



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

September 20, 2011

Reference Number: 2011-20-116

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

Phone Number | 202-622-6500

Email Address | TIGTACommunications@tigta.treas.gov

Web Site | <http://www.tigta.gov>



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 20, 2011

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 2011
(Audit # 201120006)

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 2011 evaluation period.² The FISMA requires the Offices of Inspector General to perform an annual independent evaluation of each Federal agency's information security program and practices. This report reflects our independent evaluation of the Internal Revenue Service's (IRS) information security program for the period under review.

We based our evaluation of the IRS on the Department of Homeland Security's (DHS) Fiscal Year 2011 Inspector General FISMA Reporting guidelines, issued June 1, 2011. During the Fiscal Year 2011 FISMA evaluation period, we conducted 14 audits, as shown in Appendix I, to evaluate the adequacy of information security in the IRS. We considered the results of these audits in our evaluation. In addition, we evaluated a representative sample of 10 major IRS information systems for our FISMA work. For each system in the sample, we assessed the quality of the security assessment and authorization 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 reporting, security training, remote access

¹ 44 U.S.C. Sections 3541–3549.

² The FISMA evaluation period for the Department of the Treasury is July 1, 2010, through June 30, 2011. All subsequent references to 2011 refer to the FISMA evaluation period.



*Treasury Inspector General for Tax
Administration - Federal Information Security
Management Act Report for Fiscal Year 2011*

management, identity and access management, contractor systems, and security architecture and capital planning. Major contributors to this report are listed in Appendix II.

Based on our Fiscal Year 2011 FISMA evaluation, we determined that the IRS's information security program is in place and generally compliant with the FISMA legislation, but improvements are needed. We determined that the following program areas met the level of performance specified by the DHS's 2011 FISMA checklist.

- Risk management.
- Incident response and reporting.
- Remote access management.
- Continuous monitoring management.
- Contingency planning.
- Contractor systems.
- Security capital planning.

We determined the following program areas were not fully effective as a result of the conditions identified that need improvement.

- Configuration management.
- Security training.
- Plans of action and milestones.
- Identity and access management.

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.



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

Table of Contents

BackgroundPage 1

Results of ReviewPage 2

Appendices

Appendix I – Treasury Inspector General for Tax Administration
Information Technology Security Reports Issued During the
Fiscal Year 2011 Evaluation PeriodPage 20

Appendix II – Major Contributors to This ReportPage 22

Appendix III – Report Distribution ListPage 23



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

Abbreviations

DHS	Department of Homeland Security
FCD1	Federal Continuity Directive 1
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information System Management Act
GAO	Government Accountability Office
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
TIGTA	Treasury Inspector General for Tax Administration
US-CERT	United States Computer Emergency Response Team
USGCB	United States Government Configuration Baseline



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

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. Under the FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of the FISMA, related Office of Management and Budget (OMB) policies, and National Institute of Standards and Technology (NIST) procedures, standards, and guidelines.

As part of this legislation, each Federal Government agency is required to report annually to the OMB on the adequacy and effectiveness of its information security program and practices and compliance with the FISMA. In addition, the FISMA requires the agencies to have an annual independent evaluation of their information security programs and practices performed by the agency Inspector General or an independent external auditor as determined by the Inspector General. The OMB uses the information from the agencies and independent evaluations in its FISMA oversight capacity to assess agency-specific and Federal Government-wide security performance, develop its annual security report to Congress, and assist in improving and maintaining adequate agency security performance. For the Fiscal Year 2011 FISMA evaluation, the Department of Homeland Security (DHS) issued the information security performance measures by which each agency was evaluated.

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. Attached is the TIGTA's Fiscal Year 2011 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. Sections 3541–3549.



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

Results of Review

The DHS issued a checklist² for use by Offices of Inspectors General to assess the level of performance achieved by agencies in the specified program areas during the Fiscal Year 2011 FISMA evaluation period.³ This report presents our completed DHS 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 DHS, agencies achieve an “a” status for the program area if they have met all the attributes specified by DHS in the “a” section. Agencies achieve a “b” status if they have established the program area, but significant improvements were needed in regards to certain conditions specified by the DHS. The DHS listed the 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 DHS. We checked IRS program areas as a “b” status where we determined that one or more conditions listed by the DHS needed significant improvement at the IRS. Due to time and resource constraints, we were unable to test all conditions listed by the DHS 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 DHS.

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 199 impact level of high, and 9 systems were of a moderate impact level. All 10 systems had a current security assessment and authorization, had security controls tested within the past year, and had contingency plans tested in accordance with policy. Of the 10 IRS systems the TIGTA selected for the Fiscal Year 2011 FISMA evaluation, 4 systems completed the security assessment and authorization process, and 6 systems completed annual testing of selected controls during the Fiscal Year 2011 FISMA evaluation period.

² Due to the nature of the list that follows, many abbreviations are used exactly as presented in the original document reproduced and are not defined therein. However, please see the Abbreviations page after the Table of Contents of this report for a list of abbreviations that we have defined.

³ The FISMA evaluation period for the Department of the Treasury is July 1, 2010, through June 30, 2011. All subsequent references to 2011 refer to the FISMA evaluation period.



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

**RESPONSES TO FISCAL YEAR 2011
DHS QUESTIONS FOR INSPECTOR GENERALS**

1: Risk Management

Status of Risk Management Program [check one]	<input checked="" type="checkbox"/>	<p>1.a. The Agency has established and is maintaining a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the Office of the Inspector General (OIG), the program includes the following attributes:</p> <p>1.a(1). Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.</p> <p>1.a(2). Addresses risk from an <i>organization</i> perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev. 1.</p> <p>1.a(3). Addresses risk from a <i>mission and business process</i> perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev. 1.</p> <p>1.a(4). Addresses risk from an <i>information system</i> perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1.</p> <p>1.a(5). Categorizes information systems in accordance with government policies.</p> <p>1.a(6). Selects an appropriately tailored set of baseline security controls.</p> <p>1.a(7). Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.</p> <p>1.a(8). Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.</p> <p>1.a(9). Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.</p> <p>1.a(10). Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness.</p> <p>1.a(11). Information system specific risks (tactical), mission/business specific risks, and organizational level (strategic) risks are communicated to appropriate levels of the organization.</p> <p>1.a(12). Senior officials are briefed on threat activity on a regular basis by</p>
--	-------------------------------------	---



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

	<p>appropriate personnel. (e.g., Chief Information Security Officer (CISO)).</p> <p>1.a(13). Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.</p> <p>1.a(14). Security authorization package contains system security plan, security assessment report, and Plans of Action and Milestones (POA&M) in accordance with government policies.</p>
	<p>1.b. The Agency has established and is maintaining a risk management program. However, the Agency needs to make significant improvements as noted below.</p>
If 1.b. is checked above, check areas that need significant improvement:	<p>1.b(1). Risk management policy is not fully developed.</p>
	<p>1.b(2). Risk management procedures are not fully developed, sufficiently detailed (SP 800-37, SP 800-39, SP 800-53).</p>
	<p>1.b(3). Risk management procedures are not consistently implemented in accordance with government policies (SP 800-37, SP 800-39, SP 800-53).</p>
	<p>1.b(4). A comprehensive governance structure and Agency-wide risk management strategy has not been fully developed in accordance with government policies (SP 800-37, SP 800-39, SP 800-53).</p>
	<p>1.b(5). Risks from a mission and business process perspective are not addressed (SP 800-37, SP 800-39, SP 800-53).</p>
	<p>1.b(6). Information systems are not properly categorized (FIPS 199/ SP 800-60).</p>
	<p>1.b(7). Appropriately tailored baseline security controls are not applied to information systems in accordance with government policies (FIPS 200/ SP 800-53).</p>
	<p>1.b(8). Risk assessments are not conducted in accordance with government policies (SP 800-30).</p>
	<p>1.b(9). Security control baselines are not appropriately tailored to individual information systems in accordance with government policies (SP 800-53).</p>
	<p>1.b(10). The communication of information system specific risks, mission/business specific risks, and organizational level (strategic) risks to appropriate levels of the organization is not in accordance with government policies.</p>
	<p>1.b(11). The process to assess security control effectiveness is not in accordance with government policies (SP800-53A).</p>
	<p>1.b(12). The process to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate is not in accordance with government policies (SP 800-37).</p>
	<p>1.b(13). The process to continuously monitor changes to information systems that may necessitate reassessment of control effectiveness is not in accordance with government policies (SP 800-37).</p>
	<p>1.b(14). Security plan is not in accordance with government policies (SP 800-18, SP 800-37).</p>
	<p>1.b(15). Security assessment report is not in accordance with government policies (SP 800-53A, SP 800-37).</p>
	<p>1.b(16). Accreditation boundaries for agency information systems are not defined in accordance with government policies.</p>



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

		1.b(17). Other
		1.b(17ex). Explanation for Other
		1.c. The Agency has not established a risk management program.
Comments:		

2: Configuration Management

Status of Configuration Management Program [check one]		<p>2.a. The Agency has established and is maintaining a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p>2.a(1). Documented policies and procedures for configuration management.</p> <p>2.a(2). Standard baseline configurations defined.</p> <p>2.a(3). Assessing for compliance with baseline configurations.</p> <p>2.a(4). Process for timely, as specified in agency policy or standards, remediation of scan result deviations.</p> <p>2.a(5). For Windows-based components, Federal Desktop Core Configuration (FDCC)/United States Government Configuration Baseline (USGCB) secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.</p> <p>2.a(6). Documented proposed or actual changes to hardware and software configurations.</p> <p>2.a(7). Process for timely and secure installation of software patches.</p>
	X	<p>2.b. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.</p>
If 2.b. is checked above, check areas that need significant improvement:		2.b(1). Configuration management policy is not fully developed (NIST 800-53: CM-1)
		2.b(2). Configuration management procedures are not fully developed (NIST 800-53: CM-1).
	X	2.b(3). Configuration management procedures are not consistently implemented (NIST 800-53: CM-1).
		2.b(4). Standard baseline configurations are not identified for software components (NIST 800-53: CM-2).
		2.b(5). Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).
	X	2.b(6). Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).
		2.b(7). FDCC/USGCB is not fully implemented (OMB) and/or all deviations are not fully documented (NIST 800-53: CM-6).
	X	2.b(8). Software assessing (scanning) capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

X	2.b(9). Configuration-related vulnerabilities, including scan findings, have not been remediated in a timely manner, as specified in agency policy or standards (NIST 800-53: CM-4, CM-6, RA-5, SI-2).
X	2.b(10). Patch management process is not fully developed, as specified in agency policy or standards (NIST 800-53: CM-3, SI-2).
	2.b(11). Other
	2.b(11ex). Explanation for Other
	2.c. The Agency has not established a security configuration management program.

Comments: In March 2011, the Government Accountability Office (GAO) reported⁴ that the IRS had newly identified and unresolved weaknesses related to access controls, configuration management, and segregation of duties that continue to jeopardize the confidentiality, integrity, and availability of the financial and sensitive taxpayer information processed by the IRS’s systems. Considered collectively, these weaknesses were the basis for GAO’s determination that the IRS had a material weakness in internal control over its financial reporting related to information security in Fiscal Year 2010. In May 2011, the TIGTA reported⁵ that nonmainframe databases containing taxpayer data were not always configured in a secure manner and were running out-of-date software that no longer received security patches and other vendor support. In addition, the TIGTA reported that the IRS had not fully implemented its plans to complete vulnerability scans of databases within its enterprise. Further, the IRS has been unable to establish an enterprise-wide process for timely remediation of weaknesses reported by vulnerabilities scans because of the limited information it gets from the scan results. To correct configuration management deficiencies, the IRS is in the process of implementing an Enterprise Configuration Management System, with planning dates through Fiscal Year 2014, that will provide oversight and enforcement of configuration and change management processes.

3: Incident Response and Reporting

Status of Incident Response & Reporting Program [check one]	X	<p>3.a. The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p>3.a(1). Documented policies and procedures for detecting, responding to, and reporting incidents.</p> <p>3.a(2). Comprehensive analysis, validation, and documentation of incidents.</p> <p>3.a(3). When applicable, reports to United States Computer Emergency Response Team (US-CERT) within established timeframes.</p> <p>3.a(4). When applicable, reports to law enforcement within established timeframes.</p> <p>3.a(5). Responds to and resolves incidents in a timely manner, as specified in</p>
---	---	--

⁴ *INFORMATION SECURITY: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data* (GAO-11-308, dated March 2011).

⁵ *Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected* (Reference Number 2011-20-044, dated May 4, 2011).



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

		<p>agency policy or standards, to minimize further damage.</p> <p>3.a(6). Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.</p> <p>3.a(7). Is capable of correlating incidents.</p>
		3.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.
If 3.b. is checked above, check areas that need significant improvement:		3.b(1). Incident response and reporting policy is not fully developed (NIST 800-53: IR-1).
		3.b(2). Incident response and reporting procedures are not fully developed or sufficiently detailed (NIST 800-53: IR-1).
		3.b(3). Incident response and reporting procedures are not consistently implemented in accordance with government policies (NIST 800-61, Rev 1).
		3.b(4). Incidents were not identified in a timely manner, as specified in agency policy or standards (NIST 800-53, 800-61 and OMB M-07-16, M-06-19).
		3.b(5). Incidents were not reported to the US-CERT as required (NIST 800-53, 800-61 and OMB M-07-16, M-06-19).
		3.b(6). Incidents were not reported to law enforcement as required (SP 800-86).
		3.b(7). Incidents were not resolved in a timely manner (NIST 800-53, 800-61 and OMB M-07-16, M-06-19).
		3.b(8). Incidents were not resolved to minimize further damage (NIST 800-53, 800-61 and OMB M-07-16, M-06-19).
		3.b(9). There is insufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61 and OMB M-07-16, M-06-19).
		3.b(10). The agency cannot or is not prepared to track and manage incidents in a virtual/cloud environment.
		3.b(11). The agency does not have the technical capability to correlate incident events.
		3.b(12). Other
		3.b(12ex). Explanation for Other
		3.c. The Agency has not established an incident response and reporting program.
Comments:		



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

4: Security Training

Status of Security Training Program [check one]		<p>4.a. The Agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p>4.a(1). Documented policies and procedures for security awareness training.</p> <p>4.a(2). Documented policies and procedures for specialized training for users with significant information security responsibilities.</p> <p>4.a(3). Security training content based on the organization and roles, as specified in agency policy or standards.</p> <p>4.a(4). Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other agency users) with access privileges that require security awareness training.</p> <p>4.a(5). Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other agency users) with significant information security responsibilities that require specialized training.</p>
	X	<p>4.b. The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below.</p>
If 4.b. is checked above, check areas that need significant improvement:		<p>4.b(1). Security awareness training policy is not fully developed (NIST 800-53: AT-1).</p>
		<p>4.b(2). Security awareness training procedures are not fully developed and sufficiently detailed (NIST 800-53: AT-1).</p>
		<p>4.b(3). Security awareness training procedures are not consistently implemented in accordance with government policies (NIST 800-53: AT-2).</p>
		<p>4.b(4). Specialized security training policy is not fully developed (NIST 800-53: AT-3).</p>
		<p>4.b(5). Specialized security training procedures are not fully developed or sufficiently detailed in accordance with government policies (SP 800-50, SP 800-53).</p>
		<p>4.b(6). Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).</p>
		<p>4.b(7). Identification and tracking of the status of security awareness training for personnel (including employees, contractors, and other agency users) with access privileges that require security awareness training is not adequate in accordance with government policies (SP 800-50, SP 800-53).</p>
	X	<p>4.b(8). Identification and tracking of the status of specialized training for personnel (including employees, contractors, and other agency users) with significant information security responsibilities is not adequate in accordance with government policies (SP 800-50, SP 800-53).</p>
		<p>4.b(9). Training content for individuals with significant information security responsibilities is not adequate in accordance with government policies (SP 800-53, SP 800-16).</p>
		<p>4.b(10). Less than 90% of personnel (including employees, contractors, and other agency users) with access privileges completed security awareness</p>



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

		training in the past year.
		4.b(11). Less than 90% of employees, contractors, and other users with significant security responsibilities completed specialized security awareness training in the past year.
		4.b(12). Other
		4.b(12ex). Explanation for Other
		4.c. The Agency has not established a security training program.
<p>Comments: In June 2011, the TIGTA reported⁶ that the IRS was unable to track whether employees with disaster recovery roles attend required annual disaster recovery training. The IRS plans to develop a process for identifying and tracking the completion of training for employees with disaster recovery roles by December 31, 2011. In addition, the IRS did not identify or track contractors that require specialized training for the Fiscal Year 2011 FISMA year, but plans to begin collecting and tracking information on contractor completion of specialized training for the Fiscal Year 2012 FISMA year. Contractors will self identify and report the completion of specialized training where required and provide these data to the IRS.</p>		

5: POA&M

Status of Plan of Action & Milestones (POA&M) Program [check one]		<p>5.a. The Agency has established and is maintaining a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p>5.a(1). Documented policies and procedures for managing information technology security weaknesses discovered during security control assessments and requiring remediation.</p> <p>5.a(2). Tracks, prioritizes, and remediates weaknesses.</p> <p>5.a(3). Ensures remediation plans are effective for correcting weaknesses.</p> <p>5.a(4). Establishes and adheres to milestone remediation dates.</p> <p>5.a(5). Ensures resources are provided for correcting weaknesses.</p> <p>5.a(6). Program officials and contractors report progress on remediation to the Chief Information Officer on a regular basis, at least quarterly, and the Chief Information Officer centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly.</p>
	X	<p>5.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.</p>
If 5.b. is checked above, check areas that need significant improvement:		5.b(1). POA&M Policy is not fully developed.
		5.b(2). POA&M procedures are not fully developed and sufficiently detailed.

⁶ *Corrective Actions to Address the Disaster Recovery Material Weakness Are Being Completed* (Reference Number 2011-20-060, dated June 27, 2011).



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

	5.b(3). POA&M procedures are not consistently implemented in accordance with government policies.
	5.b(4). POA&Ms do not include security weaknesses discovered during assessments of security controls and requiring remediation (OMB M-04-25).
	5.b(5). Remediation actions do not sufficiently address weaknesses in accordance with government policies (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls).
	5.b(6). Source of security weaknesses are not tracked (OMB M-04-25).
	5.b(7). Security weaknesses are not appropriately prioritized (OMB M-04-25).
	5.b(8). Milestone dates are not adhered to (OMB M-04-25).
	5.b(9). Initial target remediation dates are frequently missed (OMB M-04-25).
	5.b(10). POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).
x	5.b(11). Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25).
	5.b(12). Agency Chief Information Officer does not track and review POA&Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).
	5.b(13). Other
	5.b(13ex). Explanation for Other
	5.c. The Agency has not established a POA&M program.
<p>Comments: Our review of the 10 IRS systems selected for the Fiscal Year 2011 FISMA evaluation found that improvements were needed to ensure costs associated with remediating weaknesses are identified.</p> <ul style="list-style-type: none"> Thirteen (39 percent) of 33 closed weaknesses and 24 (31 percent) of 77 open weaknesses, maintained in the 10 IRS systems' Fiscal Year 2011 POA&Ms, did not have costs associated with remediating the weaknesses in accordance with IRS policy. 	

6: Remote Access Management

Status of Remote Access Management Program [check one]	x	<p>6.a. The Agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p>6.a(1). Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.</p> <p>6.a(2). Protects against unauthorized connections or subversion of authorized connections.</p> <p>6.a(3). Users are uniquely identified and authenticated for all access.</p> <p>6.a(4). If applicable, multi-factor authentication is required for remote access.</p> <p>6.a(5). Authentication mechanisms meet NIST Special Publication 800-63</p>
---	---	---



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

		<p>guidance on remote electronic authentication, including strength mechanisms.</p> <p>6.a(6). Defines and implements encryption requirements for information transmitted across public networks.</p> <p>6.a(7). Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication is required.</p>
		6.b. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.
If 6.b. is checked above, check areas that need significant improvement:		6.b(1). Remote access policy is not fully developed (NIST 800-53: AC-1, AC-17).
		6.b(2). Remote access procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1, AC-17).
		6.b(3). Remote access procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-1, AC-17).
		6.b(4). Telecommuting policy is not fully developed (NIST 800-46, Section 5.1).
		6.b(5). Telecommuting procedures are not fully developed or sufficiently detailed in accordance with government policies (NIST 800-46, Section 5.4).
		6.b(6). Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, Section 5.1).
		6.b(7). Multi-factor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).
		6.b(8). Agency has not identified all remote devices (NIST 800-46, Section 2.1).
		6.b(9). 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).
		6.b(10). Agency does not adequately monitor remote devices when connected to the agency’s networks remotely in accordance with government policies (NIST 800-46, Section 3.2).
		6.b(11). Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).
		6.b(12). Remote access rules of behavior are not adequate in accordance with government policies (NIST 800-53, PL-4).
		6.b(13). Remote access user agreements are not adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6).
		6.b(14). Other
	6.b(14ex). Explanation for Other	
		6.c. The Agency has not established a program for providing secure remote access.
Comments:		



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

7: Identity and Access Management

Status of Account and Identity Management Program [check one]		<p>7.a. The Agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p>7.a(1). Documented policies and procedures for account and identity management.</p> <p>7.a(2). Identifies all users, including Federal employees, contractors, and others who access Agency systems.</p> <p>7.a(3). Identifies when special access requirements (e.g., multi-factor authentication) are necessary.</p> <p>7.a(4). If multi-factor authentication is in use, it is linked to the Agency’s personal identity verification program where appropriate.</p> <p>7.a(5). Ensures that the users are granted access based on needs and separation of duties principles.</p> <p>7.a(6). Identifies devices that are attached to the network and distinguishes these devices from users.</p> <p>7.a(7). Ensures that accounts are terminated or deactivated once access is no longer required.</p> <p>7.a(8). Identifies and controls use of shared accounts.</p>
	X	<p>7.b. The Agency has established and is maintaining an identity and access management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.</p>
If 7.b. is checked above, check areas that need significant improvement:		<p>7.b(1). Account management policy is not fully developed (NIST 800-53: AC-1).</p> <p>7.b(2). Account management procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1).</p> <p>X 7.b(3). Account management procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-2).</p> <p>7.b(4). Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).</p> <p>7.b(5). Accounts are not properly issued to new users (NIST 800-53, AC-2).</p> <p>X 7.b(6). Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).</p> <p>7.b(7). Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).</p> <p>7.b(8). Agency has not adequately planned for implementation of personal identity verification for logical access in accordance with government policies (Homeland Security Presidential Directive 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).</p>



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

x	7.b(9). Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).
	7.b(10). Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).
	7.b(11). Network devices are not properly authenticated (NIST 800-53, IA-3).
	7.b(12). The process for requesting or approving membership in shared privileged accounts is not adequate in accordance to government policies.
	7.b(13). Use of shared privileged accounts is not necessary or justified.
	7.b(14). When shared accounts are used, the Agency does not renew shared account credentials when a member leaves the group.
	7.b(15). Other
	7.b(15ex). Explanation for Other
	7.c. The Agency has not established an identity and access management program.
<p>Comments: In March 2011, the GAO reported⁷ that the IRS had newly identified and unresolved weaknesses related to access controls, configuration management, and segregation of duties that continue to jeopardize the confidentiality, integrity, and availability of the financial and sensitive taxpayer information processed by IRS's systems. Considered collectively, these weaknesses were the basis for GAO's determination that the IRS had a material weakness in internal control over its financial reporting related to information security in Fiscal Year 2010. In May 2011, the TIGTA reported⁸ access controls had not been implemented or were not operating effectively on an IRS bankruptcy case tracking system, on which many IRS employees had excessive privileges. In addition, the TIGTA reported that user accounts on the bankruptcy case tracking system were not properly terminated when users no longer required access. Our review of the 10 IRS systems selected for the Fiscal Year 2011 FISMA evaluation found that all systems needed improvement in implementing NIST baseline access controls and identity and authentication controls.</p>	

⁷ *INFORMATION SECURITY: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data* (GAO-11-308, dated March 2011).

⁸ *Access Controls for the Automated Insolvency System Need Improvement* (Reference Number 2011-20-046, dated May 16, 2011).



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

8: Continuous Monitoring Management

Status of Continuous Monitoring Program [check one]	<input checked="" type="checkbox"/>	<p>8.a. The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p>8.a(1). Documented policies and procedures for continuous monitoring.</p> <p>8.a(2). Documented strategy and plans for continuous monitoring.</p> <p>8.a(3). Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.</p> <p>8.a(4). Provides 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 and updates with the frequency defined in the strategy and/or plans.</p>
		<p>8.b. The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.</p>
If 8.b. is checked above, check areas that need significant improvement:		<p>8.b(1). Continuous monitoring policy is not fully developed (NIST 800-53: CA-7).</p>
		<p>8.b(2). Continuous monitoring procedures are not fully developed (NIST 800-53: CA-7).</p>
		<p>8.b(3). Continuous monitoring procedures are not consistently implemented (NIST 800-53: CA-7; 800-37 Rev 1, Appendix G).</p>
		<p>8.b(4). Strategy or plan has not been fully developed for enterprise-wide continuous monitoring (NIST 800-37 Rev 1, Appendix G).</p>
		<p>8.b(5). Ongoing assessments of security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).</p>
		<p>8.b(6). The following were not provided to the 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).</p>
		<p>8.b(7). Other</p>
		<p>8.b(7ex). Explanation for Other</p>
Comments:		<p>8.c. The Agency has not established a continuous monitoring program.</p>



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

9: Contingency Planning

Status of Contingency Planning Program [check one]	<input checked="" type="checkbox"/>	<p>9.a. The Agency established and is maintaining an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p>9.a(1). Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.</p> <p>9.a(2). The agency has performed an overall business impact analysis.</p> <p>9.a(3). Development and documentation of division, component, and information technology infrastructure recovery strategies, plans and procedures.</p> <p>9.a(4). Testing of system specific contingency plans.</p> <p>9.a(5). The documented business continuity and disaster recovery plans are in place and can be implemented when necessary.</p> <p>9.a(6). Development of test, training, and exercise programs.</p> <p>9.a(7). Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans.</p>
		<p>9.b. The Agency has established and is maintaining an enterprise-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.</p>
If 9.b. is checked above, check areas that need significant improvement:		<p>9.b(1). Contingency planning policy is not fully developed contingency planning policy is not consistently implemented (NIST 800-53: CP-1).</p> <p>9.b(2). Contingency planning procedures are not fully developed (NIST 800-53: CP-1).</p> <p>9.b(3). Contingency planning procedures are not consistently implemented (NIST 800-53; 800-34).</p> <p>9.b(4). An overall business impact assessment has not been performed (NIST SP 800-34).</p> <p>9.b(5). Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).</p> <p>9.b(6). A business continuity/disaster recovery plan has not been developed (Federal Continuity Directive 1 (FCD1), NIST SP 800-34).</p> <p>9.b(7). A business continuity/disaster recovery plan has been developed but not fully implemented (FCD1, NIST SP 800-34).</p> <p>9.b(8). System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).</p> <p>9.b(9). System contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53).</p> <p>9.b(10). Test, training, and exercise programs have not been developed (FCD1, NIST SP 800-34, NIST 800-53).</p>



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

	9.b(11). Test, training, and exercise programs have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).
	9.b(12). After-action report did not address issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).
	9.b(13). Systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).
	9.b(14). Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).
	9.b(15). Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).
	9.b(16). Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).
	9.b(17). Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).
	9.b(18). Contingency planning does not consider supply chain threats.
	9.b(19). Other
	9.b(19ex). Explanation for Other
	9.c. The Agency has not established a business continuity/disaster recovery program.
Comments:	



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

10: Contractor Systems

Status of Agency Program to Oversee Contractor Systems [check one]	<input checked="" type="checkbox"/>	<p>10.a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p>10.a(1). Documented policies and procedures for information security oversight of systems operated on the Agency’s behalf by contractors or other entities, including Agency systems and services residing in public cloud.</p> <p>10.a(2). The Agency obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and agency guidelines.</p> <p>10.a(3). A complete inventory of systems operated on the Agency’s behalf by contractors or other entities, including Agency systems and services residing in public cloud.</p> <p>10.a(4). The inventory identifies interfaces between these systems and Agency-operated systems.</p> <p>10.a(5). The agency requires appropriate agreements (e.g., Memorandums of Understanding, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.</p> <p>10.a(6). The inventory of contractor systems is updated at least annually.</p> <p>10.a(7). Systems that are owned or operated by contractors or entities, including Agency systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.</p>
		<p>10.b. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in public cloud. However, the Agency needs to make significant improvements as noted below.</p>
If 10.b. is checked above, check areas that need significant improvement:		<p>10.b(1). Policies to oversee systems operated on the Agency’s behalf by contractors or other entities, including Agency systems and services residing in public cloud, are not fully developed.</p> <p>10.b(2). Procedures to oversee systems operated on the Agency’s behalf by contractors or other entities, including Agency systems and services residing in public cloud, are not fully developed.</p> <p>10.b(3). Procedures to oversee systems operated on the Agency’s behalf by contractors or other entities, including Agency systems and services residing in public cloud are not consistently implemented.</p> <p>10.b(4). The inventory of systems owned or operated by contractors or other entities, including Agency systems and services residing in public cloud, is not complete in accordance with government policies (NIST 800-53: PM-5).</p> <p>10.b(5). The inventory does not identify interfaces between contractor/entity-operated systems to Agency owned and operated systems.</p>



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

	10.b(6). The inventory of contractor/entity-operated systems, including interfaces, is not updated at least annually.
	10.b(7). Systems owned or operated by contractors and entities are not subject to NIST and OMB’s FISMA requirements (e.g., security requirements).
	10.b(8). Systems owned or operated by contractors and entities do not meet NIST and OMB’s FISMA requirements (e.g., security requirements).
	10.b(9). Interface agreements (e.g., Memorandums of Understanding) are not properly documented, authorized, or maintained.
	10.b(10). Other
	10.b(10ex). Explanation for Other:
	10.c. The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in public cloud.
Comments:	

11: Security Capital Planning

Status of Agency Program to Oversee Security Capital Planning [check one]	<input checked="" type="checkbox"/>	<p>11.a. The Agency has established and maintains a security capital planning and investment program for information security. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:</p> <p>11.a(1). Documented policies and procedures to address information security in the capital planning and investment control process.</p> <p>11.a(2). Includes information security requirements as part of the capital planning and investment process.</p> <p>11.a(3). Establishes a discrete line item for information security in organizational programming and documentation.</p> <p>11.a(4). Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.</p> <p>11.a(5). Ensures that information security resources are available for expenditure as planned.</p>
		<p>11.b. The Agency has established and maintains a capital planning and investment program. However, the Agency needs to make significant improvements as noted below.</p>
If 11.b. is checked above, check areas that need significant improvement:		11.b(1). Capital planning and investment control information security policy is not fully developed.
		11.b(2). Capital planning and investment control information security procedures are not fully developed.
		11.b(3). Capital planning and investment control information security procedures are not consistently implemented.
		11.b(4). The Agency does not adequately plan for information technology security during the capital planning and investment control process (SP 800-65).



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

	11.b(5). The Agency does not include a separate line for information security in appropriate documentation (NIST 800-53: SA-2).
	11.b(6). Exhibits 300/53 or business cases do not adequately address or identify information security costs (NIST 800-53: PM-3).
	11.b(7). The Agency does not provide information technology security funding to maintain the security levels identified.
	11.b(8). Other
	11.b(8ex). Explanation for Other
	11.c. The Agency does not have a capital planning and investment program.
Comments:	



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

Appendix I

Treasury Inspector General for Tax Administration Information Technology Security Reports Issued During the Fiscal Year 2011 Evaluation Period

1. *The Internal Revenue Service Is Improving Management Controls for Information Technology Strategic Planning and Capital Investments* (Reference Number 2010-20-064, dated July 9, 2010).
2. *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).
3. *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).
4. *The Federal Student Aid Datashare Application Was Successfully Deployed, but Improvements in Systems Development Disciplines Are Needed* (Reference Number 2010-20-099, dated September 3, 2010).
5. *Treasury Inspector General for Tax Administration Federal Information Security Management Act (Non-Intelligence National Security Systems) Report for Fiscal Year 2010* (Reference Number 2010-20-101, dated September 9, 2010).
6. *Annual Assessment of the Business Systems Modernization Program* (Reference Number 2010-20-094, dated September 23, 2010).
7. *Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2010* (Reference Number 2011-20-003, dated November 10, 2010).
8. *Prototype Process Improvements Will Benefit Efforts to Modernize Taxpayer Account Administration* (Reference Number 2011-20-001, dated November 24, 2010).
9. *The Sustaining Infrastructure Program Is Significantly Improved and a Comprehensive Information Technology Infrastructure Strategy Has Been Developed* (Reference Number 2011-20-006, dated December 30, 2010).
10. *Additional Security Is Needed for the Taxpayer Secure Email Program* (Reference Number 2011-20-012, dated February 4, 2011).



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

11. *The Applications Development Function’s Quality Assurance Program Office Can Make Its Processes More Effective* (Reference Number 2011-20-007, dated February 17, 2011).
12. *Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected* (Reference Number 2011-20-044, dated May 4, 2011).
13. *Access Controls for the Automated Insolvency System Need Improvement* (Reference Number 2011-20-046, dated May 16, 2011).
14. *Corrective Actions to Address the Disaster Recovery Material Weakness Are Being Completed* (Reference Number 2011-20-060, dated June 27, 2011).



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Louis Lee, Lead Auditor
Charles Ekunwe, Senior Auditor
Bret Hunter, Senior Auditor
Esther Wilson, Senior Auditor
Victor Taylor, Auditor



*Treasury Inspector General for Tax
Administration – Federal Information Security
Management Act Report for Fiscal Year 2011*

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
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM