Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2013

September 27, 2013

Reference Number: 2013-20-128

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 2013

Highlights

Issued on September 27, 2013

Highlights of Reference Number: 2013-20-128 to the Department of the Treasury, Office of the Inspector General, Assistant Inspector General for Audit.

IMPACT ON TAXPAYERS

The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. The Federal Information Security Management Act (FISMA) was enacted to strengthen the security of information and systems within Federal Government agencies. Until the IRS takes steps to fully implement all 11 security program areas covered by FISMA, taxpayer data will remain vulnerable to inappropriate use, modification, or disclosure, possibly without being detected.

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's information security program for Fiscal Year (FY) 2013.

WHAT TIGTA FOUND

Based on our FY 2013 FISMA evaluation, TIGTA found that nine of 11 security program areas were generally compliant with the FISMA requirements. Six of the nine security program areas included all of the program attributes specified by the Department of Homeland Security's (DHS) *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*:

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

Three of the nine security program areas, while generally compliant, were not fully effective due to one program attribute that was missing or not working as intended:

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

However, two of the 11 security program areas were not compliant with FISMA requirements and did not meet the level of performance specified by the DHS's *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics* due to the majority of the DHS-specified attributes being missing or not working as intended:

- Configuration Management.
- Identity and Access Management.

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 DHS for the applicable FISMA evaluation period.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 27, 2013

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

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2013 (Audit # 201320001)

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 2013. The Act requires the agency's Inspector General to perform an annual independent evaluation of the agency's information security program and practices to determine the effectiveness of such program and practices.

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 Alan R. Duncan, 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
CM	Continuous Monitoring
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
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 Internal Revenue Service (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. Otherwise, taxpayers could be exposed to invasion of privacy and financial loss or damage from identity theft or other financial crimes.

The Federal Information Security Management Act (FISMA) of 2002[1] was enacted to strengthen the security of information and systems within Federal agencies. Under the FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of the FISMA, related Office of Management and Budget (OMB) policies, and National Institute of Standards and Technology (NIST) procedures, standards, and guidelines.

One of the provisions of the FISMA requires the agencies to have an annual independent evaluation of their information security programs and practices performed by the agency Inspector General or an independent external auditor as determined by the Inspector General.[2] The OMB uses the information from the agencies and independent evaluations in its FISMA oversight capacity to assess agency-specific and Federal Governmentwide security performance, develop its annual security report to Congress, and assist in improving and maintaining adequate agency security performance.

In July 2010, the OMB delegated its responsibility to the Department of Homeland Security (DHS) for the collection of annual FISMA responses.[3] The DHS issued the *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics* on November 30, 2012, for Fiscal Year[4] (FY) 2013 FISMA responses. These reporting metrics specified the security program areas for the Inspectors General to evaluate and listed specific attributes that each security program area should include. Detailed information on our audit

[1] Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.
[2] The FISMA evaluation period for the Department of the Treasury is July 1, 2012, through June 30, 2013.
[3] In OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*, OMB delegated the responsibility for various operational aspects of Federal cyber security to the DHS, including overseeing the agencies' compliance with the FISMA and developing analyses for the OMB to assist in the development of the FISMA annual report.
[4] A 12-consecutive-month period ending on the last day of any month. The Federal Government's fiscal year begins on October 1 and ends on September 30.

objective, scope, and methodology is presented in Appendix I. Major contributors to this 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

The DHS *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics* that were issued on November 30, 2012, specified 11 information security program areas and a total of 98 attributes within the 11 areas for the Inspectors General to evaluate and determine compliance with FISMA requirements. The 11 information security program areas are as follows:

- Continuous Monitoring Management.
- Configuration Management.
- Identity and Access Management.
- Incident Response and Reporting.
- Risk Management.
- Security Training.
- Plan of Action and Milestones (POA&M).
- Remote Access Management.
- Contingency Planning.
- Contractor Systems.
- Security Capital Planning.

To complete our FISMA evaluation, we reviewed a representative judgmental sample[5] of 10 major IRS information systems. For each system in the sample, we assessed the risk management process, the annual testing of controls for continuous monitoring, the testing of information technology contingency plans, and the plan of action and milestones process. In addition, we evaluated the IRS's enterprise-level processes over configuration management, identity and access management, incident response and reporting, security training, remote access management, contractor systems, and security capital planning. During the FY 2013 FISMA evaluation period, we also completed seven audits, as shown in Appendix IV, which evaluated various aspects of information security at the IRS. We considered the results of these

[5] A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.

audits in our evaluation, as well as results from ongoing audits for which draft reports were issued to the IRS by August 8, 2013.

Based on our FY 2013 FISMA evaluation, we determined that nine of the 11 security program areas were generally compliant with the FISMA requirements. The following six security program areas included all of the program attributes specified by the DHS's *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*:

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

The following three security program areas, while generally compliant, were not fully effective due to one program attribute that was missing or not working as intended:

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

However, two security program areas were not compliant with FISMA requirements and did not meet the level of performance specified by the DHS's *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics* due to the majority of the DHS-specified attributes being missing or not working as intended:

- Configuration Management.
- Identity and Access Management

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

The following matrix[6] presents TIGTA's results for the 11 security program areas as specified by the DHS's *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*. We have provided comments to support the "no" responses. TIGTA's results will be

[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.

consolidated with the Department of the Treasury Office of Inspector General's results of non-IRS bureaus and reported to the OMB.

1: Continuous Monitoring

Status of Continuous Monitoring Program [check one: Yes or No]	Yes	**1.1.** Has the organization established an enterprisewide 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 and plans for continuous monitoring (NIST SP 800-37 Rev 1, Appendix G).
	Yes	**1.1.3.** 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 800-53A).
	Yes	**1.1.4.** Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as 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. TIGTA Comments: The IRS's annual assessments of system security controls are predominantly manual. The IRS's strategy for automating continuous monitoring includes the implementation of a tool called Archer, which will be a central repository and analysis engine for assessment results, such as automated vulnerability scans. Archer is in its initial development phases.

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. During FY 2013, the IRS was in the process of implementing the Security Compliance Posture Monitoring and Reporting application, which is intended to provide the ability to assess compliance with baseline security controls in a SCAP-compliant format on an enterprisewide level; however, its implementation has been delayed.
	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 vulnerability scanning tools and processes on all systems to ensure timely remediation of scan result deviations. Also, the IRS processes to share vulnerability information to system owners and administrators are still under development.
	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. During FY 2013, the Enterprise Services organization was in the process of implementing the Enterprise Configuration Management System to provide an enterprise solution for configuration and change management.
	No	**2.1.7.** Process for the timely and secure installation of software patches. TIGTA Comments: The IRS has not yet fully implemented a process to ensure timely and secure installation of software patches. During FY 2013, the IRS was in the process of evaluating tools that have the capability to perform automated patch management activities across a multitude of technologies and feed results to a centralized location. During the FY 2013 FISMA evaluation period, TIGTA and the Government Accountability Office (GAO) identified critical patches that were missing or installed in an untimely manner on IRS computers.
	No	**2.1.8.** Software assessing (scanning) capabilities are fully implemented. (NIST SP 800-53: RA-5, SI-2) TIGTA Comments: Monthly vulnerability scans are not being 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 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. During the FY 2013 FISMA evaluation period, TIGTA and the GAO identified servers that were not consistently configured to have strong controls.
	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 yet implemented a process to ensure timely and secure installation of software patches. During FY 2013, the IRS was in the process of evaluating tools that have the capability to perform automated patch management activities across a multitude of technologies and feed results to a centralized location. During FY 2013, TIGTA and the GAO identified critical patches that were missing or installed in an untimely manner on IRS computers.
		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.

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 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: The IRS has not fully implemented unique user identification that complies with Homeland Security Presidential Directive-12 (HSPD-12). In addition, five of our 10 sampled systems did not have the NIST SP 800-53 AC-2 security control in place.
	No	**3.1.3.** Identifies when special access requirements (*e.g.*, multifactor authentication) are necessary. TIGTA Comments: The IRS did not fully implement 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: Although the IRS is working to achieve its goal of 85 percent mandatory PIV use by the end of Calendar Year 2013, considerable challenges still exist for achieving full compliance due to its legacy environment.
	Yes	**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)
	No	**3.1.7.** Ensures that the users are granted access based on needs and separation-of-duties principles. TIGTA Comments: During FY 2013, TIGTA and 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. (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: During FY 2013, the IRS was still in the process of implementing tools to achieve automated asset discovery and asset management.
	Yes	**3.1.9.** Identifies all user and non-user 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: During FY 2013, 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.
	Yes	**3.1.11.** Identifies and controls use of shared accounts.

		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 due to resource constraints.
	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 organizationwide 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 at 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.

6: Security Training

Status of Security Training Program [check one: Yes or No]	Yes	**6.1** Has the organization established a security training 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	**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 did not track completions of specialized information technology security training by contractors during the FY 2013 FISMA evaluation period.
	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: 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: 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. In addition, virtual private network server components do not comply with password requirements.
	Yes	**8.1.4.** Telecommuting policy is fully developed. (NIST SP 800-46, Section 5.1)
	Yes	**8.1.5.** If applicable, multifactor authentication is required for remote access. (NIST SP 800-46, Section 2.2, Section 3.3)
	Yes	**8.1.6.** Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.
	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 re-authentication 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 enterprisewide 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 exercises 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 that was not noted in the questions above.

10: Contractor Systems

Status of Contractor Systems [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 2013, the IRS maintained two contractor managed systems in the Trusted Agent FISMA, the U.S. Department of the Treasury's system for reporting FISMA data. The IRS also maintained a list of 130 contractor sites in FY 2013 that required annual security reviews because each handles or processes IRS information. The IRS Infrastructure and Security Review organization conducts reviews to ensure that security controls and standards are met and issues reports of findings to these contractors.
	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) 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 that was not noted in the questions above.

11: Security Capital Planning

Status of Security Capital Planning [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 that was not noted in the questions above.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to provide an annual independent evaluation of the effectiveness of the IRS's information technology security program and practices, and to assess the progress made by the IRS in meeting the responsibilities established by the NIST and the OMB. The following 11 evaluative sections are taken directly from the DHS *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*, issued on November 30, 2012.

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.

To accomplish our objective, we reviewed a judgmental sample[1] of 10 major IRS information systems from a total of 75 major applications maintained in the Trusted Agent FISMA system as of April 11, 2013. We selected a judgmental sample because we did not plan to project the results. We conducted tests to determine the appropriate level of performance that the IRS has achieved for each of the security program areas. We also evaluated completed TIGTA work during the FISMA period, as well as audits from the GAO, and determined its applicability to the FISMA questions.

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 2013 Inspector General Federal Information Security Management Act Reporting Metrics*. The Department of the Treasury Office of Inspector General will combine

[1] A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.

our results for the IRS with its results for the non-IRS bureaus and submit the combined yes or no responses to OMB.

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
Charles Ekunwe, Senior Auditor
Bret Hunter, Senior Auditor
Mary Jankowski, Senior Auditor
Esther Wilson, Senior Auditor
Tina Wong, Senior Auditor

Appendix III

Report Distribution List

Acting Commissioner
Office of the Commissioner – Attn: Chief of Staff C
Office of the Deputy Commissioner for Services and Enforcement SE
Deputy Commissioner for Operations Support OS
Chief Technology Officer OS:CTO
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM

Appendix IV

Treasury Inspector General for Tax Administration Information Technology Security-Related Reports Issued During the Fiscal Year 2013 Evaluation Period

1. TIGTA, Ref. No. 2012-20-099, *Audit Trails Did Not Comply With Standards or Fully Support Investigations of Unauthorized Disclosure of Taxpayer Data* (Sept. 2012).
2. TIGTA, Ref. No. 2012-20-112, *An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers* (Sept. 2012).
3. TIGTA, Ref. No. 2012-20-109, *The Customer Account Data Engine 2 Database Was Initialized; However, Database and Security Risks Remain, and Initial Timeframes to Provide Data to Three Downstream Systems May Not Be Met* (Sept. 2012).
4. TIGTA, Ref. No. 2012-20-115, *Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected* (Sept. 2012).
5. TIGTA, Ref. No. 2013-20-016, *Significant Delays Hindered Efforts to Provide Continuous Monitoring of Security Settings on Computer Workstations* (Jan. 2013).
6. TIGTA, Ref. No. 2013-20-023, *Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process* (Feb. 2013).
7. TIGTA, Ref. No. 2013-20-030, *Integrated Financial System Updates Are Improving System Security, but Remaining Weaknesses Should Be Addressed* (Mar. 2013).