TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2014

September 23, 2014

Reference Number: 2014-20-090

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
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION – FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT FOR FISCAL YEAR 2014

Highlights

Final Report Issued on September 23, 2014

Highlights of Reference Number: 2014-20-090 to the Department of the Treasury, Office of the Inspector General, Assistant Inspector General for Audit.

IMPACT ON TAXPAYERS

The Federal Information Security Management Act of 2002 (FISMA) was enacted to strengthen the security of information and systems within Federal Government agencies. The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. As custodians of taxpayer information, the IRS has an obligation to protect the confidentiality of this sensitive information against unauthorized access or loss.

WHY TIGTA DID THE AUDIT

As part of the FISMA legislation, the Offices of Inspectors General are required to perform an annual independent evaluation of each Federal agency's information security programs and practices. This report presents the results of TIGTA's FISMA evaluation of the IRS for Fiscal Year 2014.

WHAT TIGTA FOUND

Based on this year's FISMA evaluation, five of the 11 security program areas met the performance metrics specified by the Department of Homeland Security's *Fiscal Year 2014 Inspector General Federal Information Security Management Act Reporting Metrics:*

- Risk Management.
- Plan of Action and Milestones.
- Contingency Planning.
- Contractor Systems.
- Security Capital Planning.

Four security program areas were not fully effective due to one or more program attributes that were not met:

- Continuous Monitoring Management.
- Incident Response and Reporting.
- Security Training.
- Remote Access Management.

Two security program areas did not meet the level of performance specified due to the majority of the attributes not being met:

- Configuration Management.
- Identity and Access Management.

To meet the expected level of performance for Configuration Management, the IRS needs to improve enterprise-wide processes for assessing configuration settings and vulnerabilities through automated scanning, timely remediating scan result deviations, timely installing software patches, and controlling changes to hardware and software configurations.

To meet the expected level of performance for Identity and Access Management, the IRS needs to fully implement unique user identification and authentication that complies with Homeland Security Presidential Directive-12, ensure that users are only granted access based on needs, ensure that user accounts are terminated when no longer required, and control the improper use of shared accounts.

WHAT TIGTA RECOMMENDED

TIGTA does not include recommendations as part of its annual FISMA evaluation and reports only on the level of performance achieved by the IRS using the guidelines issued by the Department of Homeland Security for the applicable FISMA evaluation period.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 23, 2014

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

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2014 (Audit # 201420001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Management Act[1] evaluation of the Internal Revenue Service for Fiscal Year 2014. The Act requires Federal agencies to have an annual independent evaluation performed of their information security programs and practices and to report the results of the evaluations to the Office of Management and Budget.

The report was forwarded to the Treasury Inspector General for consolidation into a report issued to the Department of the Treasury Chief Information Officer. Copies of this report are also being sent to the IRS managers affected by the report results.

If you have any questions, please contact me or Kent Sagara, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

[1] Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.

Table of Contents

Abbreviations

CIO	Chief Information Officer
DHS	Department of Homeland Security
FCD1	Federal Continuity Directive 1
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
HSPD-12	Homeland Security Presidential Directive-12
IP	Internet Protocol
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring
IT	Information Technology
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
SCAP	Security Content Automation Protocol
SP	Special Publication
TIGTA	Treasury Inspector General for Tax Administration
US-CERT	United States Computer Emergency Response Team
USGCB	United States Government Configuration Baseline

Background

The Federal Information Security Management Act (FISMA) of 2002[1] was enacted to strengthen the security of information and systems within Federal agencies. The FISMA requires Federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

The FISMA requires the Office of Management and Budget (OMB) to develop and oversee the implementation of policies, principles, standards, and guidelines on information security that are commensurate with the risk and magnitude of the possible harm to Federal systems or information. To ensure uniformity in this process, the FISMA requires the National Institute of Standards and Technology (NIST) to prescribe standards and guidelines pertaining to Federal information systems. The FISMA also charges the OMB with producing an annual report to keep Congress apprised of Federal progress in increasing information security.

Agency heads are responsible for complying with the requirements of FISMA and related OMB policies and NIST procedures, standards, and guidelines. In addition, the FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to the OMB. The FISMA states that the independent evaluation is to be performed by the agency Inspector General or an independent external auditor as determined by the Inspector General.

In July 2010, OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, expanded the role of the DHS in regard to the operational aspects of Federal agency cybersecurity and information systems that fall within FISMA requirements. The DHS prepares the security metrics to assist the Federal agencies and the Inspectors General in evaluating agency progress in achieving compliance with Federal security standards.

FISMA oversight of the Department of the Treasury is performed by two distinct Inspector General offices: the Treasury Inspector General for Tax Administration (TIGTA) and the Treasury Office of the Inspector General (OIG). The TIGTA is responsible for oversight of the Internal Revenue Service (IRS), while the Treasury OIG is responsible for all other Treasury bureaus. The Treasury OIG has contracted with KPMG LLP to perform the FISMA evaluation of the non-IRS bureaus. The TIGTA will issue its final report with the results of its evaluation of the IRS to the Treasury OIG, which will then combine the results for all the Treasury bureaus into one report for the OMB.

[1] Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.

The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. As custodians of taxpayer information, the IRS is responsible for implementing appropriate security controls to protect the confidentiality of this sensitive information against unauthorized access or loss.

This review was performed at, and with information obtained from, the IRS Information Technology organization's Office of Cybersecurity in New Carrollton, Maryland, during the period May through August 2014. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

The Internal Revenue Service's Information Security Program Generally Complies With the Federal Information Security Management Act, but Improvements Are Needed in Configuration Management and Identity and Access Management

To assist the Inspectors General in evaluating Federal agencies' compliance with the FISMA, the DHS issued the *Fiscal Year (FY) 2014 Inspector General Federal Information Security Management Act Reporting Metrics* on December 2, 2013, which specified 11 information security program areas and listed specific attributes within each area for evaluation. The 11 information security program areas are continuous monitoring management, configuration management, identity and access management, incident and response reporting, risk management, security training, plan of action and milestones, remote access management, contingency planning, contractor systems, and security capital planning.

Overall, the IRS has established an information security program and related practices that cover the 11 FISMA program areas. However, based on our FY 2014 FISMA evaluation, two of the program areas, Configuration Management and Identity and Access Management, did not meet applicable FISMA requirements due to the majority of the program attributes specified by the DHS guidelines not being met. We also identified improvements needed in five other FISMA program areas.

Based on our FY 2014 FISMA evaluation, five of the 11 security program areas met the performance metrics specified in the DHS guidelines:

- Risk Management.[2]
- Plan of Action and Milestones.
- Contingency Planning.
- Contractor Systems.
- Security Capital Planning.

[2] Although the IRS met the performance metrics specified by the DHS for Risk Management, TIGTA found deficiencies with the IRS's risk-based decisions process that were not in alignment with policy. Specifically, we found that not all risk-based decisions are adequately documented and tracked.

Four security program areas were not fully effective due to one or more DHS guideline program attributes that were not met:

- Continuous Monitoring Management.

  The IRS has not yet implemented its Information Security Continuous Monitoring (ISCM) strategy, but stated that it is fully participating in the DHS's Continuous Diagnostics and Mitigation Program to comply with the OMB M-14-03[3] mandate to implement ISCM and is in the process of determining its final toolset to meet the program requirements.

- Incident Response and Reporting.

  The IRS did not always report incidents involving Personally Identifiable Information to the U.S. Computer Emergency Response Team (US-CERT) within established time frames.

- Security Training.

  The IRS has not yet fully implemented a process for identifying and tracking contractors who are required to complete specialized training, but stated that it continues to make progress and is working to incorporate a clause into contracts that requires contractors to complete and record such training.

- Remote Access Management.

  The IRS has not fully implemented unique user identification and authentication that complies with Homeland Security Presidential Directive-12 (HSPD-12).

Two security program areas, Configuration Management and Identity and Access Management, did not meet the level of performance specified by the DHS guidelines due to the majority of the specified attributes not being met:

- Configuration Management.

  To meet the expected level of performance for Configuration Management, the IRS needs to improve enterprise-wide processes for assessing configuration settings and vulnerabilities through automated scanning, timely remediating scan result deviations, timely installing software patches, and controlling changes to hardware and software configurations.

[3] OMB, OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems* (Nov. 2013).

- Identity and Access Management.

  To meet the expected level of performance for Identity and Access Management, the IRS needs to fully implement unique user identification and authentication that complies with HSPD-12, ensure that users are only granted access based on needs, ensure that user accounts are terminated when no longer required, and control the improper use of shared accounts.

Until the IRS takes steps to improve its security program deficiencies and fully implements all 11 security program areas required by the FISMA, taxpayer data will remain vulnerable to inappropriate use, modification, or disclosure, possibly without being detected.

Figure 1 presents TIGTA's detailed results for the 11 security program areas in response to the DHS's *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*.[4] TIGTA's results will be consolidated with the Treasury OIG's results of non-IRS bureaus and reported to the OMB.

Figure 1: TIGTA's Responses to the DHS's FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics

1: Continuous Monitoring Management

Status of Continuous Monitoring Management Program [check one: Yes or No]	Yes	**1.1.** Has the organization 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? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**1.1.1.** Documented policies and procedures for continuous monitoring. (NIST SP 800-53: CA-7)
	Yes	**1.1.2.** Documented strategy for information security continuous monitoring. (ISCM)
	No	**1.1.3.** Implemented ISCM for information technology assets. **TIGTA Comments:** The IRS has not yet implemented its ISCM strategy, but it stated that it is fully participating in the DHS's Continuous Diagnostics and Mitigation Program to comply with the OMB M-14-03 mandate and is in the process of determining its final toolset to meet the program requirements.
	Yes	**1.1.4.** Evaluate risk assessments used to develop their ISCM strategy.

[4] Many abbreviations in this matrix are used as presented in the original document and are not defined therein. However, we have provided the definitions in the Abbreviations page after the Table of Contents of this report.

	No	**1.1.5.** Conduct and report on ISCM results in accordance with their ISCM strategy. **TIGTA Comments:** The IRS has not yet implemented its ISCM strategy, but it stated that it is fully participating in the DHS's Continuous Diagnostics and Mitigation Program to comply with the OMB M-14-03 mandate and is in the process of determining its final toolset to meet the program requirements.
	Yes	**1.1.6.** Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans. (NIST SP 800-53, NIST SP800-53A)
	Yes	**1.1.7.** Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans. (NIST SP 800-53, 800-53A)
		1.2. Please provide any additional information on the effectiveness of the organization's Continuous Monitoring Management Program that was not noted in the questions above.

2: Configuration Management

Status of Configuration Management Program [check one: Yes or No]	**No**	**2.1.** Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**2.1.1.** Documented policies and procedures for configuration management.
	Yes	**2.1.2.** Defined standard baseline configurations.
	No	**2.1.3.** Assessments of compliance with baseline configurations. **TIGTA Comments:** The IRS has not deployed automated mechanisms to centrally manage, apply, and verify baseline configuration settings and produce FISMA compliance reports using the NIST-defined Security Content Automation Protocol (SCAP) format for all of its IT assets.
	No	**2.1.4.** Process for timely (as specified in organization policy or standards) remediation of scan result deviations. **TIGTA Comments:** The IRS has not yet fully implemented configuration baseline scanning tools and processes on all systems to ensure timely remediation of scan result deviations.
	Yes	**2.1.5.** For Windows-based components, USGCB secure configuration settings are fully implemented and any deviations from USGCB baseline settings are fully documented.

	No	**2.1.6.** Documented proposed or actual changes to the hardware and software configurations. **TIGTA Comments:** The IRS has not yet fully implemented configuration and change management controls to ensure that proposed or actual changes to hardware and software configurations are documented and controlled.
	No	**2.1.7.** Process for the timely and secure installation of software patches. **TIGTA Comments:** The IRS has not implemented an adequate enterprise-wide process to ensure timely installation of software patches on all platforms.
	No	**2.1.8.** Software assessing (scanning) capabilities are fully implemented. (NIST SP 800-53: RA-5, SI-2) **TIGTA Comments:** Monthly software assessment vulnerability scans are not performed on all systems.
	No	**2.1.9.** Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards. (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2) **TIGTA Comments:** The IRS has not yet fully implemented configuration-related vulnerability scanning tools and processes on all systems to ensure timely remediation of scan result deviations. Also, IRS processes to share vulnerability information with system owners and administrators are still under development.
	No	**2.1.10.** Patch management process is fully developed, as specified in organization policy or standards. (NIST SP 800-53: CM-3, SI-2) **TIGTA Comments**: The IRS has not implemented an adequate enterprise-wide process to ensure timely installation of software patches on all platforms.
		2.2. Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above. **TIGTA Comments:** The IRS intends to create and deploy a standard change management process for its Information Technology organization, supported by an integrated change management system called the Enterprise Configuration Management System.
	No	**2.3.** Does the organization have an enterprise deviation handling process and is it integrated with the automated capability? **TIGTA Comments:** The IRS has not yet implemented its ISCM strategy in order to accomplish an enterprise deviation handling process that is integrated with an automated capability.

	No	**2.3.1.** Is there a process for mitigating the risk introduced by those deviations? **TIGTA Comments:** The IRS has not yet implemented its ISCM strategy in order to accomplish an enterprise deviation handling process that is integrated with an automated capability.

3: Identity and Access Management

Status of Identity and Access Management Program [check one: Yes or No]	**No**	**3.1.** Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and that identifies users and network devices? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**3.1.1.** Documented policies and procedures for account and identity management. (NIST SP 800-53: AC-1)
	No	**3.1.2.** Identifies all users, including Federal employees, contractors, and others who access organization systems. (NIST SP 800-53: AC-2) **TIGTA Comments:** Users are not uniquely identified and authenticated on all IRS systems. Also, the IRS has not fully implemented unique user identification and authentication that complies with HSDP-12. In addition, nine of the 10 systems we reviewed did not have the NIST SP 800-53 AC-2 security control fully in place.
	No	**3.1.3.** Identifies when special access requirements (*e.g.*, multifactor authentication) are necessary. **TIGTA Comments:** The IRS has not fully implemented multifactor authentication in compliance with HSPD-12.
	No	**3.1.4.** If multifactor authentication is in use, it is linked to the organization's PIV program where appropriate. (NIST SP 800-53: IA-2) **TIGTA Comments:** The IRS has not fully deployed multifactor authentication via the use of an HSPD-12 PIV card for all users for network and local access to nonprivileged or privileged accounts as required by HSPD-12.
	No	**3.1.5.** Organization has planned for implementation of PIV for logical access in accordance with Government policies. (HSPD-12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11) **TIGTA Comments:** Considerable challenges still exist for the IRS in achieving full implementation of PIV for logical access due to its legacy environment and other factors.

	No	**3.1.6.** Organization has adequately planned for implementation of PIV for physical access in accordance with Government policies. (HSPD-12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11) **TIGTA Comments:** During the FY14 FISMA evaluation period, the IRS had not planned to implement PIV for physical access at all its facilities. However, the IRS has informed us that it has prioritized the remaining locations and developed a long-range plan, dependent on the availability of funding.
	No	**3.1.7.** Ensures that the users are granted access based on needs and separation-of-duties principles. **TIGTA Comments:** During FY 2013 and FY 2014, the GAO identified users that had been granted more access than needed and instances where the separation-of-duties principle was not enforced.
	No	**3.1.8.** Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts.) **TIGTA Comments:** The IRS is still in the process of implementing technical solutions and introducing automated tools to achieve full asset discovery and asset management in accordance with policy.
	Yes	**3.1.9.** Identifies all user and nonuser accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.)
	No	**3.1.10.** Ensures that accounts are terminated or deactivated once access is no longer required. **TIGTA Comments:** The IRS identified systems that do not have controls in place to ensure that accounts are terminated or deactivated once access is no longer needed.
	No	**3.1.11.** Identifies and controls use of shared accounts. **TIGTA Comments:** During FY 2013 and FY 2014, the GAO identified improper use of shared accounts; for example, use of a generic administrator accounts and passwords.
		3.2. Please provide any additional information on the effectiveness of the organization's Identity and Access Management that was not noted in the questions above.

4: Incident Response and Reporting

Status of Incident Response and Reporting Program [check one: Yes or No]	Yes	**4.1.** Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**4.1.1.** Documented policies and procedures for detecting, responding to, and reporting incidents. (NIST SP 800-53: IR-1)
	Yes	**4.1.2.** Comprehensive analysis, validation, and documentation of incidents.
	No	**4.1.3.** When applicable, reports to US-CERT within established time frames. (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19) **TIGTA Comments:** The IRS did not always report incidents involving Personally Identifiable Information to the US-CERT within established time frames.
	Yes	**4.1.4.** When applicable, reports to law enforcement within established time frames. (NIST SP 800-61)
	Yes	**4.1.5.** Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage. (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19)
	Yes	**4.1.6.** Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.
	Yes	**4.1.7.** Is capable of correlating incidents.
	Yes	**4.1.8.** Has sufficient incident monitoring and detection coverage in accordance with Government policies. (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19)
		4.2. Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.

5: Risk Management

Status of Risk Management Program [check one: Yes or No]	Yes	**5.1.** Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**5.1.1.** Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.

	Yes	**5.1.2.** Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev.1.
	Yes	**5.1.3.** Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1.
	Yes	**5.1.4.** Addresses risk from an information system perspective and is guided by the risk decisions from the organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1.
	Yes	**5.1.5.** Has an up-to-date system inventory.
	Yes	**5.1.6.** Categorizes information systems in accordance with Government policies.
	Yes	**5.1.7.** Selects an appropriately tailored set of baseline security controls.
	Yes	**5.1.8.** Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.
	Yes	**5.1.9.** 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.
	Yes	**5.1.10.** 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.
	Yes	**5.1.11.** Ensures that information security controls are monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.
	Yes	**5.1.12.** Information system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.
	Yes	**5.1.13.** Senior officials are briefed on threat activity on a regular basis by appropriate personnel (*e.g.*, Chief Information Security Officer).
	Yes	**5.1.14.** 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.

	Yes	**5.1.15.** Security authorization package contains system security plan, security assessment report, and POA&M in accordance with Government policies. (NIST SP 800-18, 800-37)
	Yes	**5.1.16.** Security authorization package contains accreditation boundaries, defined in accordance with Government policies, for organization information systems**.**
		5.2. Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above. **TIGTA Comments:** TIGTA found deficiencies with the IRS's risk-based decisions process that were not in alignment with policy. Specifically, we found that not all risk-based decisions are adequately documented and tracked.

6: Security Training

Status of Security Training Program [check one: Yes or No]	Yes	**6.1.** Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**6.1.1.** Documented policies and procedures for security awareness training. (NIST SP 800-53: AT-1)
	Yes	**6.1.2.** Documented policies and procedures for specialized training for users with significant information security responsibilities.
	Yes	**6.1.3.** Security training content based on the organization and roles, as specified in organization policy or standards.
	Yes	**6.1.4.** Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training.
	No	**6.1.5.** Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training. **TIGTA Comments:** The IRS has not yet fully implemented a process for identifying and tracking contractors who are required to complete specialized training, but it stated that it continues to make progress and is working to incorporate a clause into contracts that requires contractors to complete and record such training.
	Yes	**6.1.6.** Training material for security awareness training contains appropriate content for the organization. (NIST SP 800-50, 800-53)

		6.2. Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.

7: Plan of Action & Milestones (POA&M)

Status of POA&M Program [check one: Yes or No]	Yes	**7.1.** Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**7.1.1.** Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.
	Yes	**7.1.2.** Tracks, prioritizes, and remediates weaknesses.
	Yes	**7.1.3.** Ensures that remediation plans are effective for correcting weaknesses.
	Yes	**7.1.4.** Establishes and adheres to milestone remediation dates.
	Yes	**7.1.5.** Ensures that resources and ownership are provided for correcting weaknesses.
	Yes	**7.1.6.** POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weaknesses due to a risk-based decision to not implement a security control). (OMB M-04-25)
	Yes	**7.1.7.** Costs associated with remediating weaknesses are identified. (NIST SP 800-53: PM-3; OMB M-04-25)
	Yes	**7.1.8.** Program officials report progress on remediation to the CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly. (NIST SP 800-53: CA-5; OMB M-04-25)
		7.2. Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above.

8: Remote Access Management

Status of Remote Access Management Program [check one: Yes or No]	Yes	**8.1.** Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**8.1.1.** Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access. (NIST SP 800-53: AC-1, AC-17)

	Yes	**8.1.2.** Protects against unauthorized connections or subversion of authorized connections.
	No	**8.1.3.** Users are uniquely identified and authenticated for all access. (NIST SP 800-46, Section 4.2, Section 5.1) **TIGTA Comments:** The IRS has not fully implemented unique user identification and authentication that complies with HSPD-12. In addition, system administrators of the virtual private network infrastructure and server components do not use NIST-compliant multifactor authentication for local or network access to privileged accounts.
	Yes	**8.1.4.** Telecommuting policy is fully developed. (NIST SP 800-46, Section 5.1)
	No	**8.1.5.** If applicable, multifactor authentication is required for remote access. (NIST SP 800-46, Section 2.2, Section 3.3) **TIGTA Comments:** The IRS has not fully implemented multifactor authentication that complies with HSPD-12.
	No	**8.1.6.** Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. **TIGTA Comments:** The IRS has not fully implemented multifactor authentication that complies with HSPD-12.
	Yes	**8.1.7.** Defines and implements encryption requirements for information transmitted across public networks.
	Yes	**8.1.8.** Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity, after which reauthentication is required.
	Yes	**8.1.9.** Lost or stolen devices are disabled and appropriately reported. (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines)
	Yes	**8.1.10.** Remote access rules of behavior are adequate in accordance with Government policies. (NIST SP 800-53: PL-4)
	Yes	**8.1.11.** Remote access user agreements are adequate in accordance with Government policies. (NIST SP 800-46, Section 5.1; NIST SP 800-53: PS-6)
		8.2. Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.
	Yes	**8.3.** Does the organization have a policy to detect and remove unauthorized (rogue) connections?

9: Contingency Planning

Status of Contingency Planning Program [check one: Yes or No]	Yes	**9.1.** Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**9.1.1.** Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster. (NIST SP 800-53: CP-1)
	Yes	**9.1.2.** The organization has incorporated the results of its system's Business Impact Analysis into the analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan. (NIST SP 800-34)
	Yes	**9.1.3.** Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures. (NIST SP 800-34)
	Yes	**9.1.4.** Testing of system-specific contingency plans.
	Yes	**9.1.5.** The documented business continuity and disaster recovery plans are in place and can be implemented when necessary. (FCD1, NIST SP 800-34)
	Yes	**9.1.6.** Development of test, training, and exercise programs**.** (FCD1, NIST SP 800-34, NIST SP 800-53)
	Yes	**9.1.7.** Testing or exercising of business continuity and disaster recovery plans to determine effectiveness and to maintain current plans.
	Yes	**9.1.8.** After-action report that addresses issues identified during contingency/disaster recovery exercises. (FDC1, NIST SP 800-34)
	Yes	**9.1.9.** Systems that have alternate processing sites. (FCD1, NIST SP 800-34, NIST SP 800-53)
	Yes	**9.1.10.** Alternate processing sites are not subject to the same risks as primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53)
	Yes	**9.1.11.** Backups of information that are performed in a timely manner. (FCD1, NIST SP 800-34, NIST SP 800-53)
	Yes	**9.1.12.** Contingency planning that considers supply chain threats.
		9.2. Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.

10: Contractor Systems

Status of Contractor Systems Program [check one: Yes or No]	Yes	**10.1.** Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**10.1.1.** Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud.
	Yes	**10.1.2.** The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines. (NIST SP 800-53: CA-2)
	Yes	**10.1.3.** A complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud. **TIGTA Comments:** In FY 2014, the IRS maintained two contractor-managed systems in the Treasury FISMA Information Management System (formerly, the Trusted Agent FISMA), which is the U.S. Department of the Treasury's system for reporting FISMA data. The IRS Contractor Security Assessments Office maintains a separate listing of contractor sites that the IRS does not consider "FISMA-reportable," but that require annual security reviews because each handles or processes IRS information. The IRS Contractor Security Assessments Office is responsible for evaluating security controls at these contractor sites.
	Yes	**10.1.4.** The inventory identifies interfaces between these systems and organization-operated systems. (NIST SP 800-53: PM-5)
	Yes	**10.1.5.** The organization 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.
	Yes	**10.1.6.** The inventory of contractor systems is updated at least annually.
	Yes	**10.1.7.** Systems that are owned or operated by contractors or entities, including organization systems and services residing in a public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.
		10.2. Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.

11: Security Capital Planning

Status of Security Capital Planning Program [check one: Yes or No]	Yes	**11.1.** Has the organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?
	Yes	**11.1.1.** Documented policies and procedures to address information security in the capital planning and investment control process.
	Yes	**11.1.2.** Includes information security requirements as part of the capital planning and investment process.
	Yes	**11.1.3.** Establishes a discrete line item for information security in organizational programming and documentation. (NIST SP 800-53: SA-2)
	Yes	**11.1.4.** Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required. (NIST SP 800-53: PM-3)
	Yes	**11.1.5.** Ensures that information security resources are available for expenditure as planned.
		11.2. Please provide any additional information on the effectiveness of the organization's Security Capital Planning Program that was not noted in the questions above.

Source: Results of TIGTA's FY 2014 FISMA evaluation of the IRS.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of this independent evaluation was to assess the effectiveness of the IRS's information technology security program and practices for the period July 1, 2013, to June 30, 2014. To accomplish our objective, we responded to the questions provided in the DHS *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, issued on December 2, 2013. The questions related to the following 11 security program areas:

1. Continuous Monitoring Management.
2. Configuration Management.
3. Identity and Access Management.
4. Incident Response and Reporting.
5. Risk Management.
6. Security Training.
7. Plan of Action and Milestones.
8. Remote Access Management.
9. Contingency Planning.
10. Contractor Systems.
11. Security Capital Planning.

We based our evaluation work, in part, on a representative subset of 10 major IRS information systems. We used the system inventory contained within the Treasury FISMA Information Management System[1] of major applications and general support systems with a security classification of "Moderate" or "High" as the population for this subset.

We also considered the results of TIGTA audits completed during the FY 2014 FISMA evaluation period, as listed in Appendix IV, as well as results from ongoing audits for which draft reports were issued to the IRS by August 8, 2014.

Based on our evaluative work, we indicated with a yes or no whether the IRS had achieved a satisfactory level of performance for each security program area as well as each specific attribute listed in the DHS *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*. The Treasury OIG will combine our results for the IRS with its results for the non-IRS bureaus and submit the combined yes or no responses to the OMB.

[1] Formerly the Trusted Agent FISMA system.

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
Midori Ohno, Lead Auditor
Cindy Harris, Senior Auditor
Bret Hunter, Senior Auditor
Mary Jankowski, Senior Auditor
Louis Lee, Senior Auditor
Esther Wilson, Senior Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
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 Liaisons:
- Business Planning and Risk Management OS:CTO:SP:RM
- Cybersecurity OS:CTO:C

Appendix IV

Treasury Inspector General for Tax Administration Information Technology Security-Related Reports Issued During the Fiscal Year 2014 Evaluation Period

1. TIGTA, Ref. No. 2014-20-021, *Used Information Technology Assets Are Being Properly Donated; However, Disposition Procedures Need to Be Improved* (April 2014).
2. TIGTA, Ref. No. 2014-20-016, *Planning Is Underway for the Enterprise-Wide Transition to Internet Protocol Version 6, but Further Actions Are Needed* (Feb. 2014).
3. TIGTA, Ref. No. 2013-20-063, *Improvements Are Needed to Ensure Successful Development and System Integration for the Return Review Program* (Jul. 2013).
4. TIGTA, Ref. No. 2013-20-089, *Weaknesses in Asset Management Controls Leave Information Technology Assets Vulnerable to Loss* (Sept. 2013).
5. TIGTA, Ref. No. 2013-20-106, *Automated Monitoring Is Needed for the Virtual Infrastructure to Ensure Secure Configurations* (Sept. 2013).
6. TIGTA, Ref. No. 2013-20-107, *Full Compliance With Trusted Internet Connection Requirements Is Progressing; However, Improvements Would Strengthen Security* (Sept. 2013).
7. TIGTA, Ref. No. 2013-20-108, *Better Cost-Benefit Analysis and Security Measures Are Needed for the Bring Your Own Device Pilot* (Sept. 2013).
8. TIGTA, Ref. No. 2013-20-117, *Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data* (Sept. 2013).
9. TIGTA, Ref. No. 2013-20-118, *Foreign Account Tax Compliance Act: Improvements Are Needed to Strengthen Systems Development Controls for the Foreign Financial Institution Registration System* (Sept. 2013).
10. TIGTA, Ref. No. 2013-20-125, *Customer Account Data Engine 2 Database Deployment Is Experiencing Delays and Increased Costs* (Sept. 2013)
11. TIGTA, Ref. No. 2013-20-127, *While Efforts Are Ongoing to Deploy a Secure Mechanism to Verify Taxpayer Identities, the Public Still Cannot Access Their Tax Account Information Via the Internet* (Sept. 2013).