related vulnerabilities have not been remediated in a timely manner (NIST 800-53: CM-4, CM-6, RA-5, SI-2).
	✓	2a(11) Patch management process is not fully developed (NIST 800-53: CM-3, SI-2).
		2a(12) Other.
		Explanation for Other:

Comments:

2a(2): The IRS has not completed corrective actions to resolve the software configuration management component of the IRS computer security material weakness.[2] Although the IRS has made progress in implementing its configuration management program, the IRS corrective action plan for resolving this material weakness indicates ongoing corrective actions with scheduled completion dates ranging from April to December 2011. Until the IRS has implemented adequate configuration management controls Agencywide, it cannot ensure the security and integrity of system programs, files, and data.

- 1-3-20: Ensure security configuration requirements for all system software are documented in an IRS Internal Revenue Manual. (Planned implementation date of April 2011)
- 1-3-21: Implement and maintain baseline standard configurations on system software platforms and perform scheduled testing. This capability covers translation of Internal Revenue Manuals into standard build procedures and implementation/testing processes. (Planned implementation date of April 2011)
- 1-3-22: Ensure system software is controlled under a documented change control process with procedures for assessment of security impact, notifications to Designated Approving Authorities, and appropriate baseline configuration updates. (Planned implementation date of April 2011)
- 1-3-25: Establish and maintain collection and reporting of metrics to assess progress and track improvements in all component activity implementations over time. Successful operation of the policy, procedures, and plans for component activities for at least 2 consecutive quarters. Quarterly reviews by Cybersecurity and annual FISMA security reviews will revalidate compliance. (Planned implementation date of December 2011)

2a(10): In March 2010, TIGTA reported[3] that the IRS was not timely addressing high- and medium-risk system vulnerabilities that it identified on Automated Collection System servers. The IRS UNIX Policy Checker scans that the IRS ran on the servers from January through May 2009 reported that some high- and medium-risk vulnerabilities remained on the servers for 2 to 5 months before system administrators took corrective actions.

[2] The IRS declared its security program as a material weakness in 1997. The IRS further categorized the material weakness into nine areas relating to computer security: (1) network access controls; (2) key computer applications and system access controls; (3) software configuration; (4) functional business, operating, and program units security roles and responsibilities; (5) segregation of duties between system and security administrators; (6) contingency planning and disaster recovery; (7) monitoring of key networks and systems; (8) security training; and (9) certification and accreditation. An Executive Steering Committee oversees the plan, ensuring that material weakness areas are addressed by all affected organizations, appropriate policy and procedures are implemented, and actions resolve the systemic cause of the material weakness. The IRS has closed four of the material weakness areas: (4) functional business, operating, and program units security roles and responsibilities (5) segregation of duties between system and security administrators; (8) security training; and (9) certification and accreditation. The TIGTA did not concur with the IRS's closure of area (4), functional business, operating, and program units security roles and responsibilities.

[3] *Additional Security Controls Are Needed to Protect the Automated Collection System* (Reference Number 2010-20-028, dated March 30, 2010).

In addition, during the 2010 FISMA evaluation period, the TIGTA concluded fieldwork on an audit to evaluate IRS email servers and found that the IRS is not taking timely actions to correct medium-risk security vulnerabilities identified through monthly scans on its email servers. The Modernization and Information Technology Services organization's Enterprise Operations office uses the Windows Policy Checker to conduct monthly scans of its 70 email servers. The scans conducted from September 2009 through February 2010 determined the servers failed between 73 and 79 medium-risk security checks each month. The number of failed security checks on each server was the same each month. 2a(11): The IRS computer security material weakness relating to configuration management includes unresolved weaknesses in the IRS patch management process. The IRS corrective action plan for resolving the patch management weaknesses indicates the following two corrective actions will be completed in April 2011. • 1-3-23: Ensure system software is patched under a documented process that includes standard procedures and fall-back procedures, ensures patch testing, and ensures the dissemination, installation, and verification of patch installations for all components. (Planned implementation date of April 2011) • 1-3-24: Internal and external monitoring and reporting on secure configuration setting changes and patch levels. "Review" includes comparison to approved changes. "Remediation" includes followup on noncompliant components and testing and implementation of proposed corrections. (Planned implementation date of April 2011)

2b. Identify baselines reviewed:		
2b(1)	Software Name	None.
2b(2)	Software Version	None.

S3: Incident Response and Reporting

Status of Incident Response & Reporting Program [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: 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 time frames. 4. When applicable, reports to law enforcement within established time frames. 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.
3a. If b. checked above, check areas that need significant improvement:		3a(1) Incident response and reporting policy is not fully developed.
		3a(2) Incident response and reporting procedures are not fully developed, sufficiently detailed, or consistently implemented.
		3a(3) Incidents were not identified in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).

		3a(4) Incidents were not reported to US-CERT as required (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
		3a(5) Incidents were not reported to law enforcement as required.
		3a(6) Incidents were not resolved in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
		3a(7) Incidents were not resolved to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
		3a(8) There is insufficient incident monitoring and detection coverage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).
		3a(9) Other.
		Explanation for Other:
Comments:		

S4: Security Training

Status of Security Training Program [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.
4a. If b. checked above, check areas that need significant improvement:		4a(1) Security awareness training policy is not fully developed.
		4a(2) Security awareness training procedures are not fully developed, sufficiently detailed, or consistently implemented.
		4a(3) Specialized security training policy is not fully developed.
		4a(4) Specialized security awareness training procedures are not fully developed or sufficiently detailed (SP 800-50, SP 800-53).
		4a(5) Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).
		4a(6) Identification and tracking of employees with login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).

		4a(7) Identification and tracking of employees without login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).
		4a(8) Identification and tracking of employees with significant security information security responsibilities is not adequate (SP 800-50, SP 800-53).
		4a(9) Training content for individuals with significant information security responsibilities is not adequate (SP 800-53, SP 800-16).
		4a(10) Less than 90 percent of employees with login privileges attended security awareness training in the past year.
		4a(11) Less than 90 percent of employees, contractors, and other users with significant security responsibilities attended specialized security awareness training in the past year.
	✓	4a(12) Other(s). (i): Not all contractors with staff-like access were provided with security awareness training. (ii): Until the IRS improves its identification and tracking of employees and contractors with significant security responsibilities, the percentage of those who completed specialized security training in the past year cannot be verified.
		Explanation for Other(s): (i): In accordance with FISMA requirements, IRS policy requires the Agency to provide security awareness training to inform all IRS employees and contractors of the information security risks associated with their activities and their responsibilities in complying with IRS policies and procedures designed to reduce these risks. However, in June 2010, the GAO reported that the IRS did not provide security awareness training for all IRS contractors, such as janitors and security guards, who are provided unescorted physical access to its facilities containing taxpayer receipts and information.[4] Based on the GAO's finding, the IRS stated it updated its policy as of September 7, 2010, to require all contractors to take security awareness training suitable to their type of access. The IRS also stated that it modified its contractor tracking system to track the completion of the required training modules for each contractor during the Fiscal Year 2011 FISMA evaluation period. (ii): We were unable to definitively determine the percentage of employees and contractors with significant security responsibilities that completed specialized security training in the Fiscal Year 2010 FISMA evaluation period. The IRS reported 6,014 of 6,029 (99.8 percent) employees completed their required hours of specialized security training for the Fiscal Year 2010 FISMA evaluation period. The IRS did not track

[4] *Management Report: Improvements Are Needed in IRS's Internal Controls and Compliance with Laws and Regulations* (GAO-10-565R, dated June 2010).

		contractor completion of specialized security training. In a recent TIGTA review,[5] we reported that the IRS needed to improve processes to identify all IRS employees and contractors performing in security roles requiring specialized training. The IRS had not yet documented in its official policy five security roles that the Department of the Treasury policy states must receive specialized training. As a result, the IRS agreed to update its policy to include all security roles in existence at the IRS and crosswalk these with its current training curriculum. In addition, the IRS stated it has recently modified its contractor tracking system to identify contractors that require specialized training and plans to write policy and associated security clauses to require contractors to comply with these training requirements, to be effective for the Fiscal Year 2012 FISMA evaluation period. Until the IRS completes these actions, we cannot verify the population of IRS employees and contractors that require specialized training or the numbers of those that completed their required training.
Comments:		

S5: POA&M

Status of Plan of Action & Milestones (POA&M) Program [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 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.
5a. If b. checked above, check areas that need significant improvement:		5a(1) POA&M policy is not fully developed.
		5a(2) POA&M procedures are not fully developed, sufficiently detailed, or consistently implemented.
	✓	5a(3) POA&Ms do not include all known security weaknesses (OMB M-04-25).

[5] *More Actions Are Needed to Correct the Security Roles and Responsibilities Portion of the Computer Security Material Weakness* (Reference Number 2010-20-084, dated August 26, 2010).

	5a(4)	Remediation actions do not sufficiently address weaknesses (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls).
	5a(5)	Initial dates of security weaknesses are not tracked (OMB M-04-25).
	5a(6)	Security weaknesses are not appropriately prioritized (OMB M-04-25).
	5a(7)	Estimated remediation dates are not reasonable (OMB M-04-25).
	5a(8)	Initial target remediation dates are frequently missed (OMB M-04-25).
	5a(9)	POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, & OMB M-04-25).
	5a(10)	Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 & OMB M-04-25).
	5a(11)	Agency CIO does not track and review POA&Ms (NIST SP 810-53m, Rev. 3, Control CA-5 & OMB M-04-25).
✓	5a(12)	Other: Security weaknesses were closed in POA&Ms before effective corrective action was taken.
	Explanation for Other:	In August 2009, the TIGTA reported[6] that the IRS had prematurely reported resolution of 6 of 13 security control vulnerabilities in the POA&M for the Customer Accounts Data Engine before effective corrective action was taken. In May 2010, the TIGTA reported[7] that the IRS closed four POA&M weaknesses identified in the Modernized e-File system before effective corrective action was taken. During the 2010 FISMA evaluation period, the IRS took steps to improve its POA&M procedures, including requiring system owners to document sufficient detail regarding how weaknesses were remediated before changing their status to "completed." We reviewed the weaknesses that were closed during the 2010 FISMA cycle for our 10 sample systems and found system owners had documented information to support their corrective actions. However, we did not find information to indicate that required verifications were performed before closing these weaknesses as per IRS policy. The Cybersecurity organization indicated that this verification step may be implemented during the next FISMA cycle, depending on available resources.

Comments:

5a(3): In May 2010, the TIGTA reported[8] that security weaknesses identified by the IRS at seven of the eight contractor facilities we sampled were not maintained in POA&Ms as required by the FISMA. These weaknesses

[6] *Customer Account Data Engine Release 4 Includes Most Planned Capabilities and Security Requirements for Processing Individual Tax Account Information* (Reference Number 2009-20-100, dated August 28, 2009).
[7] *Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement* (Reference Number 2010-20-041, dated May 26, 2010).

included access control, configuration management control, and system integrity control issues. The IRS agreed with our report finding that these security weaknesses should be tracked in POA&Ms.

In addition, during the Fiscal Year 2010 FISMA evaluation period, the TIGTA completed fieldwork on an audit to evaluate IRS email servers and found that medium-risk weaknesses the IRS repeatedly detected on its email servers through monthly scans were not posted to POA&Ms. Monthly scans conducted from September 2009 through February 2010 determined that the servers failed between 73 and 79 medium-risk security checks each month.

S6: Remote Access Management

Status of Remote Access Program [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: 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.
6a. If b. checked above, check areas that need significant improvement:		6a(1) Remote access policy is not fully developed.
		6a(2) Remote access procedures are not fully developed, sufficiently detailed, or consistently implemented.
		6a(3) Telecommuting policy is not fully developed (NIST 800-46 Section 5.1).
		6a(4) Telecommuting procedures are not fully developed or sufficiently detailed (NIST 800-46 Section 5.4).
		6a(5) Agency cannot identify all users who require remote access (NIST 800-46 Section 4.2, Section 5.1).
		6a(6) Multi-factor authentication is not properly deployed (NIST 800-46 Section 2.2, Section 3.3).

[8] *Taxpayer Data Used at Contractor Facilities May Be at Risk for Unauthorized Access or Disclosure* (Reference Number 2010-20-51, dated May 18, 2010).

		6a(7) Agency has not identified all remote devices (NIST 800-46 Section 2.1).
		6a(8) Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46 Section 3.1 and Section 4.2).
		6a(9) Agency does not adequately monitor remote devices when connected to the Agency's networks remotely (NIST 800-46 Section 3.2).
		6a(10) Lost or stolen devices are not disabled and appropriately reported (NIST 800-46 Section 4.3, US-CERT Incident Reporting Guidelines).
		6a(11) Remote access rules of behavior are not adequate (NIST 800-53, PL-4).
		6a(12) Remote access user agreements are not adequate (NIST 800-46 Section 5.1 & NIST 800-53, PS-6).
		6a(13) Other.
		Explanation for Other:

S7: Identity and Access Management

Status of Account and Identity Management Program [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., multi-factor 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 identity 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.
7a. If b. checked above, check areas that need significant improvement:		7a(1) Account management policy is not fully developed.
	✓	7a(2) Account management procedures are not fully developed, sufficiently detailed, or consistently implemented.
		7a(3) Active directory is not properly implemented (NIST 800-53, AC-2).
		7a(4) Other non-Microsoft account management software is not properly implemented (NIST 800-53, AC-2).

	7a(5)	Agency cannot identify all User and Non-User accounts (NIST 800-53, AC-2).
	7a(6)	Accounts are not properly issued to new users (NIST 800-53, AC-2).
✓	7a(7)	Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).
	7a(8)	Agency does not use multi-factor authentication when required (NIST 800-53, IA-2).
	7a(9)	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).
✓	7a(10)	Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).
	7a(11)	Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).
	7a(12)	Network devices are not properly authenticated (NIST 800-53, IA-3).
	7a(13)	Other.
		Explanation for Other:

Comments:

7a(2): The IRS has not completed corrective actions to resolve the component of the IRS computer security material weakness relating to access controls. While the IRS's corrective action plan for this material weakness indicates progress has been made in completing the planned actions, there are still ongoing corrective actions with scheduled completion dates ranging from April to December 2011. These involve ensuring that effective access controls are implemented IRS-wide. Until the IRS completes these corrective actions, it cannot ensure that access to key computer applications and systems is limited to authorized persons for authorized purposes.

- 1-2-20: Develop implementation plan to ensure that corrective actions 1-2-11, 12, 13, 14, 15, and 16[9] can be applied to all organizations, systems, and applications to full levels of effectiveness regarding policies, procedures, implementations, monitoring, and testing. (Planned implementation date of April 2011)
- 1-2-21: Execute implementation plan to ensure that corrective actions 1-2-11, 12, 13, 14, 15, and 16 can be applied to all organizations, systems, and applications to full levels of effectiveness regarding policies, procedures, implementations, monitoring, and testing. (Planned implementation date of April 2011)
- 1-2-22: Establish and maintain collection and reporting of metrics to assess progress and track improvements in all component activity implementations over time. Successful operation of the policy, procedures, and plans for component activities for at least two consecutive quarters. Quarterly review by Cybersecurity and annual FISMA security review will revalidate compliance. (Planned implementation date of December 2011)

7a(7): In July 2009, the TIGTA reported[10] that, in a sample of 7 systems, 53 of 376 contractors had active user accounts but did not have a business need to access these systems. These 53 contractors consisted of contractors whose job duties or access privileges had changed and no longer needed system access, contractors who had

[9] These corrective actions listed relate to account management procedures, including controlling user authorizations and levels of privileges on all systems, applications, databases, and other software. This footnote also applies the corrective action 1-2-21.
[10] *Computer System Access Controls Over Contractors Need to Be Improved* (Reference Number 2009-20-108, dated July 24, 2009).

separated from the contract with the IRS, and contractors who had never logged on to the system or had not logged on to the system within 45 calendar days. We also identified 15 contractors whose system access was not deleted in a timely manner upon separation from the contract with the IRS. The IRS agreed with our report findings. The IRS stated that, effective September 7, 2010, it began tracking information from contractors concerning employee status changes, including separations and changes in duties, to ensure timely account termination when access is no longer required.

In addition, in March 2010, the TIGTA reported[11] that the Registered User Portal, which allows tax professionals to electronically submit and retrieve tax-related information, was not configured to disable and remove users' access accounts in accordance with IRS security policies and procedures. Rather than implement the control to disable inactive accounts after 45 days as required by IRS policy, the IRS set the control to 720 days. In addition, the IRS did not implement a control to remove inactive accounts. Inactive accounts unnecessarily increase the opportunity for malicious individuals to gain access to taxpayer data through an unused account.

7a(10): In July 2009, the TIGTA reported[12] that, from a sample of 7 IRS systems, 12 system development contractors had access and full privileges to the production environment of the system on which they worked, in violation of the IRS policy on separation of duties. Developers with access to the production system could bypass controls and make unapproved and untested changes. In addition, 39 system administration contractors also had database administrator privileges. This lack of separation of duties could jeopardize the integrity of the data and allow unauthorized changes to the data to go undetected. The IRS stated it is now notifying contractors during the on-boarding process of the separation of duties requirement and requiring contractors to identify which one of those duties they will perform, if any.

In addition, in March 2010, the TIGTA reported[13] that 6 of 109 sampled employees' system privileges on the Automated Collection System were not restricted to only those privileges needed to perform assigned duties. Excessive privileges granted included the ability to increase the privileges of other users and to perform management queries to view large amounts of sensitive tax collection data. When users are granted access permissions beyond their assigned responsibilities, the risks of malicious actions and unauthorized disclosure of taxpayer data are increased. In addition, 58 employees had unneeded privileges that allowed them the authority to create, modify, or delete the system audit trails. These actions, taken either accidently or intentionally, could conceal unauthorized activity and compromise the integrity of the audit trail.

[11] *Additional Security Is Needed for Access to the Registered User Portal* (Reference Number 2010-20-027, dated March 31, 2010).
[12] *Computer System Access Controls Over Contractors Need to Be Improved* (Reference Number 2009-20-108, dated July 24, 2009).
[13] *Additional Security Controls Are Needed to Protect the Automated Collection System* (Reference Number 2010-20-028, dated March 30, 2010).

S8: Continuous Monitoring Management

Status of Continuous Monitoring Program [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: 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.
8a. If b. checked above, check areas that need significant improvement:		8a(1) Continuous monitoring policy is not fully developed.
		8a(2) Continuous monitoring procedures are not fully developed or consistently implemented.
		8a(3) Strategy or plan has not been fully developed for entity-wide continuous monitoring (NIST 800-37).
		8a(4) Ongoing assessments of selected security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).
		8a(5) 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).
	✓	8a(6) Other: The IRS has not resolved its computer security material weakness relating to audit logging.
		Explanation for Other: The IRS has not completed corrective actions to resolve the audit logging component of the IRS computer security material weakness. The IRS corrective action plan for resolving the audit logging weakness indicates that there are still ongoing corrective actions with scheduled completion dates ranging from February 2011 to October 2013. Until corrective actions are completed to resolve the audit logging material weakness, the IRS cannot effectively monitor key networks and systems to identify unauthorized activities and inappropriate system configurations.

		During the 2010 FISMA evaluation period, the TIGTA reported that the IRS continues to have problems with audit logging. In March 2010, the TIGTA reported[14] that the IRS does not analyze the audit logs for the Registered User Portal system to detect unlawful or unauthorized activities. Consequently, unauthorized access to taxpayer data could go undetected. In March 2010, the TIGTA reported[15] that the IRS is not capturing all of the required auditable events in Automated Collection System audit trails. The IRS informed us that enabling all required auditing events would negatively affect system performance. In July 2010, the TIGTA reported[16] **********2(f)**********.
Comments:		

S9: Contingency Planning

Status of Contingency Planning Program [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 all 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.

[14] *Additional Security Is Needed for Access to the Registered User Portal* (Reference Number 2010-20-027, dated March 31, 2010).
[15] *Additional Security Controls Are Needed to Protect the Automated Collection System* (Reference Number 2010-20-028, dated March 30, 2010).
[16] *Additional Actions and Resources Are Needed to Resolve the Audit Trail Portion of the Computer Security Material Weakness* (Reference Number 2010-20-082, dated July 28, 2010).

	✓	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.
9a. If b. checked above, check areas that need significant improvement:		9a(1) Contingency planning policy is not fully developed.
		9a(2) Contingency planning procedures are not fully developed or consistently implemented.
		9a(3) An overall business impact assessment has not been performed (NIST SP 800-34).
		9a(4) Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).
		9a(5) A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34).
		9a(6) A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34).
		9a(7) System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(8) Critical systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(9) Training, testing, and exercises approaches have not been developed (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(10) Training, testing, and exercises approaches have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(11) Disaster recovery exercises were not successful (NIST SP 800-34).
		9a(12) After-action plans did not address issues identified during disaster recovery exercises (FCD1, NIST SP 800-34).
		9a(13) Critical systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(14) Alternate processing sites are subject to same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(15) Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(16) Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).
		9a(17) Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).
	✓	9a(18) Other: The IRS has made significant progress, but has not resolved its material weakness relating to disaster recovery controls.
		Explanation for Other: The IRS has not yet fully implemented adequate processes to ensure disaster recovery capabilities are implemented IRS-wide. While the IRS's material weakness corrective action plan indicates progress has been made in mitigating disaster recovery issues, the following disaster recovery corrective actions are still ongoing with scheduled completion dates

		ranging from October 2010 to December 2011. These involve ensuring effective disaster recovery controls are implemented IRS-wide. Until the IRS has completed its corrective actions to resolve this weakness, it cannot ensure critical business systems can be timely restored when unexpected events occur. • 1-6-16 – Disaster Recovery Compliance: Complete internal auditing of the disaster recovery efforts to ensure accuracy and completeness as it relates to day-to-day operations and efforts to mitigate the material weakness. Establish and maintain metrics documentation to assess progress and track improvements in all component activities over time. Conduct an annual evaluation to revalidate compliance. (Planned implementation date of July 2011) • 1-6-17 – Disaster Recovery Plans: Develop and maintain Information Technology contingency plans associated with general support systems to include all components that support critical applications. Establish and maintain data and processing backup-recovery capability. Ensure maximum allowable outage times meet the recovery time objectives of the applications being supported. (Planned implementation date of December 2010) • 1-6-19 – Technical Assessment: Perform annual system risk assessments. Develop a true redundancy/resilience analysis. Based on the critical business processes, develop a site-based restoration vulnerability analysis. Create a Recovery Point Objective and Recovery Time Objective analysis and gain concurrence from both the business operating divisions and the Modernization and Information Technology Services organizations. Incorporate a technical assessment tool that will provide an infrastructure impact analysis in the event of a disaster. Implement backup-recovery capabilities to meet application maximum allowable outages and recovery time objectives of all Information Technology systems supporting the critical business processes. (Planned implementation date of July 2011) • 1-6-20 – Metrics: Establish and maintain metrics to assess progress and track improvements in all component activities over time. Successful operation of the policy, procedures, and plans for component activities for at least two quarters. Annual FISMA testing will revalidate compliance. (Planned implementation date of December 2011)
Comments:		

S10/S11: Contractor Systems/Financial Audit

Status of Agency Program to Oversee Contractor Systems [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 of the Agency obtains sufficient assurance that security controls of systems operated by contractors or others on its behalf are effectively implemented and comply 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.
10a.If (b) checked above, check areas that need significant improvement:		10a(1) Policies to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed.
		10a(2) Procedures to oversee systems operated on the Agency's behalf by contractors or other entities are not fully developed or consistently implemented.
	✓	10a(3) The inventory of systems owned or operated by contractors or other entities is not sufficiently complete.
		10a(4) The inventory does not identify interfaces between contractor/ entity-operated systems to Agency-owned and operated systems.
		10a(5) The inventory of contractor/entity-operated systems, including interfaces, is not updated at least annually.
		10a(6) 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).
		10a(7) Systems owned or operated by contractors and entities do not meet NIST's and OMB's FISMA requirements (e.g., certification and accreditation requirements).
		10a(8) Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained.
		10a(9) Other.
		Explanation for Other:

<table>
<tr><td colspan="2">Comments:

10a(3): The IRS was unable to provide us with a definitive inventory of contractor managed systems and agreed that this inventory required improvement. In May 2010, the TIGTA reported[17] that current processes were not effective at identifying all contractors who receive IRS taxpayer data and therefore are subject to required security reviews. The IRS agreed with our finding and has implemented an automated mechanism to identify all contractors that have access to sensitive data. This information will be available to target sites for security reviews during the Fiscal Year 2012 review cycle. The IRS stated it will also use this information to determine which of these meet the definition of a contractor system. In addition, where contracts may not fall into the definition of a contract system, the IRS is working towards developing new contract language to address security requirements and to potentially provide these contractors with IRS-configured laptops to help enforce security policy.</td></tr>
<tr><td>11. Financial Audit</td><td>11a. For the latest Financial Audit Report issued for the Agency, please provide the date of the report and indicate whether there was a material weakness or reportable condition concerning information security.</td></tr>
<tr><td></td><td>Input for 11a:

In March 2010, the GAO reported[18] newly identified and unresolved information security control weaknesses in key financial and tax processing systems continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information. Until these control weaknesses and program deficiencies are corrected, the IRS remains unnecessarily vulnerable to insider threats related to the unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as the disruption of system operations and services. The new and unresolved weaknesses and deficiencies at the IRS were the basis for the GAO's determination that the IRS had a material weakness in internal controls over financial reporting related to information security in Fiscal Year 2009.</td></tr>
</table>

[17] *Taxpayer Data Used at Contractor Facilities May Be at Risk for Unauthorized Access or Disclosure* (Reference Number 2010-20-051, dated May 18, 2010).
[18] *INFORMATION SECURITY: IRS Needs to Continue to Address Significant Weaknesses* (GAO-10-355, dated March 2010).

Appendix II

Treasury Inspector General for Tax Administration Information Technology Security Reports Issued During the 2010 Evaluation Period

1. *Computer System Access Controls Over Contractors Need to Be Improved* (Reference Number 2009-20-108, dated July 24, 2009).
2. *Customer Account Data Engine Release 4 Includes Most Planned Capabilities and Security Requirements for Processing Individual Tax Account Information* (Reference Number 2009-20-100, dated August 28, 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).
4. *Progress Has Been Made, but Additional Steps Are Needed to Ensure Taxpayer Accounts Are Monitored to Detect Unauthorized Employee Accesses* (Reference Number 2009-20-119, dated September 9, 2009).
5. *While Effective Actions Have Been Taken to Address Previously Reported Weaknesses in the Protection of Federal Tax Information at State Government Agencies, Additional Improvements Are Needed* (Reference Number 2010-20-003, dated November 10, 2009).
6. *Additional Security Controls Are Needed to Protect the Automated Collection System* (Reference Number 2010-20-028, dated March 30, 2010).
7. *Additional Security Is Needed for Access to the Registered User Portal* (Reference Number 2010-20-027, dated March 31, 2010).
8. *Taxpayer Data Used at Contractor Facilities May Be at Risk for Unauthorized Access or Disclosure* (Reference Number 2010-20-051, dated May 18, 2010).
9. *Modernized e-File Will Enhance Processing of Electronically Filed Individual Tax Returns, but System Development and Security Need Improvement* (Reference Number 2010-20-041, dated May 26, 2010).
10. *Implementation of General Support System Security Controls Needs Improvement to Protect Taxpayer Data* (Reference Number 2010-20-063, dated June 7, 2010).

Appendix III

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
Richard Borst, Senior Auditor
Bret Hunter, Senior Auditor
Louis Lee, Senior Auditor
Larry Reimer, Senior Auditor
Frank O'Connor, Auditor
Victor Taylor, Auditor

Appendix IV

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