TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

# *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2016*

**September 28, 2016**

**Reference Number: 2016-20-092**

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*


**To report fraud, waste, or abuse, call our toll-free hotline at:**

1-800-366-4484

**By Web**:

***www.treasury.gov/tigta/***

**Or Write:**

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

**TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION – FEDERAL INFORMATION SECURITY MODERNIZATION ACT REPORT FOR FISCAL YEAR 2016**

# Highlights

**Final Report issued on September 28, 2016**

Highlights of Reference Number: 2016-20-092 to the Department of the Treasury, Office of the Inspector General, Assistant Inspector General for Audit.

## IMPACT ON TAXPAYERS

The Federal Information Security Modernization Act of 2014 (FISMA) focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. As a custodian 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 Inspector Generals 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 2016.

## WHAT TIGTA FOUND

The IRS's information security program was generally in alignment with FISMA requirements, but it was not fully effective due to program attributes not yet implemented. Based on the Department of Homeland Security's (DHS) scoring methodology for the Fiscal Year 2016 FISMA evaluation period, four Cybersecurity Framework functions (*Identify*, *Protect*, *Detect*, and *Respond*) were rated as "not effective" and one security function (*Recover*) was rated as "effective." Within the Cybersecurity Framework functions, three security program areas (*Contractor Systems, Security and Privacy Training,* and *Contingency Planning*) met all the FISMA performance attributes specified by the DHS. The security program area *Risk Management* met most of the performance attributes. Based on the maturity model issued in the Fiscal Year 2016 FISMA evaluation period, the security program area *Incident Response* was rated at level four on a scale of one to five.

However, significant improvements are needed in three program areas that were rated as "not effective" and were missing many performance attributes specified by the DHS for meeting FISMA requirements. These security program areas were *Information Security Continuous Monitoring*, *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 DHS for the applicable FISMA evaluation period.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 28, 2016

**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 Report – Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2016 (Audit # 201620001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Modernization Act[1] (FISMA) evaluation of the Internal Revenue Service (IRS) for Fiscal Year 2016. The FISMA requires Federal agencies to have an annual independent evaluation performed of their information security programs and practices and to report the results of the evaluation to the Office of Management and Budget. Our overall objective was to assess the effectiveness of the IRS's information security program and practices for the period July 1, 2015, to June 30, 2016, and to evaluate the IRS's compliance with the FISMA and related information security policies, procedures, standards, and guidelines.

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 being sent to the IRS managers affected by the report.

If you have any questions, please contact me or Danny R. 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

| | |
|---|---|
| CF | Cybersecurity Framework |
| CIO | Chief Information Officer |
| DHS | Department of Homeland Security |
| FCD1 | Federal Continuity Directive 1 |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Modernization Act |
| FY | Fiscal Year |
| GAO | Government Accountability Office |
| IRS | Internal Revenue Service |
| ISCM | Information Security Continuous Monitoring |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| PIV | Personal Identity Verification |
| PMC | President's Management Council |
| POA&M | Plan of Action and Milestones |
| SP | Special Publication |
| TIC | Trusted Internet Connection |
| TIGTA | Treasury Inspector General for Tax Administration |
| US-CERT | United States Computer Emergency Readiness Team |

# Background

The Federal Information Security Modernization Act of 2014,[1] commonly referred to as the FISMA, focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. The FISMA requires Federal agencies to develop, document, and implement an agencywide 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. It assigns specific responsibilities to agency heads and Inspectors General in complying with requirements of the FISMA. The FISMA is supported by the Office of Management and Budget (OMB), Department of Homeland Security (DHS), agency security policy, and risk-based standards and guidelines published by the National Institute of Standards and Technology (NIST) related to information security practices.

***As a custodian 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 Internal Revenue Service (IRS) collects and maintains a significant amount of personal and financial information on each taxpayer. As a custodian 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. 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 and related OMB policies and NIST procedures, standards, and guidelines. The FISMA directs Federal agencies to report annually to the OMB Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with the FISMA. The DHS is responsible for the operational aspects of Federal cybersecurity, such as establishing governmentwide incident response and operating the tool to collect FISMA metrics. 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

[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.

General. The OMB uses annual FISMA metrics to assess the implementation of agency information security capabilities and to measure overall program effectiveness in reducing risks.

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. TIGTA is responsible for oversight of the IRS, while the Treasury Office of the Inspector General 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 Office of the Inspector General, which will then combine the results for all the Treasury bureaus into one report for the OMB.

The DHS issued the *Fiscal Year (FY)*[2] *2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*[3] with three significant changes from the prior year.

1) The DHS organized the FY 2016 Inspector General FISMA Reporting Metrics around the five information security functions outlined in the NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework (CF)):[4] *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*. Eight security program areas evaluated in prior FISMA evaluations were aligned within the CF functions and include *Risk Management*, *Contractor Systems*, *Configuration Management*, *Identity and Access Management*, *Information Security Continuous Monitoring*, *Incident Response*, *Security and Privacy Training*, and *Contingency Planning*.

2) The DHS implemented a new scoring methodology. Agencies are allotted points for each CF function area based on their achievement of a five-level scale of maturity. The scale, from lowest to highest, includes: *Ad Hoc* (Level 1), *Defined* (Level 2), *Consistently Implemented* (Level 3), *Managed and Measurable* (Level 4), and *Optimized* (Level 5).

   Agencies with programs that score at or above the *Managed and Measureable* level for a CF function are considered to have "effective" programs within that area in accordance with the definition of effectiveness in NIST Special Publication (SP) 800-53.[5] To score

[2] Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
[3] DHS, *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (Version 1.1.2, Sep. 2016).
[4] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, Feb. 2014).
[5] The Inspector General FISMA metrics leverage NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013, updated Jan. 2015), which defines security control effectiveness as the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies.

at or above the *Managed and Measurable* level, all metrics designated *Defined* and *Consistently Implemented* must be met, plus half or more of metrics designated as *Managed and Measureable* must be met. See Figure 1 for a description of these maturity levels.

3) The DHS, in coordination with other key stakeholders, continued the effort begun in 2015 to develop specific maturity models for various security program areas. In addition to the *Information Security Continuous Monitoring* maturity model, which was included in the FY 2015 Inspector General FISMA Reporting Metric, the FY 2016 Inspector General FISMA Reporting Metrics included a maturity model for the *Incident Response* program area.

**Figure 1: DHS Maturity Level Descriptions**

| Maturity Level | Maturity Level Description |
|---|---|
| Level 1: ***Ad-Hoc*** | For the **Identify**, **Protect**, **and Recover** function areas, has not met at least half of all metrics designated as *Defined*.<br><br>For the **Detect** and **Respond** function areas, has not met at least half of all metrics designated in the *Ad-Hoc* level. |
| Level 2: ***Defined*** | For the **Identify**, **Protect**, **and Recover** function areas, has met half or greater of all metrics designated as *Defined*.<br><br>For the **Detect** and **Respond** function areas, has met all metrics designated in the *Ad-Hoc* level and half or greater of the metrics designated in the *Defined* level. |
| Level 3: ***Consistently Implemented*** | For all function areas, met all metrics designated at the *Defined* level and half or greater of the metrics designated at the *Consistently Implemented* level. |
| Level 4: ***Managed and Measurable*** | For all function areas, met all metrics designated in the *Consistently Implemented* level and half or greater of the metrics designated at the *Managed and Measurable* level. |
| Level 5: **Optimized** | For all function areas, met all metrics designated in the *Managed and Measurable* and *Optimized* levels. |

*Source: DHS's FY 2016 Inspector General FISMA Reporting Metrics.*

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 2016. This report covers the period from July 1, 2015, through June 30, 2016. 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 Information Security Program Is Generally Aligned With the Federal Information Security Modernization Act, but It Is Not Fully Effective Due to Program Attributes Not Yet Implemented

To determine the effectiveness of the IRS's information security program, we evaluated whether the IRS had implemented the attributes that the DHS had specified for each security function area. We based our work, in part, on a representative subset of 10 IRS information systems and the implementation status of key security controls. We also considered the results of TIGTA and Government Accountability Office (GAO) reports issued during the FY 2016 FISMA evaluation period that contained results applicable to the FISMA questions, as listed in Appendix IV.

The IRS has established an information security program that is generally aligned with applicable FISMA requirements, OMB policy and guidance, and the NIST standards and guidelines. However, due to program attributes not yet implemented, the IRS's information security program is not fully effective. Based on the DHS's scoring methodology for the FY 2016 FISMA evaluation period, three CF functions are rated as "not effective" and two security functions are rated as "effective," as shown in Figure 2.

### Figure 2: Security Function Effectiveness Based on Implementation of DHS-Specified Attributes

| Cybersecurity Framework Security Function | FY 2016 Inspector General FISMA Reporting Metric Domains | Effective Security Function |
|---|---|---|
| **Identify** | • *Risk Management* (met 13 of 16 attributes)<br>• *Contractor Systems* (met all attributes) | No |
| **Protect** | • *Configuration Management* (did not meet a majority of attributes)<br>• *Identity and Access Management* (did not meet a majority of attributes)<br>• *Security and Privacy Training* (met all attributes) | No |
| **Detect** | • *Information Security Continuous Monitoring* (maturity model level of two) | No |
| **Respond** | • *Incident Response* (maturity model level of four) | Yes |
| **Recover** | • *Contingency Planning* (met all attributes) | Yes |

*Source: TIGTA's evaluation of security program attributes as presented in Figure 3, which determined whether security functions were rated "effective" or "not effective."*

## Some security program areas met all or most attributes

Three security program areas met all performance attributes specified by the DHS.

- ***Contractor Systems***

  The *Contractor Systems* security program area met all performance attributes specified by the DHS, despite being aligned with the *Identify* function that was scored as "not effective."

- ***Security and Privacy Training***

  The *Security and Privacy Training* program area met all performance attributes specified by the DHS, despite being aligned with the *Protect* function that was scored as "not effective."

- ***Contingency Planning***

  The *Contingency Planning* security program area, aligned with the *Recover* function, met all performance attributes specified by the DHS.

One security program area, *Risk Management*, needed improvement on three of 16 attributes.

- ***Risk Management***
  - The IRS did not have sufficient processes in place to ensure that system interconnections in use at the IRS had proper authorization or security agreements. (Metric 1.1.9) During a prior review, TIGTA identified[6] that the IRS did not have sufficient processes in place to ensure that interconnections in use at the IRS had proper authorization or security agreements. After the end of the FY 2016 FISMA evaluation period, the IRS informed us that it had completed all corrective actions. We have not verified those completed corrective actions.
  - Plans of Action and Milestones (POA&M) were not always maintained and reviewed to ensure that they were effective for correcting security weaknesses. (Metric 1.1.13) The IRS informed us that it has taken steps to remediate the POA&M consistency and accuracy issues by centralizing POA&M oversight and validation work under the IRS Enterprise FISMA Services office.
  - The IRS has not yet implemented an insider threat detection and prevention program. (Metric 1.1.16)

[6] TIGTA, Ref. No. 2015-20-087, *Improvements Are Needed to Ensure That External Interconnections Are Identified, Authorized, and Secured* (Sept. 2015).

One security program area, *Incident Response*, was rated at level four on the scale of one to five.

- ***Incident Response***

  The IRS has formalized its incident response program through the development of comprehensive incident response policies, plans, and procedures consistent with FISMA, NIST standards, and OMB guidance. Based on the maturity model issued in the FY 2016 Inspector General FISMA Reporting Metrics for this program area, the IRS's incident response program has achieved a maturity level of four, *Managed and Measurable*, on the scale of one to five. The IRS successfully demonstrated all nine of the level four attributes. However, TIGTA provided a comment on one metric (Metric 4.3.1.2) related to ensuring that key incident response personnel have the appropriate knowledge, skills, and abilities to successfully operate this mission-critical program.

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

Significant improvements are needed in three program areas that were rated as "not effective" and were missing many performance attributes specified by the DHS for meeting FISMA requirements.

- ***Information Security Continuous Monitoring (ISCM)***

  The *Information Security Continuous Monitoring* program area is at a maturity level of two (*Defined*) on the DHS's scale of one to five. The OMB requires Federal agencies to implement an ISCM program that automates asset management and maintains secure configuration of assets in real time. In July 2014, the Department of the Treasury decided to adopt a uniform approach to ISCM across the Treasury 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. 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. The IRS is working in concert with the DHS's implementation phases, and currently performs ISCM-related activities using numerous templates and tools deployed within the enterprise.

- ***Configuration Management***

  The *Configuration Management* program area did not meet the majority of the attributes specified by the DHS. The IRS has established standard baseline configurations for information systems and system components. In addition, the IRS uses automated compliance tools to scan for improper configurations, vulnerabilities, and software flaws. However, deficiencies continue to exist in ensuring baseline configurations are maintained and reported vulnerabilities are corrected timely. 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 area will benefit from the implementation of ISCM, which intends to use automation to produce an accurate inventory of devices and software on the IRS network and to automate configuration management of these devices and software in near real time.

- ***Identity and Access Management***

  The *Identity and Access Management* program area did not meet a majority of the attributes specified by the DHS. The IRS has made progress in implementing use of personal identity verification (PIV) cards for network and remote access in compliance with Homeland Security Presidential Directive 12,[7] but more work is needed to enforce PIV card access to systems and for physical access to IRS facilities.

  Also, the IRS has not consistently implemented controls to ensure that:

  - Users are not granted more access than they need.
  - The use of administrative privileges is tracked and periodically reviewed.
  - Accounts are terminated when no longer required.
  - The use of shared accounts is controlled.

Until the IRS takes steps to improve its security program area 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.

The details of our yes/no responses to the FY 2016 Inspector General FISMA Reporting Metrics for the various program areas are contained in Figure 3.

[7] Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, was signed by President Bush on August 27, 2004. This directive established a new standard for issuing and maintaining identification badges for Federal employees and contractors entering Government facilities and accessing computer systems. The intent was to improve security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Agencies are required to use PIV badges (also referred to as SmartID cards) to access computer systems (logical access).

## Figure 3: TIGTA's Responses to the DHS's FY 2016 Inspector General FISMA Reporting Metrics

| **1.0 Identify** **Status of Risk Management Program** | **Maturity Model Indicator** | ***Risk Management* (*Identify*)** |
|---|---|---|
| Yes | Level 2: Defined | **1.1** Has the organization established a risk management program that includes comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? |
| Yes | Level 2: Defined | **1.1.1** Identifies and maintains an up-to-date system inventory, including organization- and contractor-operated systems, hosting environments, and systems residing in the public, hybrid, or private cloud. (FY 2016 CIO FISMA Metrics 1.1, NIST CF ID.AM.1, NIST SP 800-53: PM-5)[8] |
| Yes | Level 3: Consistently Implemented | **1.1.2** Develops a risk management function that is demonstrated through the development, implementation, and maintenance of a comprehensive governance structure and organizationwide risk management strategy as described in NIST SP 800-37. (NIST SP 800-39)[9] |
| Yes | Level 3: Consistently Implemented | **1.1.3** Incorporates mission and business process-related risks into risk-based decisions at the organizational perspective, as described in NIST SP 800-37. (NIST SP 800-39) |
| Yes | Level 3: Consistently Implemented | **1.1.4** Conducts information system–level risk assessments that integrate risk decisions from the organizational and mission/business process perspectives and take into account threats, vulnerabilities, likelihood, impact, and risks from external parties and common control providers. (NIST SP 800-37, Rev. 1, NIST SP 800-39, NIST SP 800-53: RA-3) |
| Yes | Level 4: Managed and Measurable | **1.1.5** Provides timely communication of specific risks at the information system, mission/business, and organization-level to appropriate levels of the organization. |

[8] DHS and Executive Office of the President of the United States, *FY 2016 CIO FISMA Metrics* (Version 1.00, Oct. 2015). Note: CIO is Chief Information Officer.
[9] NIST, NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (Feb. 2010, updated June 2014). NIST, NIST SP 800-39 Rev. 1, *Managing Information Security Risk: Organization, Mission, and Information System View* (Mar. 2011).

| **1.0 Identify**<br>**Status of Risk Management Program** | **Maturity Model Indicator** | ***Risk Management* (*Identify*)** |
|---|---|---|
| Yes | Level 3: Consistently Implemented | **1.1.6** Performs comprehensive assessments to categorize information systems in accordance with Federal standards and applicable guidance. (Federal Information Processing Standards (FIPS) 199, FIPS 200, the FISMA, Cybersecurity Sprint, OMB M-16-04, President's Management Council (PMC) cybersecurity assessments)[10] |
| Yes | Level 2: Defined | **1.1.7** Selects an appropriately tailored set of baseline security controls based on mission/business requirements and policies and develops procedures to employ controls within the information system and its environment of operation. |
| Yes | Level 3: Consistently Implemented | **1.1.8** Implements the tailored set of baseline security controls as described in 1.1.7. |
| No | Level 4: Managed and Measurable | **1.1.9** Identifies and manages risks with system interconnections, including through authorizing system interconnections, documenting interface characteristics and security requirements, and maintaining interconnection security agreements. (NIST SP 800-53: CA-3)<br>**TIGTA Comments:** During a prior review, TIGTA identified[11] that the IRS did not have sufficient processes in place to ensure that interconnections in use at the IRS had proper authorization or security agreements. After the end of the FY 2016 FISMA evaluation period, the IRS informed us that it had completed all corrective actions. We have not verified those completed corrective actions. |
| Yes | Level 3: Consistently Implemented | **1.1.10** Continuously assesses the security controls, including hybrid and shared 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. |

[10] NIST, FIPS Pub. 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004). NIST, FIPS Pub. 200, *Minimum Security Requirements for Federal Information and Information Systems* (Mar. 2006). OMB, OMB M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* (Oct. 2015).
[11] TIGTA, Ref. No. 2015-20-087, *Improvements Are Needed to Ensure That External Interconnections Are Identified, Authorized, and Secured* (Sept. 2015).

| **1.0 Identify**<br>**Status of Risk Management Program** | **Maturity Model Indicator** | ***Risk Management* (*Identify*)** |
|---|---|---|
| Yes | Level 4: Managed and Measurable | **1.1.11** Maintains ongoing information system authorizations 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 (OMB M-14-03, NIST *Supplemental Guidance on Ongoing Authorization*).[12] |
| Yes | Level 4: Managed and Measurable | **1.1.12** Security authorization package contains system security plan, security assessment report, and POA&M that are prepared and maintained in accordance with government policies. (NIST SP 800-18, NIST SP 800-37)[13] |
| No | Level 3: Consistently Implemented | **1.1.13** POA&Ms are maintained and reviewed to ensure they are effective for correcting security weaknesses.<br>**TIGTA Comments:** The IRS did not consistently implement its policies and procedures to maintain and review POA&Ms to ensure that they were effective for correcting security weaknesses.<br>• The IRS did not timely create POA&Ms for 24 (52 percent) of 46 weaknesses. The 46 weaknesses were the total number of weaknesses reported during the FY 2016 annual security assessment reviews for the 10 IRS systems we selected for the FY 2016 annual FISMA evaluation of the IRS.<br>• The IRS closed five (40 percent) of 12 POA&Ms without sufficient support that the weaknesses were corrected. The 12 POA&Ms were the total number of POA&Ms closed by the 10 selected systems during the FY 2016 FISMA evaluation period. The IRS subsequently provided adequate documentation for three of the five to support that the weaknesses had been effectively corrected. The documentation subsequently provided by the IRS for the remaining two did not support that the weaknesses had been corrected.<br>• In other audit work during FY 2016, TIGTA identified that 25 of 63 POA&Ms reviewed did not meet IRS POA&M standards to ensure effective and timely resolution of the weakness. We reviewed all 63 POA&Ms that had been prepared for security control weaknesses related to IRS's external file transfer solutions. Of the 25 POA&Ms that did not meet IRS policy standards, 22 POA&Ms did not contain sufficiently defined or detailed milestone actions to ensure timely resolution of the weakness and three POA&Ms did not address the |

[12] OMB, OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems* (Nov. 2013). NIST, *Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management* (June 2014).
[13] NIST, NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems* (Feb. 2006).

| **1.0 Identify**<br>**Status of Risk Management Program** | **Maturity Model Indicator** | ***Risk Management* (*Identify*)** |
|---|---|---|
| | | weakness. The scheduled completion date for eight of the 22 POA&Ms lacking sufficient milestone actions had passed with the weaknesses remaining uncorrected.<br>• The IRS Enterprise FISMA Dashboard reported that, as of June 30, 2016, 14 percent of the IRS's total open POA&Ms have passed scheduled completion dates and therefore are in late status. The IRS's goal was to have less than 10 percent of its open POA&Ms in late status. This indicates that the IRS has not yet consistently implemented its policies and procedures to ensure timely and effective correcting of security weaknesses.<br>The IRS informed us that it has taken steps to remediate the POA&M consistency and accuracy issues by centralizing POA&M oversight and validation work under the IRS Enterprise FISMA Services office. |
| Yes | Level 4: Managed and Measurable | **1.1.14** Centrally tracks, maintains, and independently reviews/validates POA&M activities at least quarterly. (NIST SP 800-53: CA-5, OMB M-04-25)[14] |
| Yes | Level 4: Managed and Measurable | **1.1.15** 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. |
| No | Level 3: Consistently Implemented | **1.1.16** Implemented an insider threat detection and prevention program, including the development of comprehensive policies, procedures, guidance, and governance structures, in accordance with Executive Order 13587 and the National Insider Threat Policy.[15] (PMC, NIST SP 800-53: PM-12)<br>**TIGTA Comments:** The IRS does not have an insider threat detection and prevention program. Although the IRS does not own or operate any classified national security information systems subject to Executive Order 13587, its own policy requires that it implement an insider threat program. In addition, the IRS is waiting for the Department of the Treasury, which is subject to Executive Order 13587, to release its Insider Threat Program to assist in identifying potential insider threats and establish reporting requirements and thresholds for the Treasury bureaus. However, the IRS indicated that its current resources and budget do not allow for a full-scale implementation of |

[14] OMB, OMB M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* (Aug. 2004).
[15] Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (Oct. 2011). The White House, Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 2012).

| **1.0 Identify**<br>**Status of Risk Management Program** | **Maturity Model Indicator** | ***Risk Management* (*Identify*)** |
|---|---|---|
| | | an insider threat program until 2027. As such, the IRS has taken a risk-based decision to not meet this policy requirement at this time. |
| Not Effective | | **1.1.17** Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Based on all testing performed, is the risk management program effective?<br>**TIGTA Comments:** According to the new scoring methodology implemented by the DHS for the FY 2016 Inspector General FISMA Reporting Metrics, program areas must have met all attributes labeled as *Defined* and *Consistently Implemented* and half or more of the attributes labeled as *Managed and Measurable* to have an effective program. This program area did not meet all attributes at the level 3 *Consistently Implemented*. |

| **1.0 Identify**<br>**Status of Contractor Systems Program** | **Maturity Model Indicator** | ***Contractor Systems* (*Identify*)** |
|---|---|---|
| Yes | Level 2: Defined | **1.2** Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including other government agencies, managed hosting environments, and systems and services residing in a cloud external to the organization that is inclusive of policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? |
| Yes | Level 3: Consistently Implemented | **1.2.1** Establishes and implements a process to ensure that contracts/statements of work/solicitations for systems and services, include appropriate information security and privacy requirements and material disclosures, Federal Acquisition Regulation clauses, and clauses on protection, detection, and reporting of information. (Federal Acquisition Regulation Case 2007-004, Common Security Configurations,[16] Federal Acquisition Regulation Sections 24.104, 39.101, 39.105, 39.106, and 52.239-1, PMC, FY 2016 CIO FISMA Metrics 1.8, NIST SP 800-53: SA-4, Federal Risk and Authorization Management Program standard contract clauses, Cloud Computing Contract Best Practices)<br>**TIGTA Comments:** The IRS has recently established a process for reviewing contracts for appropriate security clauses. In November 2015, the |

[16] Federal Acquisition Regulation, FAR Case 2007-004, Common Security Configurations (Mar. 2008)

| **1.0 Identify Status of Contractor Systems Program** | **Maturity Model Indicator** | ***Contractor Systems* (*Identify*)** |
|---|---|---|
| | | IRS instructed its contracting officers to conduct a 100 percent review of all new and existing information technology and service contracts to ensure that all applicable security clauses were included. In June 2016, the IRS instructed its contracting officers to implement codes in the IRS procurement system to indicate whether the contract had been reviewed and includes security clauses if appropriate. The IRS Procurement staff stated that the IRS intends to begin reviewing the progress made to ensure that all contracts include appropriate security clauses on a quarterly basis. As of June 30, 2016, the IRS reported the following results.<br>• 808 contracts that have been reviewed contain appropriate security clauses.<br>• 2,095 contracts that have been reviewed do not require security clauses.<br>• 842 contracts that have been reviewed do not yet contain appropriate security clauses.<br>• 1,844 contracts have not yet been reviewed. (All are active contracts with signed dates on or after July 1, 2016.) |
| Yes | Level 3: Consistently Implemented | **1.2.2** Specifies within appropriate agreements how information security performance is measured, reported, and monitored on contractor- or other entity-operated systems. (CIO and Chief Acquisition Officers Councils' Best Practices Guide for Acquiring IT As a Service, NIST SP 800-35)[17] |
| Yes | Level 3: Consistently Implemented | **1.2.3** Obtains sufficient assurance that the security controls of systems operated on the organization's behalf by contractors or other entities and services provided on the organization's behalf meet FISMA requirements, OMB policy, and applicable NIST guidelines. (NIST SP 800-53: CA-2 and SA-9) |
| Effective | | **1.2.4** Provide any additional information on the effectiveness (positive or negative) of the organization's contractor systems program that was not noted in the questions above. Based on all testing performed, is the contractor systems program effective? |

[17] CIO and Chief Acquisition Officers Councils, *Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service* (Feb. 2012). Note: IT is Information Technology.

| **2.0 Protect**<br>**Status of Configuration Management Program** | **Maturity Model Indicator** | ***Configuration Management* (*Protect*)** |
|---|---|---|
| Yes | Level 2: Defined | **2.1** Has the organization established a configuration management program that is inclusive of comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?<br>**TIGTA Comments:** The IRS established a configuration management program. However, we did note that it had not updated its configuration management policy and procedures within three years or when a significant change occurred as required. |
| No | Level 2: Defined | **2.1.1** Develops and maintains an up-to-date inventory of the hardware assets (*i.e.*, endpoints, mobile assets, network devices, input/output assets, and SMART/NEST devices) connected to the organization's network with the detailed information necessary for tracking and reporting. (NIST CF ID.AM-1, FY 2016 CIO FISMA Metrics 1.5 and 3.17, NIST SP 800-53: CM-8)<br>**TIGTA Comments:** Although the IRS has implemented an asset management solution as its official inventory solution, during the FY 2016 FISMA evaluation period, TIGTA reported the inventory being inaccurate and/or incomplete. Also, three of the 10 systems selected for the FISMA evaluation reported in their System Security Plans that NIST SP 800-53 security control CM-8, Information System Component Inventory, was not fully in place. |
| No | Level 2: Defined | **2.1.2** Develops and maintains an up-to-date inventory of software platforms and applications used within the organization and with the detailed information necessary for tracking and reporting. (NIST SP 800-53: CM-8, NIST CF ID.AM-2)<br>**TIGTA Comments:** Information deemed necessary for effective information system component inventories includes software license information. Within the last three years, TIGTA completed three audits relating to software license management and reported that the IRS was not adequately performing software license management, was not adhering to Federal requirements, and did not have specialized software license tools for developing and maintaining an enterprisewide inventory. The IRS indicated that it is in the process of deploying a commercial-off-the-shelf software asset management framework to track and maintain its inventory of software in use across the IRS, expected to be completed by October 15, 2017. |

| **2.0 Protect**<br>**Status of Configuration Management Program** | **Maturity Model Indicator** | ***Configuration Management* (*Protect*)** |
|---|---|---|
| No | Level 3: Consistently Implemented | **2.1.3** Implements baseline configurations for information technology systems that are developed and maintained in accordance with documented procedures. (NIST SP 800-53: CM-2, NIST CF PR.IP-1)<br>**TIGTA Comments:** The IRS has established and documented standard baseline configurations for its information technology systems; however, the IRS has not always maintained the configurations in accordance with its documented procedures. Four of the 10 systems selected for the FISMA evaluation reported in their System Security Plans that NIST SP 800-53 security control CM-2, Baseline Configuration, was not fully in place. |
| No | Level 3: Consistently Implemented | **2.1.4** Implements and maintains standard security settings (also referred to as security configuration checklists or hardening guides) for information technology systems in accordance with documented procedures. (NIST SP 800-53: CM-6, FY 2016 CIO FISMA Metrics 2.3)<br>**TIGTA Comments:** The IRS has not always implemented and maintained standard security settings in accordance with documented procedures. All 10 System Security Plans of the systems selected for the FISMA evaluation showed that some or all of the required configuration settings for servers within their respective authorization boundaries were not implemented in accordance with IRS policy. |
| No | Level 4: Managed and Measurable | **2.1.5** Assesses configuration change control processes, including processes to manage configuration deviations across the enterprise that are implemented and maintained. (NIST SP 800-53: CM-3, NIST CF PR.IP-3)<br>**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. The GAO reported that the IRS did not document requests and approvals for all changes to the mainframe production system. TIGTA identified that the IRS did not always correct configuration vulnerabilities or apply patches on servers within the established time frames. Also, IRS security change management process and procedure documents are outdated and currently in the IRS's review process. Lastly, three of the 10 systems reported in their System Security Plans that NIST SP 800-53 security control CM-3, Configuration Change Control, was not fully in place. |
| Yes | Level 4: Managed and Measurable | **2.1.6** Identifies and documents deviations from configuration settings. Acceptable deviations are approved with business justification and risk acceptance. Where appropriate, automated means that enforce and redeploy configuration settings to systems at regularly scheduled intervals are deployed, while evidence of deviations is also maintained. (NIST SP 800-53: CM-6, Center for Internet Security Controls 3.7) |

| **2.0 Protect**<br>**Status of Configuration Management Program** | **Maturity Model Indicator** | ***Configuration Management* (*Protect*)** |
|---|---|---|
| No | Level 4: Managed and Measurable | **2.1.7** Implemented Security Content Automation Protocol certified software assessing (scanning) capabilities against all systems on the network to assess both code-based and configuration-based vulnerabilities in accordance with risk management decisions. (NIST SP 800-53: RA-5 and SI-2, FY 2016 CIO FISMA Metrics 2.2, Center for Internet Security Controls 4.1)<br>**TIGTA Comments:** The IRS has not implemented Security Content Automation Protocol certified software assessing (scanning) capabilities against all systems on the network. In addition, the 10 systems selected for review reported in their System Security Plans that eight and four systems, respectively, did not have NIST SP 800-53 security controls RA-5, Vulnerability Management, and SI-2, Flaw Remediation, fully in place. |
| No | Level 3: Consistently Implemented | **2.1.8** Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST SP 800-53: CM-4, CM-6, RA-5, and SI-2)<br>**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. During the FY 2016 FISMA evaluation period, TIGTA reported that the IRS was not timely remediating high-risk vulnerabilities and POA&Ms did not meet standards. Also, a significant number (six, eight, and four systems, respectively) of the 10 systems selected for review reported in their System Security Plans that they did not have NIST SP 800-53 security controls CM-6, RA-5, and SI-2 fully in place. |
| No | Level 4: Managed and Measurable | **2.1.9** Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3 and SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01)<br>**TIGTA Comments:** The IRS has developed a comprehensive patch management standard operating procedure. However, the IRS indicated that a patch implementation standard operating procedure is currently being developed to include the tools that will be used for patch installation, standardize processes for common patching activities, and to ensure that patch deployment timelines meet the IRS policy. Both TIGTA and the GAO continue to report on weaknesses in the IRS patch management process. For instance, the IRS did not always ensure that critical security patch updates were applied to its systems in a timely manner. Also, the IRS continues to run outdated and unsupported software on its systems. |

| **2.0 Protect**<br>**Status of Configuration Management Program** | **Maturity Model Indicator** | ***Configuration Management* (*Protect*)** |
|---|---|---|
| Not Effective | | **2.1.10** Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above. Based on all testing performed, is the configuration management program effective?<br>**TIGTA Comments:** According to the new scoring methodology implemented by the DHS for the FY 2016 Inspector General FISMA Reporting Metrics, program areas must have met all attributes labeled as *Defined* and *Consistently Implemented* and half or more of the attributes labeled as *Managed and Measurable* to have an effective program. This program area did not meet all attributes at the level 2 *Defined*. |

| **2.0 Protect**<br>**Status of Identity and Access Management Program** | **Maturity Model Indicator** | ***Identity and Access Management* (*Protect*)** |
|---|---|---|
| Yes | Level 2: Defined | **2.2** Has the organization established an identity and access management program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? |
| No | Level 3: Consistently Implemented | **2.2.1** Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements, participate in required training prior to being granted access, and recertify access agreements on a predetermined interval. (NIST SP 800-53: PL-4 and PS-6)<br>**TIGTA Comments:** While the IRS has an enterprisewide process to register and grant users access to information systems, during the FY 2016 FISMA evaluation period, TIGTA reported that an IRS office did not use the process to register and grant users access to a system, and therefore appropriate access agreements were not signed. In addition, the System Security Plans for the 10 systems selected for review also reported occurrences of access granted to systems without proper authorization. |

| **2.0 Protect**<br>**Status of Identity and Access Management Program** | **Maturity Model Indicator** | ***Identity and Access Management* (*Protect*)** |
|---|---|---|
| No | Level 3: Consistently Implemented | **2.2.2** Ensures that all users are only granted access based on least privilege and separation-of-duties principles.<br>**TIGTA Comments:** TIGTA identified 27 systems that did not support that users were granted access based on least privilege, due to incomplete, inaccurate, and outdated documentation for user access. In addition, TIGTA reported that the IRS's standard process to annually recertify that the users have a continued business need for access to the system was not used for users with elevated privileges. Also, during the FY 2016 FISMA evaluation period, the GAO identified users that the IRS allowed to have excessive privileges to systems. Lastly, the system security plans for the 10 IRS systems selected for review reported that 50 percent did not have NIST SP 800-53 security control AC-5, Separation of Duties, fully in place and 50 percent did not have NIST SP 800-53 security control AC-6, Least Privilege, fully in place. |
| Yes | Level 3: Consistently Implemented | **2.2.3** Distinguishes hardware assets that have user accounts (*e.g.*, desktops, laptops, servers) from those without user accounts (*e.g.*, networking devices, such as load balancers and intrusion detection/prevention systems, and other input/output devices such as faxes and Internet Protocol phones). |
| No | Level 3: Consistently Implemented | **2.2.4** Implements PIV for physical access in accordance with government policies. (Homeland Security Presidential Directive 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11)[18]<br>**TIGTA Comments:** The IRS has implemented the required Homeland Security Presidential Directive 12 and FIPS 201 access control systems in only 61 percent of the buildings that require them. The projected completion of the remaining 39 percent of the buildings is in FY 2019 (if funded). |

[18] NIST, FIPS Pub. 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors* (Aug. 2013). Note: FIPS 201-2 superseded FIPS 201 (FIPS 201-1). OMB, OMB M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 2005). OMB, OMB M-07-06, *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials* (Jan. 2007). OMB, OMB M-08-01, *HSPD-12 Implementation Status* (Oct. 2007). OMB, OMB M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors* (Feb. 2011).

| **2.0 Protect**<br>**Status of Identity and Access Management Program** | **Maturity Model Indicator** | ***Identity and Access Management* (*Protect*)** |
|---|---|---|
| No | Level 3: Consistently Implemented | **2.2.5** Implements PIV or a NIST Level of Assurance 4 credential for logical access by all privileged users (system, network, database administrators, and others responsible for system/application control, monitoring, or administration functions). (Cybersecurity Sprint, OMB M-16-04, PMC, FY 2016 CIO FISMA Metrics 2.5.1)<br>**TIGTA Comments:** The IRS reported that all privileged users are required to log on to the IRS network with PIV cards. Work is ongoing to ensure privileged access to systems using PIV cards and to replace aging systems and retire software that do not support PIV card access. As of June 29, 2016, the IRS had enabled a privileged access solution that allowed 1,901 (62 percent) of 3,084 privileged users to log on to privileged accounts using PIV cards. |
| Yes | Level 3: Consistently Implemented | **2.2.6** Enforces PIV or a NIST Level of Assurance 4 credential for logical access for at least 85 percent of nonprivileged users. (Cybersecurity Sprint, OMB M-16-04, PMC, FY 2016 CIO FISMA Metrics 2.4.1) |
| No | Level 4: Managed and Measurable | **2.2.7** Tracks and controls the use of administrative privileges and ensures that these privileges are periodically reviewed and adjusted in accordance with organizationally defined time frames. (FY 2016 CIO FISMA Metrics 2.9 and 2.10, OMB M-16-04, Center for Internet Security Controls 5.2)<br>**TIGTA Comments:** During the FY 2016 FISMA evaluation period, TIGTA and the GAO identified deficiencies in this control, reporting that the IRS had not properly limited the use of administrative privileges or ensured that these privileges were periodically reviewed and adjusted in accordance with policy. The IRS's current system to review privileged access does not require revalidation on a semi-annual basis in accordance with IRS policy. The IRS indicated it is working to correct this deficiency. |
| No | Level 4: Managed and Measurable | **2.2.8** Ensures that accounts are terminated or deactivated once access is no longer required or after a period of inactivity, according to organizational policy.<br>**TIGTA Comments:** During the FY 2016 FISMA evaluation period, 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 | Level 3: Consistently Implemented | **2.2.9** Identifies, limits, and controls the use of shared accounts. (NIST SP 800-53: AC-2)<br>**TIGTA Comments:** During the FY 2016 FISMA evaluation period, TIGTA and the GAO identified improper use of shared accounts; for example, use of generic administrator accounts and passwords. |

| **2.0 Protect**<br>**Status of Identity and Access Management Program** | **Maturity Model Indicator** | ***Identity and Access Management* (*Protect*)** |
|---|---|---|
| Yes | Level 3: Consistently Implemented | **2.2.10** All users are uniquely identified and authenticated for remote access using Strong Authentication (multi-factor), including PIV. (NIST SP 800-46: Section 4.2 and Section 5.1, NIST SP 800-63)[19] |
| Yes | Level 3: Consistently Implemented | **2.2.11** Protects against and detects unauthorized remote access connections or subversion of authorized remote access connections, including through remote scanning of host devices. (Center for Internet Security Controls 12.7 and 12.8, FY 2016 CIO FISMA Metrics 2.17.3, 2.17.4, 3.11, and 3.11.1) |
| Yes | Level 4: Managed and Measurable | **2.2.12** Remote access sessions are timed out after 30 minutes of inactivity, requiring user reauthentication, consistent with OMB M-07-16.[20] |
| Yes | Level 3: Consistently Implemented | **2.2.13** Enforces a limit of consecutive invalid remote access logon attempts and automatically locks the account or delays the next logon prompt. (NIST SP 800-53: AC-7) |
| Yes | Level 3: Consistently Implemented | **2.2.14** Implements a risk-based approach to ensure that all agency public websites and services are accessible through a secure connection through the use and enforcement of https and strict transport security. (OMB M-15-13)[21] |
| Not Effective | | **2.2.15** Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Based on all testing performed, is the identity and access management program effective?<br>**TIGTA Comments:** According to the new scoring methodology implemented by the DHS for the FY 2016 Inspector General FISMA Reporting Metrics, program areas must have met all attributes labeled as *Defined* and *Consistently Implemented* and half or more of the attributes labeled as *Managed and Measurable* to have an effective program. This program area did not meet all attributes at the level 3 *Consistently Implemented*. |

[19] NIST, NIST SP 800-46 Rev. 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016). NIST, NIST SP 800-63-2, *Electronic Authentication Guideline* (Aug. 2013). NIST SP 800-63-2 supersedes NIST SP 800-63-1.
[20] OMB, OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 2007).
[21] OMB, OMB M-15-13, *Policy to Require Secure Connections across Federal Websites and Web Services* (June 2015).

| **2.0 Protect**<br>**Status of Security and Privacy Training Program** | **Maturity Model Indicator** | ***Security and Privacy Training (Protect)*** |
|---|---|---|
| Yes | Level 2: Defined | **2.3** Has the organization established a security and privacy awareness and training program, including comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? |
| Yes | Level 3: Consistently Implemented | **2.3.1** Develops training material for security and privacy awareness training containing appropriate content for the organization, including anti-phishing, malware defense, social engineering, and insider threat topics. (NIST SP 800-50, NIST SP 800-53: AR-5, OMB M-15-01, FY 2016 CIO FISMA Metrics, PMC, National Insider Threat Policy)[22]<br>**TIGTA Comments:** The IRS's information systems security awareness training includes basic appropriate content, but it should be further developed to meet the specific requirements relating to insider threats. The IRS said that it plans to update information systems security training for FY 2017. |
| Yes | Level 3: Consistently Implemented | **2.3.2** Evaluates the skills of individuals with significant security and privacy responsibilities and provides additional security and privacy training content or implements human capital strategies to close identified gaps. (NIST SP 800-50) |
| Yes | Level 3: Consistently Implemented | **2.3.3** Identifies and tracks the status of security and privacy awareness training for all information system users (including employees, contractors, and other organization users) requiring security awareness training with appropriate internal processes to detect and correct deficiencies. (NIST SP 800-53: AT-2) |
| Yes | Level 3: Consistently Implemented | **2.3.4** Identifies and tracks the status of specialized security and privacy training for all personnel (including employees, contractors, and other organization users) with significant information security and privacy responsibilities requiring specialized training. |
| Yes | Level 4: Managed and Measurable | **2.3.5** Measures the effectiveness of its security and privacy awareness and training programs, including through social engineering and phishing exercises. (PMC, FY 2016 CIO FISMA Metrics 2.19, NIST SP 800-50, NIST SP 800-55)[23] |

[22] NIST, NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (Oct. 2003). OMB, OMB M-15-01, *Fiscal Year 2014–2015 Guidance on Improving Federal Information Security and Privacy Management Practices* (Oct. 2014).
[23] NIST, NIST SP 800-55 Rev. 1, *Performance Measurement Guide for Information Security* (July 2008).

| **2.0 Protect**<br>**Status of Security and Privacy Training Program** | **Maturity Model Indicator** | ***Security and Privacy Training (Protect)*** |
|---|---|---|
| Effective | | **2.3.6** Provide any additional information on the effectiveness (positive or negative) of the organization's security and privacy training program that was not noted in the questions above. Based on all testing performed, is the security and privacy training program effective? |

| **3.0 Detect**<br>**Status of Information Security Continuous Monitoring Program** | **Maturity Model Indicator** | ***Information Security Continuous Monitoring*** |
|---|---|---|
| | Level 1: Ad-Hoc | **Definition**<br>**3.1.1 (Definition)** The ISCM program is not formalized and ISCM activities are performed in a reactive manner, resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, NIST SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.[24] |
| Met | Level 1: Ad-Hoc | **People**<br>**3.1.1.1 (People)** ISCM stakeholders and their responsibilities have not been fully defined and communicated across the organization. |
| Met | Level 1: Ad-Hoc | **3.1.1.2 (People)** The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Key personnel do not possess knowledge, skills, and abilities to successfully implement an effective ISCM program.<br>**TIGTA Comments:** The IRS stated that an assessment it completed for all its information technology organization covered the ISCM program areas. |
| Met | Level 1: Ad-Hoc | **3.1.1.3 (People)** The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. |

[24] NIST, NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (Sept. 2011).

| **3.0 Detect**<br>**Status of Information Security Continuous Monitoring Program** | **Maturity Model Indicator** | ***Information Security Continuous Monitoring*** |
|---|---|---|
| Met | Level 1: Ad-Hoc | **3.1.1.4 (People)** The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. |
| Met | Level 1: Ad-Hoc | **Processes**<br>**3.1.1.5 (Processes)** ISCM processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security-related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. |
| Met | Level 1: Ad-Hoc | **3.1.1.6 (Processes)** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. |
| Met | Level 1: Ad-Hoc | **3.1.1.7 (Processes)** The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. |
| Met | Level 1: Ad-Hoc | **3.1.1.8 (Processes)** The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes. |
| Met | Level 1: Ad-Hoc | **Technology**<br>**3.1.1.9 (Technology)** The organization has not identified and defined the ISCM technologies needed in one of more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. Use of ISCM technologies in the following areas is ad-hoc.<br>• Patch management<br>• License management<br>• Information management<br>• Software assurance<br>• Vulnerability management<br>• Event management<br>• Malware detection<br>• Asset management<br>• Configuration management |

| **3.0 Detect**<br>**Status of Information Security Continuous Monitoring Program** | **Maturity Model Indicator** | ***Information Security Continuous Monitoring*** |
|---|---|---|
| | | • Network management<br>• Incident management<br>**TIGTA Comments:** While the IRS is still in the process of implementing its ISCM program required by the OMB, the IRS indicated that the related ISCM activities are currently being performed and are supported by numerous tools within the enterprise. |
| Met | Level 1: Ad-Hoc | **3.1.1.10 (Technology)** The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. |
| | Level 2: Defined | **Definition**<br>**3.2.1 (Definition)** The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, NIST SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organizationwide. |
| Met | Level 2: Defined | **People**<br>**3.2.1.1 (People)** ISCM stakeholders and their responsibilities have been defined and communicated across the organization. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement ISCM activities. |
| Not Met | Level 2: Defined | **3.2.1.2 (People)** The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective ISCM program.<br>**TIGTA Comments:** The IRS did not identify skill and requirement gaps (if any) to effectively implement an ISCM program in accordance with OMB M-14-03. |
| Met | Level 2: Defined | **3.2.1.3 (People)** The organization has defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. However, ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions. |

| **3.0 Detect**<br>**Status of Information Security Continuous Monitoring Program** | **Maturity Model Indicator** | ***Information Security Continuous Monitoring*** |
|---|---|---|
| Met | Level 2: Defined | **3.2.1.4 (People)** The organization has defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. However, ISCM activities are not consistently integrated with the organization's risk management program. |
| Met | Level 2: Defined | **Processes**<br>**3.2.1.5 (Processes)** ISCM processes have been fully defined for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security-related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. However, these processes are inconsistently implemented across the organization. |
| Met | Level 2: Defined | **3.2.1.6 (Processes)** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. |
| Met | Level 2: Defined | **3.2.1.7 (Processes)** The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. |
| Met | Level 2: Defined | **3.2.1.8 (Processes)** The organization has a defined process for capturing lessons learned on the effectiveness of its ISCM program and making necessary improvements. However, lessons learned are not consistently shared across the organization and used to make timely improvements to the ISCM program. |

| **3.0 Detect**<br>**Status of Information Security Continuous Monitoring Program** | **Maturity Model Indicator** | ***Information Security Continuous Monitoring*** |
|---|---|---|
| Not Met | Level 2: Defined | **Technology**<br>**3.2.1.9 (Technology)** The organization has identified and fully defined the ISCM technologies it plans to utilize in the following automation areas. In addition, the organization has developed a plan for implementing ISCM technologies in these areas: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. However, the organization has not fully implemented technology is these automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some ISCM activities, the tools may not be interoperable.<br>**TIGTA Comments:** The IRS has defined and documented in its ISCM Program Plan its ISCM technologies related to vulnerability management, asset management, configuration management, and incident management. The remaining domains have yet to be documented. |
| Met | Level 2: Defined | **3.2.1.10 (Technology)** The organization has defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. However, the organization does not consistently implement the technologies that will enable it to manage an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. |
| | Level 3: Consistently Implemented | **Definition**<br>**3.3.1 (Definition)** In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions consistent with NIST SP 800-53, NIST SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. |

| **3.0 Detect**<br>**Status of Information Security Continuous Monitoring Program** | **Maturity Model Indicator** | ***Information Security Continuous Monitoring*** |
|---|---|---|
| Not Met | Level 3: Consistently Implemented | **People**<br>**3.3.1.1 (People)** ISCM stakeholders and their responsibilities have been identified and communicated across the organization, and stakeholders have adequate resources (people, processes, and technology) to effectively implement ISCM activities.<br>**TIGTA Comments:** The IRS has defined and documented the ISCM roles and responsibilities in its ISCM Program Plan; however, at this time, not all ISCM stakeholders have adequate resources (people and technology) to implement their defined responsibilities. |
| Not Met | Level 3: Consistently Implemented | **3.3.1.2 (People)** The organization has fully implemented its plans to close any gaps in skills, knowledge, and resources required to successfully implement an ISCM program. Personnel possess the required knowledge, skills, and abilities to effectively implement the organization's ISCM program.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Met | Level 3: Consistently Implemented | **3.3.1.3 (People)** ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations. |
| Not Met | Level 3: Consistently Implemented | **3.3.1.4 (People)** ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements.<br>**TIGTA Comments:** The IRS has defined and documented how ISCM activities integrate with organizational risk tolerance, the threat environment, and the business/mission requirements within the ISCM Program Plan. However, ISCM activities are not yet consistently integrated with the organization's risk management program. |
| Met | Level 3: Consistently Implemented | **Processes**<br>**3.3.1.5 (Processes)** ISCM processes are consistently performed across the organization in the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security-related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. |

| **3.0 Detect**<br>**Status of Information Security Continuous Monitoring Program** | **Maturity Model Indicator** | ***Information Security Continuous Monitoring*** |
|---|---|---|
| Met | Level 3: Consistently Implemented | **3.3.1.6 (Processes)** The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. |
| Not Met | Level 3: Consistently Implemented | **3.3.1.7 (Processes)** The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting. ISCM measures provide information on the effectiveness of ISCM processes and activities.<br>**TIGTA Comments:** The IRS has identified and defined the performance measures and requirements within the ISCM Program Plan. The measures are consistently collected, analyzed, and used appropriately across the IRS. However, the metrics providing comprehensive information on the effectiveness of ISCM processes and activities are not collected and analyzed. |
| Not Met | Level 3: Consistently Implemented | **3.3.1.8 (Processes)** The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes.<br>**TIGTA Comments:** The ISCM Program Plan is thoroughly reviewed by all affected stakeholders, and a comprehensive update is preformed to ensure that different processes and activities making up ISCM are updated appropriately. However, consistently sharing lessons learned to make timely improvements to the ISCM program has not occurred. |
| Not Met | Level 3: Consistently Implemented | **Technology**<br>**3.3.1.9 (Technology)** The organization has consistently implemented its defined technologies in all of the following ISCM automation areas. ISCM tools are interoperable to the extent practicable.<br>• Patch management<br>• License management<br>• Information management<br>• Software assurance<br>• Vulnerability management<br>• Event management<br>• Malware detection<br>• Asset management<br>• Configuration management<br>• Network management |

| **3.0 Detect**<br>**Status of Information Security Continuous Monitoring Program** | **Maturity Model Indicator** | ***Information Security Continuous Monitoring*** |
|---|---|---|
| | | • Incident management<br>**TIGTA Comments:** The IRS has not met this metric. |
| Not Met | Level 3: Consistently Implemented | **3.3.1.10 (Technology)** The organization can produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.<br>**TIGTA Comments:** The IRS stated that it has defined the continuous diagnostics and mitigation tool requirements for inventory automation that will produce an accurate point-in-time inventory, but it has not implemented the tool yet. |
| | Level 4: Managed and Measurable | **Definition**<br>**3.4.1 (Definition)** In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations. |
| Not Met | Level 4: Managed and Measurable | **People**<br>**3.4.1.1 (People)** The organization's staff is consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of the organization's ISCM program.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 4: Managed and Measurable | **3.4.1.2 (People)** Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the ISCM program.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 4: Managed and Measurable | **3.4.1.3 (People)** Staff are assigned responsibilities for developing and monitoring ISCM metrics as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the ISCM program.<br>**TIGTA Comments:** The IRS did not meet this metric. |

| **3.0 Detect**<br>**Status of Information Security Continuous Monitoring Program** | **Maturity Model Indicator** | ***Information Security Continuous Monitoring*** |
|---|---|---|
| Not Met | Level 4: Managed and Measurable | **Processes**<br>**3.4.1.4 (Processes)** The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing ISCM.<br>**TIGTA Comments:** The IRS has not yet implemented the continuous diagnostics and mitigation tool suite needed to generate the data that will assist the IRS in analyzing quantitative and qualitative performance measures across the organization. |
| Not Met | Level 4: Managed and Measurable | **3.4.1.5 (Processes)** Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 4: Managed and Measurable | **3.4.1.6 (Processes)** The organization is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 4: Managed and Measurable | **3.4.1.7 (Processes)** The organization uses its ISCM metrics for determining risk response actions including risk acceptance, avoidance/rejection, or transfer.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 4: Managed and Measurable | **3.4.1.8 (Processes)** ISCM metrics are reported to the organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 4: Managed and Measurable | **3.4.1.9 (Processes)** ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (*i.e.*, System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis.<br>**TIGTA Comments:** The IRS did not meet this metric. |

| **3.0 Detect**<br>**Status of Information Security Continuous Monitoring Program** | **Maturity Model Indicator** | ***Information Security Continuous Monitoring*** |
|---|---|---|
| Not Met | Level 4: Managed and Measurable | **Technology**<br>**3.4.1.10 (Technology)** The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing ISCM.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 4: Managed and Measurable | **3.4.1.11 (Technology)** The organization's ISCM performance measures include data on the implementation of its ISCM program for all sections of the network from the implementation of technologies that provide standard calculations, comparisons, and presentations.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 4: Managed and Measurable | **3.4.1.12 (Technology)** The organization utilizes a security information and event management tool to collect, maintain, monitor, and analyze information technology security information, achieve situational awareness, and manage risk.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| | Level 5: Optimized | **Definition**<br>**3.5.1 (Definition)** In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape. |
| Not Met | Level 5: Optimized | **People**<br>**3.5.1.1 (People)** The organization's assigned personnel collectively possess a high skill level to perform and update ISCM activities on a near real-time basis to make any changes needed to address ISCM results based on organization risk tolerance, the threat environment, and business/mission requirements.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 5: Optimized | **Processes**<br>**3.5.1.2 (Processes)** The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity and practices.<br>**TIGTA Comments:** The IRS did not meet this metric. |

| **3.0 Detect**<br>**Status of Information Security Continuous Monitoring Program** | **Maturity Model Indicator** | ***Information Security Continuous Monitoring*** |
|---|---|---|
| Not Met | Level 5: Optimized | **3.5.1.3 (Processes)** On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 5: Optimized | **3.5.1.4 (Processes)** The ISCM program is fully integrated with strategic planning, enterprise architecture and capital planning and investment control processes, and other mission/business areas, as appropriate.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 5: Optimized | **3.5.1.5 (Processes)** The ISCM program achieves cost-effective information technology security objectives and goals and influences decisionmaking that is based on cost, risk, and mission impact.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 5: Optimized | **Technology**<br>**3.5.1.6 (Technology)** The organization has institutionalized the implementation of advanced cybersecurity technologies in near real time.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 5: Optimized | **3.5.1.7 (Technology)** The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its ISCM program.<br>**TIGTA Comments:** The IRS did not meet this metric. |

| **4.0 Respond** **Status of Incident Response Program** | **Maturity Model Indicator** | ***Incident Response Program*** |
|---|---|---|
| | Level 1: Ad-Hoc | **Definition**<br>**4.1.1 (Definition)** The incident response program is not formalized and incident response activities are performed in a reactive manner, resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with the FISMA (including guidance from NIST SP 800-83, NIST SP 800-61, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and United States-Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines).[25] |
| Met | Level 1: Ad-Hoc | **People**<br>**4.1.1.1 (People)** Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have not been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, the DHS, and the OMB for all incident response activities. |
| Met | Level 1: Ad-Hoc | **4.1.1.2 (People)** The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. Key personnel do not possess the knowledge, skills, and abilities to successfully implement an effective incident response program. |
| Met | Level 1: Ad-Hoc | **4.1.1.3 (People)** The organization has not defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders and used to make timely, risk-based decisions. |
| Met | Level 1: Ad-Hoc | **4.1.1.4 (People)** The organization has not defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas as appropriate. |

[25] NIST, NIST SP 800-83 Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* (July 2013). NIST, NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide* (Aug. 2012). OMB, OMB M-16-03, *Fiscal Year 2015–2016 Guidance on Federal Information Security and Privacy Management Requirements* (Oct. 2015).

| **4.0 Respond**<br>**Status of Incident Response Program** | **Maturity Model Indicator** | ***Incident Response Program*** |
|---|---|---|
| Met | Level 1: Ad-Hoc | **Processes**<br>**4.1.1.5 (Processes)** Incident response processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: incident response planning; incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting to internal and external stakeholders using standard data elements and impact classifications within time frames established by the US-CERT. |
| Met | Level 1: Ad-Hoc | **4.1.1.6 (Processes)** The organization has not fully defined how it will collaborate with the DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. |
| Met | Level 1: Ad-Hoc | **4.1.1.7 (Processes)** The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. |
| Met | Level 1: Ad-Hoc | **4.1.1.8 (Processes)** The organization has not defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. |
| Met | Level 1: Ad-Hoc | **Technology**<br>**4.1.1.9 (Technology)** The organization has not identified and defined the incident response technologies needed in one or more of the following areas and relies on manual/procedural methods in instances where automation would be more effective. Use of incident response technologies in the following areas is ad-hoc.<br>• Web application protections, such as web application firewalls.<br>• Event and incident management, such as intrusion detection and prevention tools and incident tracking and reporting tools.<br>• Aggregation and analysis, such as security information and event management products.<br>• Malware detection, such as antivirus and antispam software technologies.<br>• Information management, such as data loss prevention.<br>• File integrity and endpoint and server security tools. |
| Met | Level 1: Ad-Hoc | **4.1.1.10 (Technology)** The organization has not defined how it will meet the defined Trusted Internet Connection (TIC) security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points as appropriate. |

| **4.0 Respond** **Status of Incident Response Program** | **Maturity Model Indicator** | ***Incident Response Program*** |
|---|---|---|
| Met | Level 1: Ad-Hoc | **4.1.1.11 (Technology)** The organization has not defined how it plans to utilize the DHS's Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks. |
| Met | Level 1: Ad-Hoc | **4.1.1.12 (Technology)** The organization has not defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. |
| | Level 2: Defined | **Definition**<br>**4.2.1 (Definition)** The organization has formalized its incident response program through the development of comprehensive incident response policies, plans, and procedures consistent with the FISMA (including guidance from NIST SP 800-83, NIST SP 800-61, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and the US-CERT Federal Incident Notification Guidelines). However, incident response policies, plans, and procedures are not consistently implemented organizationwide. |
| Met | Level 2: Defined | **People**<br>**4.2.1.1 (People)** Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, the DHS, and the OMB for all incident response activities. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement incident response activities. Further, the organization has not verified roles and responsibilities as part of incident response testing. |
| Met | Level 2: Defined | **4.2.1.2 (People)** The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective incident response program. |
| Met | Level 2: Defined | **4.2.1.3 (People)** The organization has defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders and used to make timely, risk-based decisions. However, the organization does not consistently utilize its threat vector taxonomy, and incident response information is not always shared with individuals with significant security responsibilities and other stakeholders in a timely manner. |

| **4.0 Respond**<br>**Status of Incident Response Program** | **Maturity Model Indicator** | ***Incident Response Program*** |
|---|---|---|
| Met | Level 2: Defined | **4.2.1.4 (People)** The organization has defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas as appropriate. However, incident response activities are not consistently integrated with these areas. |
| Met | Level 2: Defined | **Processes**<br>**4.2.1.5 (Processes)** Incident response processes have been fully defined for the following areas: incident response planning; incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within time frames established by the US-CERT. However, these processes are inconsistently implemented across the organization. |
| Met | Level 2: Defined | **4.2.1.6 (Processes)** The organization has fully defined, but not consistently implemented, its processes to collaborate with the DHS and other parties, as appropriate, to provide on-site technical assistance/surge resources/special capabilities for quickly responding to incidents. |
| Met | Level 2: Defined | **4.2.1.7 (Processes)** The organization has identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. |
| Met | Level 2: Defined | **4.2.1.8 (Processes)** The organization has defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. However, lessons learned are not consistently captured and shared across the organization and used to make timely improvements to security controls and the incident response program. |
| Met | Level 2: Defined | **Technology**<br>**4.2.1.9 (Technology)** The organization has identified and fully defined the incident response technologies it plans to utilize in the following areas.<br>• Web application protections, such as web application firewalls.<br>• Event and incident management, such as intrusion detection and prevention tools and incident tracking and reporting tools.<br>• Aggregation and analysis, such as security information and event management products. However, the organization has not ensured that security and event data are aggregated and correlated from all relevant sources and sensors. |

| **4.0 Respond** **Status of Incident Response Program** | **Maturity Model Indicator** | ***Incident Response Program*** |
|---|---|---|
| | | • Malware detection such as antivirus and antispam software technologies.<br>• Information management, such as data loss prevention.<br>• File integrity and endpoint and server security tools.<br>However, the organization has not fully implemented technologies in these areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policies, plans, and procedures. |
| Met | Level 2: Defined | **4.2.1.10 (Technology)** The organization has defined how it will meet the defined TIC security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points as appropriate. However, the organization has not ensured that the TIC 2.0 provider- and agency-managed capabilities are consistently implemented. |
| Met | Level 2: Defined | **4.2.1.11 (Technology)** The organization has defined how it plans to utilize the DHS's Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its networks. |
| Met | Level 2: Defined | **4.2.1.12 (Technology)** The organization has defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. However, the organization has not established, and does not consistently maintain, a comprehensive baseline of network operations and expected data flows for users and systems. |
| | Level 3: Consistently Implemented | **Definition**<br>**4.3.1 (Definition)** In addition to the formalization and definition of its incident response program (Level 2), the organization consistently implements its incident response program across the agency in accordance with the FISMA (including guidance from NIST SP 800-83, NIST SP 800-61, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and the US-CERT Federal Incident Notification Guidelines). However, data supporting metrics on the effectiveness of the incident response program across the organization are not verified, analyzed, and correlated. |

| **4.0 Respond**<br>**Status of Incident Response Program** | **Maturity Model Indicator** | ***Incident Response Program*** |
|---|---|---|
| Met | Level 3: Consistently Implemented | **People**<br>**4.3.1.1 (People)** Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined, communicated, and consistently implemented across the organization (Level 2). Further, the organization has verified roles and responsibilities of incident response stakeholders as part of incident response testing. |
| Met | Level 3: Consistently Implemented | **4.3.1.2 (People)** The organization has fully implemented its plans to close any gaps in the skills, knowledge, and resources needed to effectively implement its incident response program. Incident response teams are periodically trained to ensure that knowledge, skills, and abilities are maintained.<br>**TIGTA Comments:** The skills gap assessment conducted by the IRS indicated a skills proficiency gap when comparing the IRS CSIRC personnel to the industry standard level of technical proficiency. In addition, the staffing assessment showed 2.6 percent of the requisite staffing was considered unmet. The IRS indicated that these staffing and skills gaps have been addressed by augmenting Federal employees with contractors. TIGTA is currently engaged in an audit of the CSIRC organization and intends to further assess this assertion to ensure that the combined skill set and staffing level is sufficient to protect the IRS network from increasingly sophisticated adversaries. |
| Met | Level 3: Consistently Implemented | **4.3.1.3 (People)** The organization consistently utilizes its defined threat vector taxonomy and shares information with individuals with significant security responsibilities and other stakeholders in a timely fashion to support risk-based decisionmaking. |
| Met | Level 3: Consistently Implemented | **4.3.1.4 (People)** Incident response activities are integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas as appropriate. |
| Met | Level 3: Consistently Implemented | **Processes**<br>**4.3.1.5 (Processes)** Incident response processes are consistently implemented across the organization for the following areas: incident response planning; incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within time frames established by the US-CERT. |
| Met | Level 3: Consistently Implemented | **4.3.1.6 (Processes)** The organization has ensured that processes to collaborate with the DHS and other parties, as appropriate, to provide on-site technical assistance/surge resources/special capabilities for quickly responding to incidents are implemented consistently across the organization. |

| **4.0 Respond**<br>**Status of Incident Response Program** | **Maturity Model Indicator** | ***Incident Response Program*** |
|---|---|---|
| Met | Level 3: Consistently Implemented | **4.3.1.7 (Processes)** The organization is consistently capturing qualitative and quantitative performance metrics on the performance of its incident response program. However, the organization has not ensured that the data supporting the metrics was obtained accurately and in a reproducible format or that the data are analyzed and correlated in ways that are effective for risk management. |
| Met | Level 3: Consistently Implemented | **4.3.1.8 (Processes)** The organization is consistently collecting and capturing lessons learned and incident data on the effectiveness of its incident response program and activities. However, lessons learned may not be shared across the organization in a timely manner and used to make timely improvements to the incident response program and security measures. |
| Met | Level 3: Consistently Implemented | **4.3.1.9 (Processes)** The rigor, intensity, scope, and results of incident response activities (*i.e.*, preparation, detection, analysis, containment, eradication, and recovery, reporting, and post incident) are comparable and predictable across the organization. |
| Met | Level 3: Consistently Implemented | **Technology**<br>**4.3.1.10 (Technology)** The organization has consistently implemented its defined incident response technologies in the following areas.<br>• Web application protections, such as web application firewalls.<br>• Event and incident management, such as intrusion detection and prevention tools and incident tracking and reporting tools.<br>• Aggregation and analysis, such as security information and event management products. The organization ensures that security and event data are aggregated and correlated from all relevant sources and sensors.<br>• Malware detection such as antivirus and antispam software technologies.<br>• Information management, such as data loss prevention.<br>• File integrity and endpoint and server security tools.<br>In addition, the tools are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans. |
| Met | Level 3: Consistently Implemented | **4.3.1.11 (Technology)** The organization has consistently implemented defined TIC security controls and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points as appropriate. |

| **4.0 Respond** **Status of Incident Response Program** | **Maturity Model Indicator** | ***Incident Response Program*** |
|---|---|---|
| Met | Level 3: Consistently Implemented | **4.3.1.12 (Technology)** The organization is utilizing the DHS's Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving their networks. |
| Met | Level 3: Consistently Implemented | **4.3.1.13 (Technology)** The organization has fully implemented technologies to develop and maintain a baseline of network operations and expected data flows for users and systems. |
| | Level 4: Managed and Measurable | **Definition**<br>**4.4.1 (Definition)** In addition to being consistently implemented (Level 3), incident response activities are repeatable and metrics are used to measure and manage the implementation of the incident response program, achieve situational awareness, and control ongoing risk. In addition, the incident response program adapts to new requirements and governmentwide priorities. |
| Met | Level 4: Managed and Measurable | **People**<br>**4.4.1.1 (People)** Incident response stakeholders are consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and are collecting, analyzing, and reporting data on the effectiveness of the organization's incident response program. |
| Met | Level 4: Managed and Measurable | **4.4.1.2 (People)** Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the incident response program. |
| Met | Level 4: Managed and Measurable | **4.4.1.3 (People)** Incident response stakeholders are assigned responsibilities for developing and monitoring incident response metrics as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the incident response program. |
| Met | Level 4: Managed and Measurable | **Processes**<br>**4.4.1.4 (Processes)** The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing incident response. |
| Met | Level 4: Managed and Measurable | **4.4.1.5 (Processes)** Data supporting incident response measures and metrics are obtained accurately, consistently, and in a reproducible format. |

| **4.0 Respond**<br>**Status of Incident Response Program** | **Maturity Model Indicator** | ***Incident Response Program*** |
|---|---|---|
| Met | Level 4: Managed and Measurable | **4.4.1.6 (Processes)** Incident response data, measures, and metrics are analyzed, collected, and presented using standard calculations, comparisons, and presentations. |
| Met | Level 4: Managed and Measurable | **4.4.1.7 (Processes)** Incident response metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. |
| Met | Level 4: Managed and Measurable | **Technology**<br>**4.4.1.8 (Technology)** The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities. |
| Met | Level 4: Managed and Measurable | **4.4.1.9 (Technology)** The organization's incident response performance measures include data on the implementation of its incident response program for all sections of the network. |
| | Level 5: Optimized | **Definition**<br>**4.5.1 (Definition)** In addition to being managed and measurable (Level 4), the organization's incident response program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape. |
| Not Met | Level 5: Optimized | **People**<br>**4.5.1.1 (People)** The organization's assigned personnel collectively possess a high skill level to perform and update incident response activities on a near real-time basis to make any changes needed to address incident response results based on organization risk tolerance, the threat environment, and business/mission requirements.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 5: Optimized | **Processes**<br>**4.5.1.2 (Processes)** The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity practices.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 5: Optimized | **4.5.1.3 (Processes)** On a near real-time basis, the organization actively adapts its incident response program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a near real-time manner.<br>**TIGTA Comments:** The IRS did not meet this metric. |

| **4.0 Respond**<br>**Status of Incident Response Program** | **Maturity Model Indicator** | ***Incident Response Program*** |
|---|---|---|
| Not Met | Level 5: Optimized | **4.5.1.4 (Processes)** The incident response program is fully integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas as appropriate.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 5: Optimized | **4.5.1.5 (Processes)** The incident response program achieves cost-effective information technology security objectives and goals and influences decisionmaking that is based on cost, risk, and mission impact.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 5: Optimized | **Technology**<br>**4.5.1.6 (Technology)** The organization has institutionalized the implementation of advanced incident response technologies in near real-time.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 5: Optimized | **4.5.1.7 (Technology)** The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its incident response program.<br>**TIGTA Comments:** The IRS did not meet this metric. |
| Not Met | Level 5: Optimized | **4.5.1.8 (Technology)** The organization uses simulation based technologies to continuously determine the impact of potential security incidents to its information technology assets and adjusts incident response processes and security measures accordingly.<br>**TIGTA Comments:** The IRS did not meet this metric. |

| **5.0 Recover**<br>**Status of Contingency Planning Program** | **Maturity Model Indicator** | ***Contingency Planning* (*Recover*)** |
|---|---|---|
| Yes | Level 2: Defined | **5.1** Has the organization established an enterprisewide business continuity/disaster recovery program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? |

| **5.0 Recover**<br>**Status of Contingency Planning Program** | **Maturity Model Indicator** | ***Contingency Planning* (*Recover*)** |
|---|---|---|
| Yes | Level 3: Consistently Implemented | **5.1.1** Develops and facilitates recovery testing, training, and exercise programs. (Federal Continuity Directive 1 (FCD1), NIST SP 800-34, NIST SP 800-53)[26] |
| Yes | Level 3: Consistently Implemented | **5.1.2** Incorporates the system's Business Impact Analysis and Business Process Analysis into analysis and strategy toward development of the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan. (NIST SP 800-34) |
| Yes | Level 3: Consistently Implemented | **5.1.3** Develops and maintains documented recovery strategies, plans, and procedures at the division, component, and information technology infrastructure levels. (NIST SP 800-34) |
| Yes | Level 3: Consistently Implemented | **5.1.4** A Business Continuity Plan and Disaster Recovery Plan are in place and ready to be executed upon if necessary. (FCD1, NIST SP 800-34, FY 2016 CIO FISMA Metrics 5.3, PMC) |
| Yes | Level 4: Managed and Measurable | **5.1.5** Tests Business Continuity Plan and Disaster Recovery Plan for effectiveness and updates plans as necessary. (FY 2016 CIO FISMA Metrics 5.4) |
| Yes | Level 3: Consistently Implemented | **5.1.6** Tests system-specific contingency plans, in accordance with organizationally defined time frames, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4) |
| Yes | Level 4: Managed and Measurable | **5.1.7** Develops after-action reports that address issues identified during contingency/disaster recovery exercises in order to improve contingency/disaster recovery processes. (FCD1, NIST SP 800-34) |
| Yes | Level 3: Consistently Implemented | **5.1.8** Determines alternate processing and storage sites based upon risk assessments which ensure that the potential disruption of the organization's ability to initiate and sustain operations is minimized and are not subject to the same physical and/or cybersecurity risks as the primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-6 and CP-7) |

[26] DHS, *Federal Continuity Directive 1 (FCD 1): Federal Executive Branch National Continuity Program and Requirements* (Oct. 2012). NIST, NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010, updated Nov. 2010).

| **5.0 Recover**<br>**Status of Contingency Planning Program** | **Maturity Model Indicator** | ***Contingency Planning* (*Recover*)** |
|---|---|---|
| Yes | Level 4: Managed and Measurable | **5.1.9** Conducts backups of information at the user and system levels and protects the confidentiality, integrity, and availability of backup information at storage sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-9, NIST CF PR.IP-4, National Archives and Records Administration guidance on information systems security records) |
| Yes | Level 2: Defined | **5.1.10** Contingency planning that considers supply chain threats. |
| Effective | | **5.1.11** Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Based on all testing performed, is the contingency planning program effective? |

## Appendix I

# Detailed Objective, Scope, and Methodology

Our overall objective was to assess the effectiveness of the IRS's information security program, procedures, and practices and its compliance with FISMA requirements for the period July 1, 2015, to June 30, 2016. To accomplish our objective, we responded to the questions provided in the DHS *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*,[1] issued on June 20, 2016. The questions related to five cybersecurity functions that included eight security program areas:

1. **Identify**
   - *Risk Management*
   - *Contractor Systems*
   - *Configuration Management*
2. **Protect**
   - *Identity and Access Management*
   - *Security and Privacy Training*
3. **Detect**
   - *Information Security Continuous Monitoring*
4. **Respond**
   - *Incident Response*
5. **Recover**
   - *Contingency 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 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 2016 FISMA evaluation period, as listed in Appendix IV, as well as an audit report from the GAO that contained results applicable to the FISMA questions.

Based on our evaluative work, we will indicate with a yes or a no whether the IRS has achieved a satisfactory level of performance for each security program area as well as each specific attribute. The Treasury Office of the Inspector General will combine our results for the IRS with its results for the non-IRS bureaus and input the combined yes or no responses into Cyberscope.[2]

[1] DHS, *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (Version 1.1.1, Aug. 2016).
[2] An online data collection tool administrated by the DHS to collect performance data for FISMA compliance reporting.

## 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
Cindy Harris, Senior Auditor
Bret Hunter, Senior Auditor
Mary Jankowski, Senior Auditor
Louis Lee, Senior Auditor
Esther Wilson, Senior Auditor
Linda Cieslak, Auditor

## Appendix III

# Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Chief Information Officer
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, User and Network Services
Director, Office of Audit Coordination

## Appendix IV

# Information Technology Security-Related Reports Issued During the Fiscal Year 2016 Evaluation Period

1. TIGTA, Ref. No. 2015-20-060, *The Return Review Program Enhances the Identification of Fraud; However, System Security Needs Improvement* (July 2015).
2. TIGTA, Ref. No. 2015-23-062, *Affordable Care Act Information Sharing and Reporting Project* (Aug. 2015).
3. TIGTA, Ref. No. 2015-20-079, *Stronger Access Controls and Further System Enhancements Are Needed to Effectively Support the Privacy Impact Assessment Program* (Sept. 2015).
4. TIGTA, Ref. No. 2015-20-087, *Improvements Are Needed to Ensure That External Interconnections Are Identified, Authorized, and Secured* (Sept. 2015).
5. TIGTA, Ref. No. 2015-20-088, *Improvements Are Needed to Ensure That New Information Systems Deploy With Compliant Audit Trails and That Identified Deficiencies Are Timely Corrected* (Sept. 2015).
6. TIGTA, Ref. No. 2015-20-092, *Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2015* (Sept. 2015).
7. TIGTA, Ref. No. 2015-23-081, *Affordable Care Act Verification Service: Security and Testing Risks* (Sept. 2015).
8. TIGTA, Ref. No. 2015-20-073, *Inadequate Early Oversight Led to Windows Upgrade Project Delays* (Sept. 2015).
9. TIGTA, Ref. No. 2015-20-093, *Review of the Electronic Fraud Detection System* (Sept. 2015).
10. TIGTA, Ref. No. 2015-20-094, *Annual Assessment of the Internal Revenue Service Information Technology Program* (Sept. 2015).
11. TIGTA, Ref. No. 2016-20-002, *Measurable Agreements on Security Controls Are Needed to Support the Enterprise Storage Services Solution* (Oct. 2015).
12. TIGTA, Ref. No. 2016-40-007, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed* (Nov. 2015).
13. TIGTA, Ref. No. 2016-20-019, *Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement* (Feb. 2016).
14. TIGTA, Ref. No. 2016-23-040, *Affordable Care Act Compliance Validation System: Security and Testing Risks* (May 2016).

15. TIGTA, Ref. No. 2016-2R-044, *The Internal Revenue Service's Cybersecurity Incidents, Policies, and Procedures* (June 2016).
16. TIGTA, Ref. No. 2016-10-038, *Access to Government Facilities and Computers Is Not Always Removed When Employees Separate* (June 2016).
17. GAO, Ref. No. GAO-16-398, *Information Security: IRS Needs to Further Improve Controls over Financial and Taxpayer Data* (Mar. 2016).