TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017

September 29, 2017

Reference Number: 2017-20-087

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 2017

Highlights

Final Report issued on September 29, 2017

Highlights of Reference Number: 2017-20-087 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 and has an obligation to protect this sensitive information against unauthorized access or loss in accordance with FISMA requirements.

WHY TIGTA DID THE AUDIT

As part of the FISMA legislation, the Offices of Inspectors General are required to perform an annual independent evaluation of each Federal agency's information security programs and practices. This report presents the results of TIGTA's FISMA evaluation of the IRS for Fiscal Year 2017.

WHAT TIGTA FOUND

For Fiscal Year 2017, the Inspectors General FISMA reporting metrics were aligned with the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity* and measured the maturity levels for five functional areas: IDENTIFY (organizational understanding to manage cybersecurity risk to assets and capabilities), PROTECT (appropriate safeguards to ensure delivery of critical infrastructure services), DETECT (appropriate activities to identify the occurrence of a cybersecurity event), RESPOND (appropriate activities to take action regarding a detected cybersecurity event), and RECOVER (appropriate activities to restore capabilities or services that were impaired due to a cybersecurity event).

The IRS's Cybersecurity Program was generally in alignment with FISMA requirements, but it was not fully effective due to program attributes not yet implemented. The Department of Homeland Security's scoring methodology defines "effective" as having a maturity level 4, *Managed and Measured*, or above.

Based on these evaluation parameters, TIGTA rated two Cybersecurity function areas (RESPOND and RECOVER) as "effective" and three function areas (IDENTIFY, PROTECT, and DETECT) as "not effective."

The IDENTIFY function area was based on the Risk Management performance metrics, which TIGTA deemed at a maturity level 3, *Consistently Implemented*. The PROTECT function area was based on metrics for three security program areas: Configuration Management, which was at a maturity level 2, *Defined*; Identity and Access Management, which was at a maturity level 3, *Consistently Implemented*; and Security Training, which was at a maturity level 4, *Managed and Measured*. The end result for this function area was a maturity level 3, *Consistently Implemented*. The DETECT function area was based on the Information Security Continuous Monitoring metrics, which TIGTA deemed at a maturity level 3, *Consistently Implemented*.

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 for the applicable FISMA evaluation period.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 29, 2017

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

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Treasury Inspector General for Tax Administration – Federal Information Security Modernization Act Report for Fiscal Year 2017 (Audit # 201720001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Modernization Act of 2014(FISMA)[1] evaluation of the Internal Revenue Service (IRS) for Fiscal Year 2017. The Act requires Federal agencies to have an annual independent evaluation performed of their information security programs and practices and to report the results of the evaluation to the Office of Management and Budget. 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, 2016, to June 30, 2017. This audit is included in our Fiscal Year 2017 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

This report is being forwarded to the Treasury Inspector General for consolidation into a report issued to the Department of the Treasury, Chief Information Officer. We are also sending copies of this report to the IRS managers affected by the report.

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

[1] Pub. L. No. 113-283, 128 Stat. 3073. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

Table of Contents

Abbreviations

DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAO	Government Accountability Office
ICAM	Identity, Credential, and Access Management
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
POA&M	Plan of Action and Milestones
TIGTA	Treasury Inspector General for Tax Administration

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 and is supported by the Office of Management and Budget (OMB), the 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.

The Internal Revenue Service is responsible for implementing appropriate security controls to protect the confidentiality of sensitive information against unauthorized access or loss in accordance with FISMA requirements.

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 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 Internal Revenue Service (IRS), while the Treasury Office of the Inspector General is responsible for all other Treasury bureaus.

The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. As a custodian of taxpayer information it receives and maintains, the IRS is

[1] Pub. L. No. 113-283, 128 Stat. 3073. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.

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.

Fiscal Year (FY)[2] 2017 Inspector General FISMA Reporting Metrics[3]

The FY 2017 Inspector General FISMA Reporting Metrics were developed as a collaborative effort among the OMB, the DHS, and the Council of the Inspectors General on Integrity and Efficiency, in consultation with the Federal Chief Information Officer Council. The FY 2017 metrics represent a continuation of the work that began in FY 2016 to align the Inspector General metrics with the five cybersecurity function areas in the NIST's *Framework for Improving Critical Infrastructure Cybersecurity*[4] (Cybersecurity Framework) and transition the evaluation of all the functional areas to the maturity model approach. The five Cybersecurity Framework function areas are:

- IDENTIFY – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- PROTECT – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- DETECT – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- RESPOND – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- RECOVER – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Figure 1 shows the alignment of the seven security program areas (or metric domains) to the five Cybersecurity Framework function areas.

[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 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (Version 1.0, Apr. 2017).
[4] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.0, Feb. 2014).

Figure 1: Alignment of the NIST Cybersecurity Framework's Function Areas to the FY 2017 Inspector General FISMA Metric Domains

Cybersecurity Function Areas	FY 2017 Inspector General FISMA Metric Domains
IDENTIFY	Risk Management
PROTECT	Configuration Management Identity and Access Management Security Training
DETECT	Information Security Continuous Monitoring (ISCM)
RESPOND	Incident Response
RECOVER	Contingency Planning

Source: FY 2017 Inspector General FISMA Reporting Metrics.

The Inspectors General are required to assess the effectiveness of the information security programs based on a maturity model spectrum. Figure 2 details the five maturity model levels: *ad-hoc*, *defined*, *consistently implemented*, *managed and measurable*, and *optimized*. The DHS's scoring methodology defines "effective" as having a maturity level 4, *Managed and Measurable*, or above.[5]

Figure 2: Inspector General's Assessment Maturity Levels

Maturity Level	Maturity Level Description
Level 1: *Ad-hoc*	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: *Defined*	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: *Consistently Implemented*	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: *Managed and Measureable*	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: *Optimized*	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: FY 2017 Inspector General FISMA Reporting Metrics.

[5] NIST Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013; updated as of Jan. 2014), defines security control effectiveness as 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 information system in its operational environment or enforcing/mediating established security policies.

This review was performed with information obtained from the IRS Information Technology organization's Office of Cybersecurity in New Carrollton, Maryland, during the period May through August 2017. This report covers the period from July 1, 2016, through June 30, 2017. 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 Cybersecurity Program Was Generally Aligned With the Federal Information Security Modernization Act, but It Was Not Fully Effective in Three of the Five Cybersecurity Framework Function Areas

The IRS has established a Cybersecurity Program that was generally aligned with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines. However, due to program components not yet implemented, the IRS's Cybersecurity Program was not fully effective.

To determine the effectiveness of the IRS's Cybersecurity Program, we evaluated the maturity level of the program metrics specified by the DHS in the *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.0* issued on April 17, 2017. We based our work, in part, on a representative subset of seven IRS information systems and the implementation status of key security controls. We also considered the results of TIGTA and Government Accountability Office (GAO) audits performed or completed during the FY 2017 FISMA evaluation period that contained results applicable to the FISMA metrics. See Appendix IV for a list of audits.

As shown in Figure 3, based on the DHS's scoring methodology for the FY 2017 FISMA evaluation period, we rated two Cybersecurity Framework functions as "effective" and three as "not effective."

Figure 3: Maturity Levels by Function Area

Function	Assessed Maturity Level	Effective Function
Function 1: IDENTIFY – Risk Management	**Consistently Implemented (Level 3)**	**No**
Function 2: PROTECT **Configuration Management** **Identity and Access Management** **Security Training**	**Defined (Level 2)** **Consistently Implemented (Level 3)** **Managed and Measurable (Level 4)**	**No**
Function 3: DETECT – ISCM	**Consistently Implemented (Level 3)**	**No**
Function 4: RESPOND – Incident Response	**Managed and Measurable (Level 4)**	**Yes**
Function 5: RECOVER – Contingency Planning	**Managed and Measurable (Level 4)**	**Yes**

Source: TIGTA's evaluation of security program metrics which determined whether cybersecurity functions were rated "effective" or "not effective."

The Cybersecurity Framework function areas of RESPOND and RECOVER were rated as "effective"

The FY 2017 Inspector General FISMA Reporting Metrics specified that, within the context of the maturity model evaluation process, maturity level 4, *Managed and Measurable*, represents an effective level of security. For the five Cybersecurity Framework function areas, we found that two areas, RESPOND and RECOVER, and their two security program areas, Incident Response and Contingency Planning, respectively, achieved a *Managed and Measurable* maturity level 4 and therefore were deemed as "effective." The details of the results of our evaluation of the maturity levels are presented on pages 24 and 26, respectively.

For the remaining three Cybersecurity Framework function areas, four of their five security program areas did not meet a managed and measurable maturity level for the reasons presented in the next three sections of the report. As a result, these function areas were deemed as "not effective." The details of the results of our evaluation of these three maturity levels are presented on pages 8, 13, 17, 20, and 22, respectively.

The Cybersecurity Framework function area of IDENTIFY was rated as "not effective"

Based on the FY 2017 Inspector General FISMA Reporting Metrics, we found that the function area IDENTIFY and its security program area, Risk Management, met a *Consistently Implemented* maturity level 3. In order for the IRS to meet a *Managed and Measurable* maturity level 4 (and therefore an effective level), we believe that the IRS needs to improve on the following risk management program performance metrics.

- Maintain a comprehensive and accurate inventory of its information systems (including cloud systems).
- Maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.
- Maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting.
- Ensure that plans of action and milestones (POA&M) are used to effectively mitigate security weaknesses.
- Implement an automated solution that provides a centralized enterprise-wide view of risks, including risk control and remediation activities, dependencies, risk scores, and management dashboards.

The Cybersecurity Framework function area of PROTECT was rated as "not effective"

The function area PROTECT is made up of three security program areas: Configuration Management, Identity and Access Management, and Security Training. Based on the FY 2017 Inspector General FISMA Reporting Metrics, we found that the performance metrics for Security Training achieved a *Managed and Measurable* maturity level 4 and was therefore considered "effective." However, the security program area of Identity and Access Management rated at a *Consistently Implemented* maturity level 3, and the security program area of Configuration Management rated at a *Defined* maturity level 2. As a result, both of these program areas were considered "not effective." Therefore, because two of the three program areas were "not effective," we rated the entire area as "not effective," and the end result for this function area was a maturity level 3.

In order for the IRS to meet an effective level for the Identity and Access Management program area, we believe the IRS needs to improve on the following performance metrics:

- Ensure that all nonprivileged and privileged users use strong authentication to access IRS facilities, networks, and information systems, including remote access.
- Employ automated mechanisms to support the management of privileged accounts.
- Implement Federally compliant encryption on all remote access connections.

In order for the IRS to meet an effective level for the Configuration Management program area, we believe the IRS needs to improve on the following performance metrics:

- Complete and approve configuration management plans for all IRS organizations.
- Maintain baseline (and common secure) configurations consistently on information systems, and maintain inventories of related components at a level of granularity necessary for tracking and reporting.
- Ensure timely remediation of information system vulnerabilities and patching.
- Implement change control policies, procedures, and processes consistently IRS-wide.

The Cybersecurity Framework function area of DETECT was rated as "not effective"

Based on the FY 2017 Inspector General FISMA Reporting Metrics, we found that the function area DETECT and its security program area, ISCM, met a *Consistently Implemented* maturity level 3. In order for the IRS to meet an effective level for the ISCM program area, we believe the IRS needs to improve on the following performance metrics:

- Use the NIST *National Institute for Cybersecurity Education Framework* to define ISCM roles and responsibilities and map to Cybersecurity organization employees, complete a

skills assessment, and make targeted training recommendations in order to support a workforce capable of meeting the IRS's cybersecurity needs.

- Consistently capture qualitative and quantitative performance measures on the effectiveness of its ISCM program.

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.

TIGTA's responses to the DHS's FY 2017 Inspector General FISMA Reporting Metrics

The details of the results of our evaluation of the maturity level of each of the FY 2017 Inspector General FISMA Reporting Metrics are provided below. The metrics are based on Federal Government guidance and criteria, such as NIST Special Publication 800-53 and OMB memoranda. See the embedded guidance in Appendix I for the specific references for each metric. For metrics we rated lower than a maturity level 4, we have provided comments to explain the reasons why. The overall function area rating is based on a simple majority of all performance metrics. However, we also considered agency-specific factors when determining final ratings, as instructed by the FY 2107 Inspector General FISMA Reporting Metrics.

Function 1: IDENTIFY – Risk Management

Function	Count
Ad-Hoc	**0**
Defined	**5**
Consistently Implemented	**4**
Managed and Measurable	**3**
Optimized	**0**
Function Rating: Consistently Implemented (Level 3)	

1. Does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems) and system interconnections?

   Maturity Level: **Defined (Level 2)** – The organization has defined, but not consistently implemented, a process to develop and maintain a comprehensive and accurate inventory of its information systems and system interconnections.

Comments: TIGTA reported[6] that the IRS had not identified or formalized specific cloud inventory management processes.

2. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting?

   Maturity Level: **Defined (Level 2)** – The organization has defined, but not consistently implemented, a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.

   Comments: TIGTA[7] and the GAO[8] reported instances of inaccurate inventory, including the lack of detailed information necessary for tracking and reporting.

3. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?

   Maturity Level: **Defined (Level 2)** – The organization has defined, but not consistently implemented, a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment with the detailed information necessary for tracking and reporting.

   Comments: TIGTA reported[9] that, while the IRS is in the early stages of establishing a framework for software asset management, the IRS has not compiled a reliable baseline inventory of software licenses or documented cost savings and cost avoidance attributable to improved software license management in accordance with recent laws and regulations.

4. To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions?

   Maturity Level: **Consistently Implemented (Level 3)** – Information on the organization's defined importance/priority levels for its missions, business functions, and information is consistently used and integrated with other information security areas to guide risk management activities and investments in accordance with applicable requirements and guidance.

[6] TIGTA, Ref. No. 2017-20-032, *The Internal Revenue Service Does Not Have a Cloud Strategy and Did Not Adhere to Federal Policy When Deploying a Cloud Service* (Aug. 2017).
[7] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017).
[8] GAO, GAO-17-140, *Financial Audit: IRS's Fiscal Years 2016 and 2015 Financial Statements* (Nov. 10, 2016).
[9] TIGTA, Ref. No. 2017-20-062, *The Internal Revenue Service Is Not in Compliance With Federal Requirements for Software Asset Management* (Sept. 2017).

Comments: This is the highest level for this metric.

5. To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that include the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk?

   Maturity Level: **Managed and Measurable (Level 4)** – The organization monitors and analyzes its defined qualitative and quantitative performance measures on the effectiveness of its risk management strategy across disciplines and collects, analyzes, and reports information on the effectiveness of its risk management program. Data supporting risk management metrics are obtained accurately, consistently, and in a reproducible format.

6. Has the organization defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture to provide a disciplined and structured methodology for managing risk?

   Maturity Level: **Consistently Implemented (Level 3)** – The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. Security architecture reviews are consistently performed for new/acquired hardware/software prior to introducing systems into the organization's development environment.

   Comments: This is the highest level for this metric.

7. To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission-specific resources been defined and communicated across the organization?

   Maturity Level: **Managed and Measurable (Level 4)** – The organization utilizes an integrated risk management governance structure for implementing and overseeing an enterprise risk management capability that manages risks from information security, strategic planning and strategic reviews, internal control activities, and applicable mission/business areas.

8. To what extent has the organization ensured that the POA&Ms are utilized for effectively mitigating security weaknesses?

   Maturity Level: **Defined (Level 2)** – Policies and procedures for the effective use of the POA&Ms have been defined and communicated. These policies and procedures address, at a minimum, the centralized tracking of security weaknesses, prioritization of remediation efforts, maintenance, and independent validation of POA&M activities.

   Comments: The IRS is in the process of improving its POA&M tracking and remediation processes to ensure effective mitigation of security weaknesses. We reviewed 94 weaknesses

that the IRS identified during the annual testing of controls of the seven selected systems. Of the 94 weaknesses, we could not track 17 weaknesses to either existing or closed POA&Ms that supported effective remediation. The IRS created the POA&Ms for 13 of these 17 weaknesses after we asked about them.

We also reviewed 22 POA&Ms that were closed in FY 2017 related to the seven selected systems. Of the 22 POA&Ms that were closed, three POA&Ms were closed without sufficient support that the weaknesses were corrected, even though the IRS had validated the closures through its closure verification process. After we brought this to the IRS's attention, it has reopened two of them.

9. To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system-level risk assessments, including for identifying and prioritizing: (i) internal and external threats, including through use of the common vulnerability scoring system or other equivalent framework; ii) internal and external asset vulnerabilities, including through vulnerability scanning; iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities; and iv) selecting and implementing security controls to mitigate system-level risks?

   Maturity Level: **Consistently Implemented (Level 3)** – System risk assessments are performed and appropriate security controls are implemented on a consistent basis. The organization utilizes the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities.

   Comments: TIGTA reported[10] that the IRS was not timely correcting vulnerabilities identified by scans primarily due to the lack of resources and that improvements were needed over vulnerability remediation tracking, metrics, and an escalation process.

10. To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization ensures that information about risks is communicated in a timely and consistent manner to all internal and external stakeholders with a need to know. Furthermore, the organization actively shares information with partners to ensure that accurate, current information is being distributed and consumed.

    Comments: The IRS does not yet have the "robust diagnostics and reporting frameworks" required for the managed and measureable rating; its dashboard is in its infancy stage.

11. To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, Federal

[10] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017).

Acquisition Regulation[11] clauses, and clauses on protection, detection, and reporting of information) and Service Level Agreements[12] are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services?

Maturity Level: **Managed and Measurable (Level 4)** – The organization uses qualitative and quantitative performance metrics (*e.g.*, those defined within Service Level Agreements) to measure, report on, and monitor information security performance of contractor-operated systems and services.

12. To what extent does the organization utilize technology (such as a governance, risk management, and compliance tools) to provide a centralized, enterprise-wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?

    Maturity Level: **Defined (Level 2)** – The organization has identified and defined its requirements for an automated solution that provides a centralized, enterprise-wide view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.

    Comments: The IRS continues to work with the DHS to implement Continuous Diagnostic and Mitigation solutions.

13. Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the previous metrics. Taking into consideration the overall maturity level generated from the previous metrics and based on all testing performed, is the risk management program effective?

    Maturity Level: **Consistently Implemented (Level 3)** - Based on the performance results for metrics 1 through 12, this function was evaluated at a maturity level 3, *Consistently Implemented*.

    Comments: The IRS risk management program is not effective because it did not meet the managed and measurable maturity level.

[11] The Federal Acquisition Regulation is the primary regulation for use by all Federal executive agencies in their acquisition of supplies and services with appropriated funds.
[12] A Service Level Agreement is a contract between a service provider and its internal or external customers that documents what services the provider will furnish and defines the performance standards the provider is obligated to meet.

Function 2a: PROTECT – Configuration Management

Function	Count
Ad-Hoc	**0**
Defined	**6**
Consistently Implemented	**1**
Managed and Measurable	**1**
Optimized	**0**
Function Rating: Defined (Level 2)	

14. To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced?

    Maturity Level: **Managed and Measurable (Level 4)** – Staff are assigned responsibilities for developing and maintaining metrics on the effectiveness of information system configuration management activities. The organization's staff is consistently collecting, monitoring, analyzing, and updating qualitative and quantitative performance measures across the organization and is reporting data on the effectiveness of the organization's information system configuration management program to the Chief Information Security Officer.

15. To what extent does the organization utilize an enterprise-wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board or related body; configuration management processes, including processes for identifying and managing configuration items during the appropriate location within an organization's System Development Lifecycle;[13] configuration monitoring; and applying configuration management requirements to contracted systems?

    Maturity Level: **Defined (Level 2)** – The organization has developed an organizationwide configuration management plan that includes the necessary components.

    Comments: The IRS has developed a configuration management plan template that meets standards; however, only four of seven IRS organizational divisions have completed and approved configuration management plans.[14]

[13] System Development Lifecycle is a conceptual model used in project management that describes the stages involved in an information system development project, from an initial feasibility study through maintenance of the completed application.
[14] The IRS's Metric or Key Performance Indicator for Configuration Management, July 18, 2017.

16. To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: The maturity level should take into consideration the maturity of metrics 17, 18, 19, and 21.)

    Maturity Level: **Defined (Level 2)** – The organization has developed, documented, and disseminated comprehensive policies and procedures for managing the configurations of its information systems. Policies and procedures have been tailored to the organization's environment and include specific requirements.

    Comments: While the IRS has defined policies and procedures for managing the configurations of its information systems, the IRS has not consistently implemented its policies and procedures, based on the maturity levels of metrics 17, 18, 19, and 21.

17. To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting?

    Maturity Level: **Defined (Level 2)** – The organization has developed, documented, and disseminated its baseline configuration and component inventory policies and procedures.

    Comments: While the IRS has defined baseline configurations, it has not ensured that its information systems consistently maintain the baselines or component inventories in compliance with IRS policy. The IRS's annual security testing of systems reported that three of the seven systems that we selected for the FY17 FISMA evaluation did not consistently maintain baseline configurations. In addition, TIGTA[15] and the GAO[16] reported instances of baseline configurations not being consistently implemented and inaccurate system component inventories.

18. To what extent does the organization utilize configuration settings/common secure configurations for its information systems?

    Maturity Level: **Defined (Level 2)** – The organization has developed, documented, and disseminated its policies and procedures in this area and developed common secure configurations (hardening guides) that are tailored to its environment. Further, the organization has established a deviation process.

    Comments: While the IRS has defined common secure configurations, it has not ensured that its information systems consistently maintain secure configuration settings in compliance with IRS policy. The IRS's annual security testing of systems reported that six of the seven systems that we selected for the FY17 FISMA evaluation did not maintain secure

[15] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017); and TIGTA, Ref. No. 2017-20-004, *Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners* (Oct. 2016).
[16] GAO, GAO-17-395, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 26, 2017).

configuration settings in accordance with IRS policy. Also, TIGTA[17] and the GAO[18] reported findings of systems that did not maintain secure configuration settings in accordance with agency policy. Further, the IRS's tool to assess configuration settings is not Security Content Automation Protocol–compliant.[19] In addition, the GAO reported that the mainframe tool only tests compliance with a limited subset of the agency's policies.

19. To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities?

    Maturity Level: **Defined (Level 2)** – The organization has developed, documented, and disseminated its policies and procedures for flaw remediation. Policies and procedures include processes for: identifying, reporting, and correcting information system flaws; testing software and firmware updates prior to implementation; installing security relevant updates and patches within organizationally defined time frames; and incorporating flaw remediation into the organization's configuration management processes.

    Comments: While the IRS has defined flaw remediation policies, including patching, it has not consistently implemented flaw remediation and patching on a timely basis. The IRS's annual security testing of systems reported that flaw remediation processes were not in place for four of the seven systems that we selected for the FY17 FISMA evaluation. Also, TIGTA[20] and the GAO[21] reported that the IRS did not remediate high-risk vulnerabilities or install security patches on systems in a timely manner. In addition, the IRS indicated that its enterprise patch management has a number of risks and challenges that cannot be appropriately addressed without the adoption and implementation of patch automation.

20. To what extent has the organization adopted the Trusted Internet Connection program to assist in protecting its network?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization has consistently implemented its Trusted Internet Connection–approved connections and critical capabilities that it manages internally. The organization has consistently implemented defined Trusted Internet Connection security controls, as appropriate, and implemented actions to ensure that

[17] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017); and TIGTA, Ref. No. 2017-20-004, *Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners* (Oct. 2016).
[18] GAO, GAO-17-395, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 26, 2017).
[19] A method for using specific standardized testing methods to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements.
[20] TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017); and TIGTA, Ref. No. 2017-20-004, *Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners* (Oct. 2016).
[21] GAO, GAO-17-140, *Financial Audit: IRS's Fiscal Years 2016 and 2015 Financial Statements* (Nov. 10, 2016); GAO, GAO-17-395, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 26, 2017).

all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate.

Comments: This is the highest maturity level for this metric.

21. To what extent has the organization defined and implemented configuration change control activities, including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the Configuration Control Board,[22] as appropriate?

    Maturity Level: **Defined (Level 2)** – The organization has developed, documented, and disseminated its policies and procedures for managing configuration change control. The policies and procedures address, at a minimum, the necessary configuration change control related activities.

    Comments: While the IRS has defined policy and procedures for managing configuration change control, these policy and procedures have not been consistently followed at the information system level. The IRS's annual security testing of systems reported that three of the seven systems that we selected for the FY17 FISMA evaluation did not have a documented change management process in place. In addition, TIGTA[23] and the GAO[24] both reported that the IRS did not follow its change management policy and procedures.

22. Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the previous metrics. Taking into consideration the maturity level generated from the previous metrics and based on all testing performed, is the configuration management program effective?

    Maturity Level: **Defined (Level 2)** – Based on the performance results for metrics 14 through 21, this function was evaluated at a maturity level 2, *Defined*.

    Comments: The IRS configuration management program is not effective because it did not meet the managed and measurable maturity level. The IRS anticipates that the implementation of the DHS's Continuous Diagnostic and Mitigation solution will improve its configuration management program. In the meantime, the IRS has made some improvements. In January 2016, the IRS implemented automated scanning of its firewall,

[22] A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system.
[23] TIGTA, Ref. No. 2017-20-029, *The Big Data Analytics General Support System Security Controls Need Improvement* (June 2017).
[24] GAO, GAO-17-454R, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Internal Control over Financial Reporting* (May 17, 2017).

router, and switches that updates a dashboard daily with compliance data. Also, the IRS has begun implementing components of IBM BigFix, which is being deployed as part of the DHS's Continuous Diagnostic and Mitigation solution.

Function 2b: PROTECT – Identity and Access Management

Function	Count
Ad-Hoc	**0**
Defined	**3**
Consistently Implemented	**5**
Managed and Measurable	**1**
Optimized	**0**
Function Rating: Consistently Implemented (Level 3)	

23. To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced?

    Maturity Level: **Consistently Implemented (Level 3)** – Stakeholders have adequate resources (people, processes, and technology) to effectively implement ICAM activities.

    Comments: The IRS indicated that, while it has resources to implement the ICAM, it has identified certain activities that would benefit from increased resources which would better support improved process efficiency and effectiveness.

24. To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization is consistently implementing its ICAM strategy and is on track to meet milestones.

    Comments: The IRS utilizes the Treasury Enterprise Identity Credential and Access Management 3–5 Year Roadmap to guide its ICAM initiatives and identify gaps.

25. To what degree have ICAM policies and procedures been defined and implemented? (Note: The maturity level should take into consideration the maturity of metrics 27 through 31)?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its policies and procedures for the ICAM, including for account management, separation of duties, least privilege, remote access management, identifier and authenticator management, and identification and authentication of non-organizational users. Further, the

organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policies, procedures, and processes to update the program.

Comments: The IRS follows the Department of the Treasury's policies and procedures for the ICAM as set forth in the Treasury Enterprise Identity, Credential, and Access Management 3–5 Year Roadmap.

26. To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems?

    Maturity Level: **Managed and Measurable (Level 4)** – The organization employs automation to centrally document, track, and share risk designations and screening information with necessary parties, as appropriate.

27. To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and nonprivileged users) who access its systems are completed and maintained?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. The organization utilizes more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate.

    Comments: This is the highest level for this metric.

28. To what extent has the organization implemented strong authentication mechanisms (Personal Identity Verification (PIV) or Level of Assurance 4 credential) for nonprivileged users to access the organization's facilities, networks, and systems, including for remote access?

    Maturity Level: **Defined (Level 2)** – The organization has planned for the use of strong authentication mechanisms for nonprivileged users of the organization's facilities, systems, and networks, including the completion of e-authentication risk assessments.

    Comments: The IRS has completed e-authentication risk assessments for 28 of its online applications, but only six of the 28 reassessed applications are currently using an appropriate level of assurance to authenticate users.

29. To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization has consistently implemented strong authentication mechanisms for privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets.

Comments: While the IRS reported that 100 percent of its privileged users are required to use PIV cards to access the IRS network, it reported that only eight of 136 internal systems are configured to require PIV cards. Therefore, it did not meet the managed and measurable maturity level for this metric.

30. To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed?

    Maturity Level: **Defined (Level 2)** – The organization has defined its processes for provisioning, managing, and reviewing privileged accounts. Defined processes cover approval and tracking, inventorying and validating, and logging and reviewing privileged users' accounts.

    Comments: In FY 2017, the GAO reported[25] that numerous authorization control deficiencies still exist in the IRS's computing environment, including not restricting system access based on "least privilege." The GAO reported that the IRS assigned database privileges to individual accounts instead of assigning the privileges to a specific role and that the IRS did not enable database logging, nor did it review, analyze, or report auditable and actionable events on a database supporting a tax payment system. The IRS plans to use the Continuous Diagnostic and Mitigation Phase 2 privilege management solution to enhance its privileged management process.

31. To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions?

    Maturity Level: **Defined (Level 2)** – The organization has defined its configuration/ connection requirements for remote access connections, including use of cryptographic modules, system time-outs, and how it monitors and controls remote access sessions.

    Comments: The IRS has not implemented encryption compliant with Federal Information Processing Standard Publication 140-2 on all its remote access connections.

32. 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 previous metrics. Taking into consideration the maturity level generated from the previous metrics

[25] GAO, GAO-17-395, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 26, 2017).

and based on all testing performed, is the Identity and Access Management program effective?

Maturity Level: **Consistently Implemented (Level 3)** – Based on the performance results for metrics 23 through 31, this function was evaluated at a maturity level 3, *Consistently Implemented*.

Comments: The IRS Identity and Access Management Program is not effective because it did not meet the managed and measurable maturity level.

Function 2c: PROTECT – Security Training

Function	Count
Ad-Hoc	**0**
Defined	**0**
Consistently Implemented	**1**
Managed and Measurable	**5**
Optimized	**0**
Function Rating: Managed and Measurable (Level 4)	

33. To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: This includes the roles and responsibilities for the effective establishment and maintenance of an organizationwide security awareness and training program as well as the awareness and training–related roles and responsibilities of system users and those with significant security responsibilities?

    Maturity Level: **Managed and Measurable (Level 4)** – The organization has assigned responsibility for monitoring and tracking the effectiveness of security awareness and training activities. Staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures on the effectiveness of security awareness and training activities.

34. To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization has conducted an assessment of the knowledge, skills, and abilities of its workforce to tailor its awareness and specialized training and has identified its skill gaps. Further, the organization periodically updates its assessment to account for a changing risk environment. In addition, the

assessment serves as a key input to update the organization's awareness and training strategy/plans.

Comments: The IRS has not yet addressed all of its identified knowledge, skills, and abilities gaps.

35. To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: The strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as e-mail advisories, intranet updates/wiki pages/social media, web-based training, phishing simulation tools), frequency of training, and deployment methods).

    Maturity Level: **Managed and Measurable (Level 4)** – The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

36. To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: The maturity level should take into consideration the maturity of metrics 37 and 38.)

    Maturity Level: **Managed and Measurable (Level 4)** – The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

37. To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: Awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, remote access practices, mobile device security, secure use of social media; phishing, malware, physical security, and security incident reporting.)

    Maturity Level: **Managed and Measurable (Level 4)** – The organization measures the effectiveness of its awareness training program by, for example, conducting phishing exercises and following up with additional awareness or training and/or disciplinary action, as appropriate.

38. To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures)?

    Maturity Level: **Managed and Measurable (Level 4)** – The organization obtains feedback on its security training content and makes updates to its program, as appropriate. In addition,

the organization measures the effectiveness of its specialized training program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary actions, as appropriate.

39. Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the previous metrics. Taking into consideration the maturity level generated from the previous metrics and based on all testing performed, is the security training program effective?

    Maturity Level: **Managed and Measurable (Level 4)** – Based on the performance results for metrics 33 through 38, this function was evaluated at a maturity level 4, *Managed and Measurable*.

    Comments: The IRS Security Training program is effective because overall it met the managed and measurable maturity level.

Function 3: DETECT – ISCM

Function	Count
Ad-Hoc	**0**
Defined	**2**
Consistently Implemented	**2**
Managed and Measurable	**1**
Optimized	**0**
Function Rating: Consistently Implemented (Level 3)	

40. To what extent does the organization utilize an ISCM strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organizationwide approach to the ISCM?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization's ISCM strategy is consistently implemented at the organization/business process and information levels. In addition, the strategy supports clear visibility into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captures lessons learned to make improvements to the ISCM strategy.

    Comments: The IRS did not provide information to support that the organization monitors and analyzes qualitative and quantitative measures on the effectiveness of its ISCM strategy.

41. To what extent does the organization utilize ISCM policies and procedures to facilitate organizationwide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and

monitoring of security controls; collecting security-related information required for metrics, assessments, and reporting; analyzing ISCM data; reporting findings; and reviewing and updating the ISCM strategy?

Maturity Level: **Consistently Implemented (Level 3)** – The organization's ISCM policies and procedures have been consistently implemented for the specified areas. The organization also consistently captures lessons learned to make improvements to ISCM policies and procedures.

Comments: The IRS did not provide information to support that the organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies and procedures and makes updates as appropriate.

42. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization?

Maturity Level: **Defined (Level 2)** – The organization has defined and communicated the structures of its ISCM team, roles and responsibilities of ISCM stakeholders, and levels of authority and dependencies.

Comments: The IRS is in the process of establishing a cybersecurity training plan to follow NIST Special Publication 800-181, *National Institute for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (August 2017). The *National Institute for Cybersecurity Education Framework* serves as a fundamental reference resource to support a workforce capable of meeting an organization's cybersecurity needs. It provides organizations with a common, consistent lexicon that categorizes and describes cybersecurity work. The framework contains seven categories, which are broken down into 30 specialty areas. The IRS Cybersecurity organization has developed a draft training plan with the next step to map Cybersecurity organization employees to the *National Institute for Cybersecurity Education Framework* and to make targeted training recommendations.

43. How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls?

Maturity Level: **Managed and Measurable (Level 4)** – The organization utilizes the results of security control assessments and monitoring to maintain ongoing authorizations of information systems.

44. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings?

Maturity Level: **Defined (Level 2)** – 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. In addition, the organization has defined the format of reports, frequency of reports, and tools used to provide information to individuals with significant security responsibilities.

Comments: The IRS is still in the process of implementing a data analysis tool and reporting system to achieve requirements for data collection, storage, analysis, retrieval, and reporting.

45. Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the previous metrics. Taking into consideration the maturity level generated from the previous metrics and based on all testing performed, is the ISCM program effective?

Maturity Level: **Consistently Implemented (Level 3)** – Based on the performance results for metrics 40 through 44, this function was evaluated at a maturity level 3, *Consistently Implemented*.

Comments: The IRS ISCM Program is not effective because it did not meet the managed and measurable maturity level.

Function 4: RESPOND – Incident Response

Function	Count
Ad-Hoc	**0**
Defined	**1**
Consistently Implemented	**2**
Managed and Measurable	**3**
Optimized	**1**
Function Rating: Managed and Measurable (Level 4)	

46. To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events? (Note: The overall maturity level should take into consideration the maturity of metrics 48 through 52.)

Maturity Level: **Defined (Level 2)** – The organization's incident response policies, procedures, plans, and strategies have been defined and communicated. In addition, the organization has established and communicated an enterprise-level incident response plan.

Comments: The IRS did not provide sufficient information to support that it is consistently capturing and sharing lessons learned, preventing it from achieving a *Consistently Implemented* maturity level 3.

47. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization?

Maturity Level: **Managed and Measurable (Level 4)** – The organization has assigned responsibility for monitoring and tracking the effectiveness of incident response activities. Staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures on the effectiveness of incident response activities.

48. How mature are the organization's processes for incident detection and analysis?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently utilizes its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements and analyzes precursors and indicators generated by, for example, the following technologies: intrusion detection/prevention, security information and event management, antivirus and antispam software, and file integrity checking software.

    Comments: The IRS did not provide sufficient information to support that it maintains a comprehensive baseline of network operations and expected data flows for users and systems, which prevented it from achieving a *Managed and Measurable* maturity level 4.

49. How mature are the organization's processes for incident handling?

    Maturity Level: **Optimized (Level 5)** – The organization utilizes dynamic reconfiguration (*e.g.*, changes to router rules, access control lists, and filter rules for firewalls and gateways) to stop attacks, misdirect attackers, and isolate components of systems.

50. To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner?

    Maturity Level: **Managed and Measurable (Level 4)** – Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.

51. To what extent does the organization collaborate with stakeholders to ensure that on-site technical assistance/surge capabilities can be leveraged for quickly responding to incidents and enter into contracts, as appropriate, for incident response support?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently utilizes on-site technical assistance/surge capabilities offered by the DHS or ensures that such capabilities are in place and can be leveraged when needed. In addition, the organization has entered into contractual relationships in support of incident response processes (*e.g.*, for forensic support) as needed. The organization is utilizing the DHS's Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its network.

    Comments: This is the highest maturity level for this metric.

52. To what degree does the organization utilize the following technology to support its Incident Response program?

- Web application protections, such as web application firewalls.
- Event and incident management, such as intrusion detection and prevention tools and incident tracking and reporting tools.
- Aggregation and analysis, such as security information and event management products.
- Malware detection, such as antivirus and antispam software technologies.
- Information management, such as data loss prevention.
- File integrity and endpoint and server security tools.

Maturity Level: **Managed and Measurable (Level 4)** – The organization uses technologies for 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.

53. Provide any additional information on the effectiveness (positive or negative) of the organization's Incident Response program that was not noted in the previous metrics. Taking into consideration the maturity level generated from the previous metrics and based on all testing performed, is the Incident Response program effective?

Maturity Level: **Managed and Measurable (Level 4)** – Based on the performance results for metrics 46 through 52, this function was evaluated at a maturity level 4, *Managed and Measurable*.

Comments: The IRS incident response program is effective because overall it met the managed and measurable maturity level.

Function 5: RECOVER – Contingency Planning

Function	Count
Ad-Hoc	**0**
Defined	**0**
Consistently Implemented	**2**
Managed and Measurable	**5**
Optimized	**0**
Function Rating: Managed and Measurable (Level 4)	

54. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority?

    Maturity Level: **Managed and Measurable (Level 4)** – The organization has assigned responsibility for monitoring and tracking the effectiveness of information system contingency planning activities. Staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures on the effectiveness of information system contingency planning program activities, including validating the operability of an information technology system or system component to support essential functions during a continuity event.

55. To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate? (Note: Assignment of an overall maturity level should take into consideration the maturity of metrics 56 through 60.)

    Maturity Level: **Managed and Measurable (Level 4)** – The organization understands and manages its information and communications technology supply chain risks related to contingency planning activities. As appropriate, the organization integrates information and communications technology supply chain concerns into its contingency planning policies and procedures, defines and implements a contingency plan for its information and communications technology supply chain infrastructure, applies appropriate information and communications technology supply chain controls to alternate storage and processing sites, and considers alternate telecommunication service providers for its information and communication technology supply chain infrastructure and to support critical information systems.

56. To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization incorporates the results of organizational and system-level business impact analyses into strategy and plan development efforts consistently. System-level business impact analyses are integrated with the organizational-level business impact analysis and include: characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. The results of the business impact analyses are consistently used to determine contingency planning requirements and priorities, including mission-essential functions/ high-value assets.

    Comments: This is the highest maturity level for this metric.

57. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?

Maturity Level: **Managed and Measurable (Level 4)** – The organization is able to integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency, as appropriate to deliver persistent situational awareness across the organization.

58. To what extent does the organization perform tests/exercises of its information system contingency planning processes?

    Maturity Level: **Managed and Measurable (Level 4)** – The organization employs automated mechanisms to more thoroughly and effectively test system contingency plans.

59. To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?

    Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements its processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and a redundant array of independent disks, as appropriate. Alternate processing and storage sites are chosen based upon risk assessments which ensure that the potential disruption of the organization's ability to initiate and sustain operations is minimized, and these sites are not subject to the same physical and/or cybersecurity risks as the primary sites. In addition, the organization ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site. Furthermore, backups of information at the user and system levels are consistently performed and the confidentiality, integrity, and availability of this information is maintained.

    Comments: This is the highest possible rating for this metric.

60. To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk-based decisions?

    Maturity Level: **Managed and Measurable (Level 4)** – Metrics on the effectiveness of recovery activities are communicated to relevant stakeholders, and the organization has ensured that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.

61. Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the previous metrics. Taking into consideration the maturity level generated from the previous metrics and based on all testing performed, is the contingency program effective?

    Maturity Level: **Managed and Measurable (Level 4)** – Based on the performance results for metrics 54 through 60, this function was evaluated at a maturity level 4, *Consistently Implemented.*

Comments: The IRS Contingency Planning program is effective because overall it met the managed and measurable maturity level.

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, 2016, to June 30, 2017. To accomplish our objective, we determined the maturity level for the metrics contained in the FY 2017 Inspector General FISMA Reporting Metrics (embedded in Appendix I) that pertain to the seven security program areas.

As instructed in the Reporting Metrics document, we determined the overall rating for each of the seven domains by a simple majority, by which the most frequent level across the metrics will serve as the domain rating. For example, if there are seven metrics in a domain, and the IRS receives *Defined* ratings for three of the metrics and *Managed and Measurable* ratings for four of the metrics, then the domain rating would be *Managed and Measurable*. However, we also considered agency-specific factors when determining final ratings, as instructed by the FY 2107 Inspector General FISMA Reporting Metrics. Inspectors General were required to provide comments explaining the rationale for why a given metric was rated lower than a maturity level 4, *Managed and Measurable*. 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 results into Cyberscope.[1]

I. Determine the effectiveness of the IRS's Risk Management program.

II. Determine the effectiveness of the IRS's Configuration Management program.

III. Determine the effectiveness of the IRS's Identity and Access Management program.

IV. Determine the effectiveness of the IRS's Security Training program.

V. Determine the effectiveness of the IRS's ISCM program.

VI. Determine the effectiveness of the IRS's Incident Response program.

VII. Determine the effectiveness of the IRS's Contingency Planning program.

[1] CyberScope, which was implemented in FY 2009, is the Federal repository for collecting FISMA data.

For the specific metrics within each program area, see the FY 2017 Inspector General FISMA Reporting Metrics embedded below:

Final FY 2017 OIG
FISMA Metrics v1.0 - !

We based our evaluation work, in part, on a representative subset of seven major IRS information systems. To select the representative subset of the IRS information systems, TIGTA follows the selection methodology that the Treasury Office of the Inspector General defined for the Department of the Treasury as a whole. We used the system inventory contained within the Treasury FISMA Information Management System of general support systems and major applications with a security classification of "Moderate" or "High" as the population for this subset. We used a random number table to select information systems within this population. Generally, if an information system gets selected that was selected in the past three FISMA reviews, we reselect for that system.

We also considered the results of TIGTA audits performed or completed during the FY 2017 FISMA evaluation period, as listed in Appendix IV, as well as audit reports from the GAO that contained results applicable to the FISMA metrics.

Appendix II

Major Contributors to This Report

Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Midori Ohno, Lead Auditor
Bret Hunter, Senior Auditor
Steven Stephens, Senior Auditor
Esther Wilson, Senior Auditor
Linda Cieslak, Information Technology Specialist

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
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Director, Office of Audit Coordination

Appendix IV

Information Technology Security-Related Audits Performed or Completed During the Fiscal Year 2017 Evaluation Period

1. TIGTA, Ref. No. 2017-2R-079, *Cybersecurity Act of 2015: Report on the Information Security Management Practices of the Internal Revenue Service* (Aug. 2016).
2. TIGTA, Ref. No. 2017-20-004, *Improvements Are Needed to Ensure the Protection of Data Transfers to External Partners* (Oct. 2016).
3. TIGTA, Ref. No. 2017-20-024, *Information Technology: Improvements Are Needed in Enterprise-Wide Disaster Recovery Planning and Testing* (June 2017).
4. TIGTA, Ref. No. 2017-20-029, *The Big Data Analytics General Support System Security Controls Need Improvement* (June 2017).
5. TIGTA, Ref. No. 2017-20-032, *The Internal Revenue Service Does Not Have a Cloud Strategy and Did Not Adhere to Federal Policy When Deploying a Cloud Service* (Aug. 2017).
6. TIGTA, Ref. No. 2017-20-049, *Analysis of Fiscal Year 2016 Additional Appropriations for Cybersecurity and Identity Theft Prevention Improvements* (Aug. 2017).
7. TIGTA, Ref. No. 2017-20-050, *The Computer Security Incident Response Center Is Preventing, Detecting, Reporting, and Responding to Incidents, but Improvements Are Needed* (Aug. 2017).
8. TIGTA, Ref. No. 2017-20-061, *The External Network Perimeter Was Generally Secure, Though the Security of Supporting Components Could Be Improved* (Sept. 2017).
9. TIGTA, Ref. No. 2017-20-062, *The Internal Revenue Service Is Not in Compliance With Federal Requirements for Software Asset Management* (Sept. 2017).
10. GAO, GAO-17-140, *Financial Audit: IRS's Fiscal Years 2016 and 2015 Financial Statements* (Nov. 10, 2016).
11. GAO, GAO-17-395, *Information Security: Control Deficiencies Continue to Limit IRS's Effectiveness in Protecting Sensitive Financial and Taxpayer Data* (July 26, 2017).
12. GAO, GAO-17-454R, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Internal Control over Financial Reporting* (May 17, 2017).