TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2015

September 25, 2015

Reference Number: 2015-20-092

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 MODERNIZATION ACT REPORT FOR FISCAL YEAR 2015

Highlights

Final Report issued on September 25, 2015

Highlights of Reference Number: 2015-20-092 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, and its recent amendment, the Federal Information Security Modernization Act (FISMA) of 2014, were 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 this sensitive information against unauthorized access or loss in accordance with FISMA requirements.

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 2015.

WHAT TIGTA FOUND

The IRS's Information Security Program generally complied with the FISMA requirements. Three program areas met all FISMA performance attributes specified by the Department of Homeland Security: *Risk Management*, *Incident Response and Reporting*, and *Contingency Planning*. Four other security program areas met all attributes with the exception of two or fewer program attributes that were not met: *Security Training*, *Plan of Action and Milestones*, *Remote Access Management*, and *Contractor Systems*.

However, three security program areas failed to meet FISMA requirements overall due to not meeting many of the performance attributes specified by the Department of Homeland Security: *Continuous Monitoring Management*, *Configuration Management*, and *Identity and Access Management*.

Until the IRS takes steps to improve its security program deficiencies and fully implement all security program areas in compliance with FISMA requirements, taxpayer data will remain vulnerable to inappropriate and undetected use, modification, or disclosure.

WHAT TIGTA RECOMMENDED

TIGTA does not include recommendations as part of its annual FISMA evaluation and reports on only 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 25, 2015

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 Modernization Act Report for Fiscal Year 2015 (Audit # 201520001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Modernization Act[1] evaluation of the Internal Revenue Service for Fiscal Year 2015. 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.

This 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 Internal Revenue Service managers affected by the report results.

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

[1] Pub.L. No. 113-283. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

Table of Contents

Abbreviations

DHS	Department of Homeland Security
FCD1	Federal Continuity Directive 1
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAO	Government Accountability Office
HSPD-12	Homeland Security Presidential Directive-12
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring
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
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 of 2002[2] was enacted to strengthen the security of information and information systems within Federal agencies. The Act 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 entity. To ensure uniformity in this process, the Act requires the National Institute of Standards and Technology (NIST) to prescribe standards and guidelines pertaining to Federal information systems.

The Federal Information Security Modernization Act of 2014 intends to improve security by transitioning agencies away from paperwork requirements toward a more automated and continuous security posture.

After 12 years, an amendment to the Federal Information Security Management Act of 2002 was signed into law, called the Federal Information Security Modernization Act of 2014 (FISMA).[3] It provides several modifications to the Federal Information Security Management Act of 2002 that modernize Federal security practices to current security concerns. Specifically, it:

- Reasserts the authority of the Director of the Office of Management and Budget (OMB) with oversight, while authorizing the Secretary of the Department of Homeland Security (DHS) to administer the implementation of security policies and practices for Federal information systems.
- Requires agencies to notify Congress of major security incidents within seven days. The OMB will be responsible for developing guidance on what constitutes a major incident.
- Places more responsibility on agencies for budgetary planning for security management, ensuring that senior officials accomplish information security tasks, and ensuring that all personnel are responsible for complying with agency information security programs.
- Changes the reporting guidance focusing on threats, vulnerabilities, incidents, the compliance status of systems at the time of major incidents, and data on incidents involving Personally Identifiable Information.

[2] Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.
[3] Pub. L. No. 113-283. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

- Calls for the revision of OMB Circular A-130[4] to eliminate inefficient or wasteful reporting.
- Provides for the use of automated tools in agencies' information security programs, including periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents.

These changes are intended to improve security by transitioning agencies away from paperwork requirements (*e.g.*, "check-the-box" style of approaches to compliance) toward a more automated and continuous security posture.

Under the new FISMA legislation, agency heads continue to be responsible for submitting an annual report on the adequacy and effectiveness of their information security policies, procedures, and practices to the OMB Director, the Comptroller General of the United States, and selected congressional committees. In addition, agencies continue to be responsible to have an annual independent evaluation of their information security program and practices to determine the effectiveness of such program and practices. Each independent evaluation must include:

- Testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems.
- An assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

For agencies with an Inspector General appointed under the Inspector General Act of 1978,[5] the annual independent evaluation shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency.

FISMA oversight for the Department of the Treasury is performed by the Treasury Inspector General for Tax Administration (TIGTA) and the Treasury Office of the Inspector General (OIG). TIGTA is responsible for oversight of the Internal Revenue Service (IRS), while Treasury OIG is responsible for all other Treasury bureaus. Because of this arrangement, each Inspector General conducts FISMA evaluations on its bureaus and submits separate FISMA reports. However, the OMB requires and expects only one FISMA report to be issued for each department, so coordination is required among both Inspectors General to satisfy this requirement. As a result, 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.

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

[4] OMB, OMB Circular No. A-130 (Revised), *Management of Federal Information Resources* (Nov. 2000).
[5] 5 U.S.C. app. 3 (amended 2008).

period April through August 2015. This report covers the period from July 1, 2014, through June 30, 2015. 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 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 in accordance with FISMA requirements.

The OMB uses annual FISMA metrics to assess the implementation of agency information security capabilities and to measure overall program effectiveness in reducing risks. For Inspectors' General use in assessing Federal agency information security programs, the DHS issued the *Fiscal Year (FY) 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics* on June 19, 2015, which contained 10 information security program areas for Inspectors General to assess.

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 (POA&M).
8. Remote Access Management.
9. Contingency Planning.
10. Contractor Systems.

With the exception of the Continuous Monitoring Management program area, the assessment consisted of two parts: 1) determining if a program was in place for the area and 2) evaluating a combined 83 attributes of those programs. For Continuous Monitoring Management, the Inspectors General were asked to assess the maturity level of this security program area using a maturity model approach. Using the attributes contained within the model, maturity levels from one to five were to be assigned to each of the domains of people, processes, and technology, and the lowest measure assigned to these domains would be given as the overall maturity level for this program. The Information Technology Committee of the Council of Inspectors General on Integrity and Efficiency, in coordination with the DHS, OMB, NIST, and other key stakeholders, developed this maturity model and plans to develop additional maturity models for other FISMA program areas in the coming years.

The Information Security Program Generally Complied With the Federal Information Security Modernization Act

The IRS has established an information security program and related practices in all 10 FISMA program areas. Three of the 10 program areas met all performance attributes specified by the DHS: *Incident Response and Reporting*, *Risk Management*, and *Contingency Planning*. Four other program areas were not fully effective due to two or fewer program attributes that were not met, as follows:

- *Security Training*

  The IRS does not identify and track the status of specialized training for all of its contractor employees with significant information security responsibilities that require specialized training.

- *POA&M*

  The IRS did not always ensure that weaknesses were corrected prior to POA&M closure.

- *Remote Access Management*

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

- *Contractor Systems*

  The IRS did not have sufficient processes to ensure that interfaces between IRS and contractor systems have appropriate agreements.

Significant Improvements Are Needed in Continuous Monitoring Management, Configuration Management, and Identity and Access Management

Significant improvements are needed in three program areas that failed to meet FISMA requirements overall. These program areas were missing many performance attributes specified by the DHS for meeting FISMA requirements.

- *Continuous Monitoring Management*

  The Continuous Monitoring Management program is at a maturity level of one on a scale of one to five. The IRS is still in the process of implementing its Information Security Continuous Monitoring (ISCM) program required by the OMB to automate asset management and maintain secure configuration of these assets in real time. In July 2014, the Department of the Treasury decided to adopt a uniform approach to ISCM across the Department and to use the toolset selected by the DHS to meet the program requirements.

The DHS is in the process of procuring a standard set of cybersecurity tools and services for use by Federal agencies (expected to be completed in August 2015). This toolset will include sensors that perform automated searches for known cyber flaws and send the results to dashboards that inform system managers in real time of cyber risks that need remediation. When implemented, ISCM is intended to provide security automation in 11 domains: Vulnerability Management, Patch Management, Event Management, Incident Management, Malware Detection, Asset Management, Configuration Management, Network Management, License Management, Information Management, and Software Assurance.

- *Configuration Management*

  The Configuration Management program did not meet a majority of the attributes specified by the DHS. Although the IRS has tools and processes that discover assets, evaluate configuration policy, and scan the enterprise to detect vulnerabilities, these processes have not been fully implemented Service-wide, and the IRS still relies on many tedious manual procedures. In addition, the IRS is still working to expand a standard automated process to deploy operating system patches Service-wide. Eventually, the IRS's Configuration Management program will benefit from the implementation of ISCM, which intends to automate configuration management in real time for the universe of the IRS's assets.

- *Identity and Access Management*

  The Identity and Access Management program did not meet a majority of the attributes specified by the DHS, largely due to the IRS not achieving Governmentwide set goals for implementing logical (system) and physical access to facilities in compliance with HSPD-12 requirements. The HSPD-12 requires Federal agencies to issue personal identity verification cards to employees and contractors for accessing agency systems and facilities. The IRS had not resolved existing challenges to achieving full compliance with HSPD-12.

  In mid-June 2015, the Federal Chief Information Officer launched a 30-day Cybersecurity Sprint, instructing Federal agencies to take a number of steps to further protect Federal information and assets and improve the resilience of Federal networks. As part of the Cybersecurity Sprint, agencies were instructed to dramatically accelerate the implementation of personal identity verification card use, especially for privileged users. In response to the Cybersecurity Sprint, the IRS developed a plan in July 2015 to accelerate mandatory personal identity verification card use and begin to address existing challenges related to privileged users and its legacy system environment.

Until the IRS takes steps to improve its security program deficiencies and fully implement all security program areas in compliance with FISMA requirements, taxpayer data will remain vulnerable to inappropriate and undetected use, modification, or disclosure.

Figure 1 presents TIGTA's detailed results for the 10 security program areas in response to the DHS's *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*.[6] TIGTA's results will be consolidated with the Treasury OIG's results of non-IRS bureaus and uploaded into the DHS's CyberScope[7] for the OMB's use in developing its annual report to Congress on the Federal Government's progress in meeting key security performance measures.

Figure 1: TIGTA's Responses to the DHS's FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics

1: Continuous Monitoring Management

Status of Continuous Monitoring Management Program [provide maturity level 1 – 5]	1	**1.1.** Utilizing the ISCM maturity model definitions, in conjunction with the attributes outlined in Appendix A, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall. **TIGTA Comments:** The IRS has not yet implemented its ISCM program but 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.
	1	People
	1	Processes
	1	Technology

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.

[6] 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.
[7] An online data collection tool administered by the DHS to collect performance data for FISMA compliance reporting.

	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 format for all of its information technology assets. The IRS is awaiting the outcome of the DHS's Continuous Diagnostics and Mitigation program Task Order #2 to provide the toolset to meet the program requirements.
	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.** Implemented software assessing (scanning) capabilities. (NIST SP 800-53: RA-5, SI-2) **TIGTA Comments:** The IRS has not implemented software assessment (scanning) on all systems.
	No	**2.1.8.** 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.
	No	**2.1.9.** Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2) **TIGTA Comments:** The IRS has not implemented a Service-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.

	No	**2.3.** Does the organization have an enterprise deviation handling process and is it integrated with the automated capability? **TIGTA Comments:** The IRS does not have an enterprise deviation handling process that is integrated with the automated capability for all of its information technology assets. A number of its assessment activities involve manual processes.
	No	**2.3.1.** Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented. **TIGTA Comments:** The IRS has established a process for accepting the risk introduced by deviations, but it is not integrated with the 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. (HSPD-12, NIST SP 800-53: AC-2) **TIGTA Comments:** The IRS cannot yet uniquely identify all users who access its systems in compliance with HSPD-12.
	No	**3.1.3.** Organization has planned for implementation of personal identity verification 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:** The IRS's plans did not fully address existing challenges relating to privileged user access and its legacy system environment to ensure success in achieving full and timely compliance with HSPD-12 for logical access.

	No	**3.1.4.** Organization has planned for implementation of personal identity verification 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:** The IRS's plans did not fully address existing challenges (including funding challenges) to achieving full and timely compliance with HSPD-12 for physical access.
	No	**3.1.5.** Ensures that the users are granted access based on needs and separation-of-duties principles. **TIGTA Comments:** During FY 2015, the Government Accountability Office (GAO) identified users that had been granted more access than needed and instances in which the separation-of-duties principle was not enforced.
	No	**3.1.6.** Distinguishes hardware assets that have user accounts (*e.g.*, desktops, laptops, servers) from those without user accounts (*e.g.*, Internet Protocol phones, faxes, printers). **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.
	No	**3.1.7.** Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy. **TIGTA Comments:** During FY 2015, the TIGTA and the GAO identified systems that do not have controls in place to ensure that accounts are terminated or deactivated once access is no longer needed.
	No	**3.1.8.** Identifies and controls use of shared accounts. **TIGTA Comments:** During FY 2015, the TIGTA and the GAO identified improper use of shared accounts; for example, use of 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. **TIGTA Comments:** In mid-June 2015, the Federal Chief Information Officer launched a 30-day Cybersecurity Sprint instructing Federal agencies to take a number of steps to further protect Federal information and assets and improve the resilience of Federal networks. As part of the Cybersecurity Sprint, agencies were instructed to dramatically accelerate the implementation of personal identity verification card use, especially for privileged users. In response to the Cybersecurity Sprint, the IRS developed a plan in July 2015 to accelerate mandatory personal identity verification card use and begin to address existing challenges related to privileged users and its legacy system environment.

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.
	Yes	**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)[8]
	Yes	**4.1.4.** When applicable, reports to law enforcement and the agency Inspector General 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 correlating incidents.
	Yes	**4.1.7.** 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.** 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.

[8] NIST, NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide* (Aug. 2012); OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 2006); OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 2007).

	Yes	**5.1.2.** 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	**5.1.3.** 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	**5.1.4.** Has an up-to-date system inventory.
	Yes	**5.1.5.** Categorizes information systems in accordance with Government policies.
	Yes	**5.1.6.** Selects an appropriately tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.
	Yes	**5.1.7.** Implements the approved set of tailored baseline security controls specified in metric 5.1.6.
	Yes	**5.1.8.** 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.
	Yes	**5.1.9.** 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.
	Yes	**5.1.10.** Information system–specific risks (tactical), mission/business–specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.
	Yes	**5.1.11.** Senior officials are briefed on threat activity on a regular basis by appropriate personnel (*e.g.*, Chief Information Security Officer).
	Yes	**5.1.12.** 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	**5.1.13.** Security authorization package contains system security plan, security assessment report, POA&M, and accreditation boundaries in accordance with Government policies for organization information systems. (NIST SP 800-18, 800-37)
	Yes	**5.1.14.** The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.

	Yes	**5.1.15.** For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud 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.

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 does not identify and track the status of specialized training for all of its contractor employees with significant information security responsibilities that require specialized 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 information technology security weaknesses discovered during security control assessments and that require remediation.
	Yes	**7.1.2.** Tracks, prioritizes, and remediates weaknesses.
	No	**7.1.3.** Ensures that remediation plans are effective for correcting weaknesses. **TIGTA Comments:** The IRS did not always ensure that weaknesses were corrected prior to POA&M closure. The 10 systems we evaluated closed a total of 43 POA&Ms during FY 2015. Of the 43 POA&M closures, 22 were closed without sufficient evidence that the weakness was corrected. However, the IRS's POA&M validation processes did not fail the closure of 13 of the 22. The IRS confirmed that five of the 13 POA&Ms had not been corrected, and it could not provide sufficient evidence to support the closure of an additional three. The IRS subsequently uploaded artifacts that justified closure for the remaining five POA&Ms.
	Yes	**7.1.4.** Establishes and adheres to milestone remediation dates and provides adequate justification for missed remediation dates.
	Yes	**7.1.5.** Ensures 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 in terms of dollars. (NIST SP 800-53: PM-3; OMB M-04-25)
	Yes	**7.1.8.** Program officials 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. (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 had 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.** Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. **TIGTA Comments:** The IRS had not fully implemented remote electronic authentication that complies with HSPD-12.
	Yes	**8.1.6.** Defines and implements encryption requirements for information transmitted across public networks.
	Yes	**8.1.7.** Remote access sessions, in accordance to OMB M-07-16, are timed out after 30 minutes of inactivity, after which reauthentication is required.
	Yes	**8.1.8.** Lost or stolen devices are disabled and appropriately reported. (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines)
	Yes	**8.1.9.** Remote access rules of behavior are adequate in accordance with Government policies. (NIST SP 800-53: PL-4)
	Yes	**8.1.10.** 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 and Business Process 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 information technology 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. (FCD1, NIST SP 800-34)
	Yes	**9.1.9.** Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for systems that require them. (FCD1, NIST SP 800-34, NIST SP 800-53)
	Yes	**9.1.10.** Backups of information that are performed in a timely manner. (FCD1, NIST SP 800-34, NIST SP 800-53)
	Yes	**9.1.11.** 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 other Government agencies), including organization systems and services residing in a public cloud, hybrid, or private 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 other Government agencies), including organization systems and services residing in a public cloud, hybrid, or private cloud.
	Yes	**10.1.4.** The inventory identifies interfaces between these systems and organization-operated systems. (NIST SP 800-53: PM-5)
	No	**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. **TIGTA Comments:** The IRS did not have sufficient processes to ensure that interfaces between IRS and contractor systems have appropriate agreements.
	Yes	**10.1.6.** The inventory of contractor systems is updated at least annually.
		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.

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 and their compliance with FISMA requirements for the period July 1, 2014, to June 30, 2015. To accomplish our objective, we responded to the questions provided in the DHS *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, issued on June 19, 2015. The questions related to the following 10 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.

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 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 2015 FISMA evaluation period, as listed in Appendix IV, as well as audit reports from the GAO that contained results applicable to the FISMA questions.

Appendix II

Major Contributors to This Report

Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Midori Ohno, Lead Auditor
Bret Hunter, Senior Auditor
Mary Jankowski, Senior Auditor
Esther Wilson, Senior Auditor
Chinita Coates, 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
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Director, Office of Audit Coordination OS:PPAC:AC
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
- Business Planning and Risk Management OS:CTO:SP:BPRM
- Cybersecurity OS:CTO:C

Appendix IV

Treasury Inspector General for Tax Administration Information Technology Security-Related Reports Issued During the Fiscal Year 2015 Evaluation Period

1. TIGTA, Ref. No. 2014-20-071, *Information Technology: Improvements Are Needed to Successfully Plan and Deliver the New Taxpayer Advocate Service Integrated System* (Sept. 2014).
2. TIGTA, Ref. No. 2014-20-094, *While the Financial Institution Registration System Deployed on Time, Improved Controls Are Needed* (Sept. 2014).
3. TIGTA, Ref. No. 2014-20-063, *Customer Account Data Engine 2 Database Validation Is Progressing; However, Data Coverage, Data Defect Reporting, and Documentation Need Improvement* (Sept. 2014).
4. TIGTA, Ref. No. 2014-20-088, *The Information Reporting and Document Matching Case Management System Could Not Be Deployed* (Sept. 2014).
5. TIGTA, Ref. No. 2014-20-042, *The Internal Revenue Service Should Improve Server Software Asset Management and Reduce Costs* (Sept. 2014).
6. TIGTA, Ref. No. 2014-20-087, *While the Data Loss Prevention Solution Is Being Developed, Stronger Oversight and Process Enhancements Are Needed for Timely Implementation Within Budget* (Sept. 2014).
7. TIGTA, Ref. No. 2014-20-092, *The Internal Revenue Service Does Not Adequately Manage Information Technology Security Risk-Based Decisions* (Sept. 2014).
8. TIGTA, Ref. No. 2014-20-083, *The Internal Revenue Service Should Implement an Efficient Internal Information Security Continuous Monitoring Program That Meets Its Security Needs* (Sept. 2014).
9. TIGTA, Ref. No. 2014-20-059, *The Office of Safeguards Should Improve Management Oversight and Internal Controls to Ensure the Effective Protection of Federal Tax Information* (Sept. 2014).
10. TIGTA, Ref. No. 2014-20-069, *Progress Has Been Made; However, Significant Work Remains to Achieve Full Implementation of Homeland Security Presidential Directive 12* (Sept. 2014).
11. TIGTA, Ref. No. 2015-20-031, *Planning Decisions for Customer Account Data Engine 2 Transition State 2 Should Be Effectively Linked to Actions Needed to Address the Internal Revenue Service's Financial Material Weakness* (May 2015).