TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The IRS's Cybersecurity Program Was Not Effective for Fiscal Year 2026

September 15, 2026

Report Number: 2026-200-053

TIGTACommunications@tigta.treas.gov | www.tigta.gov

HIGHLIGHTS: The IRS's Cybersecurity Program Was Not Effective for Fiscal Year 2026

Final Audit Report issued on September 15, 2026 **Report Number 2026-200-053**

Why TIGTA Did This Audit

As part of the Federal Information Security Modernization Act of 2014 (FISMA) legislation, Offices of Inspectors General are required to perform annual assessments of each federal agency's information security programs and practices.

We assessed the effectiveness of the IRS's information security program.

Impact on Tax Administration

FISMA focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. In Fiscal Year 2025, the IRS collected nearly $5.3 trillion in gross taxes and processed 271.4 million tax returns and other forms, which represents a substantial amount of taxpayer personal and financial information. As the 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.

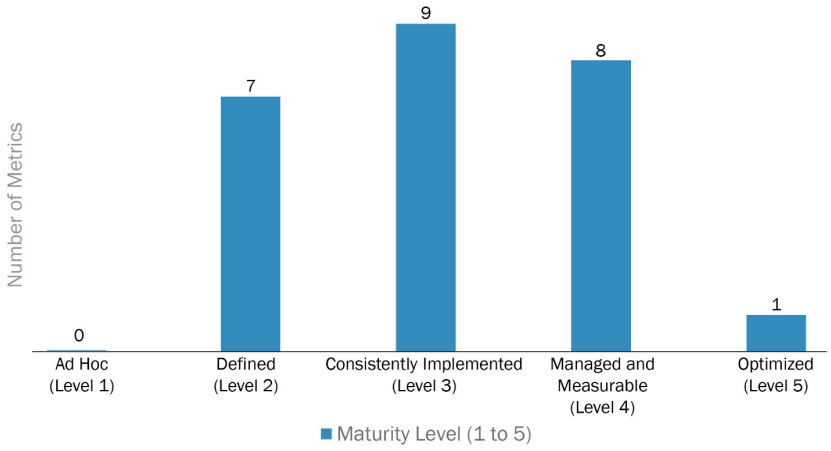
Within the IRS, the Information Technology organization's Cybersecurity function protects taxpayer information and electronic systems and services from internal and external, cybersecurity related threats. As threats grow in scale and sophistication, cybersecurity is critical to mission delivery and public trust.

What TIGTA Found

The IRS's Cybersecurity Program was considered not effective because three functions were not at an acceptable overall maturity level. Specifically, the IDENTIFY, PROTECT, and DETECT function areas were not effective. The remaining three function areas, GOVERN, RESPOND, and RECOVER were rated effective. The FISMA reporting metrics scoring methodology defines effective as being at a maturity Level 4, Managed and Measurable, or above.

In Fiscal Year 2026, we tested the 20 core reporting metrics, 5 supplemental metrics, and 10 editorial metrics. The editorial metrics provide additional information regarding the effectiveness (whether positive or negative) of the IRS's Cybersecurity Program areas.

72 Percent of the Metrics Were Rated at Advanced Levels (Levels 3, 4, or 5)



While the IRS has made some improvements over last fiscal year's reported maturity level ratings, we determined that the IRS needs to take further steps to improve its security program deficiencies. IRS Cybersecurity management needs to fully implement all security program components in compliance with FISMA requirements. For example, 86 percent (6 out of 7) of the sampled information systems had critical vulnerabilities not remediated within 30 days, as required. If the IRS does not take steps to mitigate these deficiencies, taxpayer data could be vulnerable to inappropriate and undetected use, modification, or disclosure.

What TIGTA Recommended

We do not make recommendations as part of our annual FISMA evaluation. We only report on the level of performance the IRS achieved using the guidelines for the applicable evaluation period. The IRS provided a response and disagreed with our assessment on the maturity of its Information Security Continuous Monitoring Program. Our analysis of this response is included in a separate appendix in this report.

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 15, 2026

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

FROM: Diana M. Tengesdal
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The IRS's Cybersecurity Program Was Not Effective for Fiscal Year 2026 (Audit No.: 2026200001)

This report presents the results of our Federal Information Security Modernization Act of 2014 evaluation of the Internal Revenue Service (IRS) for Fiscal Year 2026.[1] 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. This audit is included in our Fiscal Year 2026 Program Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data*.

The Treasury Inspector General for Tax Administration made no recommendations as a result of the work performed during this review. Management's complete response to the draft report and Office of Audit comments are included in Appendix III and IV, respectively.

This report is being forwarded to the Treasury Inspector General for consolidation into a report issued to the Department of the Treasury's Chief Information Officer.

If you have any questions, please contact me or Linna K. Hung, Assistant Inspector General for Audit (Security and Information Technology Services).

[1] Pub. L. No. 113-283, 128 Stat. 3073.

Table of Contents

Background

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.[1] It 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 that contractors provided or managed. FISMA assigns specific responsibilities to agency heads and Inspectors General in complying with its requirements and is supported by the Office of Management and Budget (OMB), the Department of Homeland Security, agency security policies, and risk-based standards and guidelines published by the National Institute of Standards and Technology (NIST) related to information security practices.

For example, FISMA directs federal agencies to report annually to the OMB, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency security policies, procedures, and practices, and compliance with FISMA. In addition, 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 agency Inspector General, or an independent external auditor as determined by the Inspector General, performs these independent evaluations. FISMA oversight for the Department of the Treasury (hereafter referred to as the Treasury Department) is performed by the Treasury Inspector General for Tax Administration (TIGTA) and the Treasury Office of Inspector General. TIGTA is responsible for oversight of the Internal Revenue Service (IRS) while the Treasury Office of Inspector General is responsible for all other Treasury Department bureaus. The Treasury Office of Inspector General has overall responsibility to combine the results for all the bureaus into one report for the OMB.

Overview of the IRS

The IRS's mission is to provide taxpayers with top quality service by helping them understand and meet their tax responsibilities and enforcing the law with integrity and fairness to all. In Fiscal Year 2025, the IRS collected nearly $5.3 trillion in gross taxes and processed 271.4 million tax returns and other forms. This represents a substantial amount of taxpayer personal and financial information. As the 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.

Within the IRS, the Information Technology organization's Cybersecurity function protects taxpayer information and electronic systems, and services, from internal and external cybersecurity related threats. As threats grow in scale and sophistication, cybersecurity is critical to mission delivery and public trust.

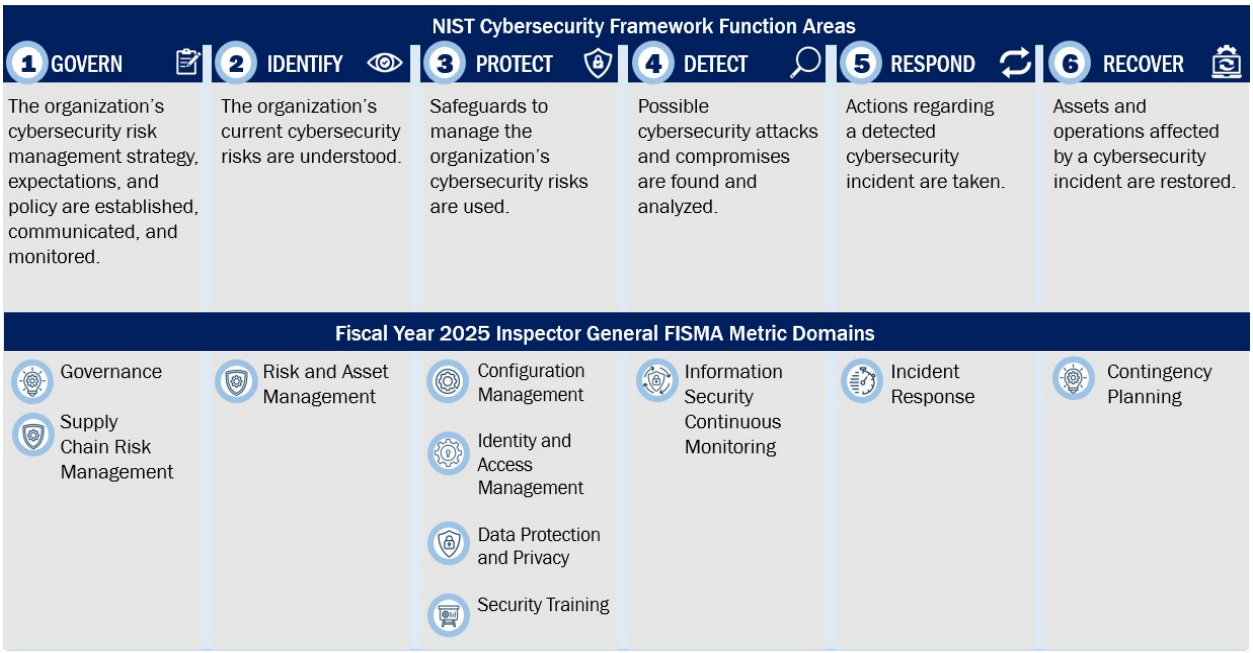
FISMA reporting metrics

Representatives from the OMB and Council of the Inspectors General on Integrity and Efficiency

[1] Pub. L. No. 113-283, 128 Stat. 3073.

coordinate annually to develop *Inspector General FISMA Reporting Metrics*. To meet the FISMA requirements for Fiscal Year 2026 FISMA, the representatives directed the Inspectors General to reuse the *Fiscal Year 2025 Inspector General FISMA Reporting Metrics*. Figure 1 presents the 6 functions in the NIST Cybersecurity Framework 2.0 (Cybersecurity Framework) areas and aligns each with the associated security program components (or metric domain).

Figure 1: Alignment of the Cybersecurity Framework Function Areas to the FISMA Reporting Metric Domains



Source: FISMA reporting metrics and the Cybersecurity Framework.

Twenty core metrics represent a combination of administration priorities and other high impact-security processes that must be evaluated annually. Specifically, these core metrics align with the Executive Order, *Improving the Nation's Cybersecurity*, and OMB security guidance.[2] In addition, five supplemental metrics contribute to the overall evaluation of the security program's effectiveness.

The Inspectors General are required to assess the overall maturity of the agency's information security program using the average rating of the individual function areas with the core and supplemental ratings averages independently. The OMB strongly encourages Inspectors General to focus on the results of the core metrics, as these tie directly to administration priorities and other high-risk areas.

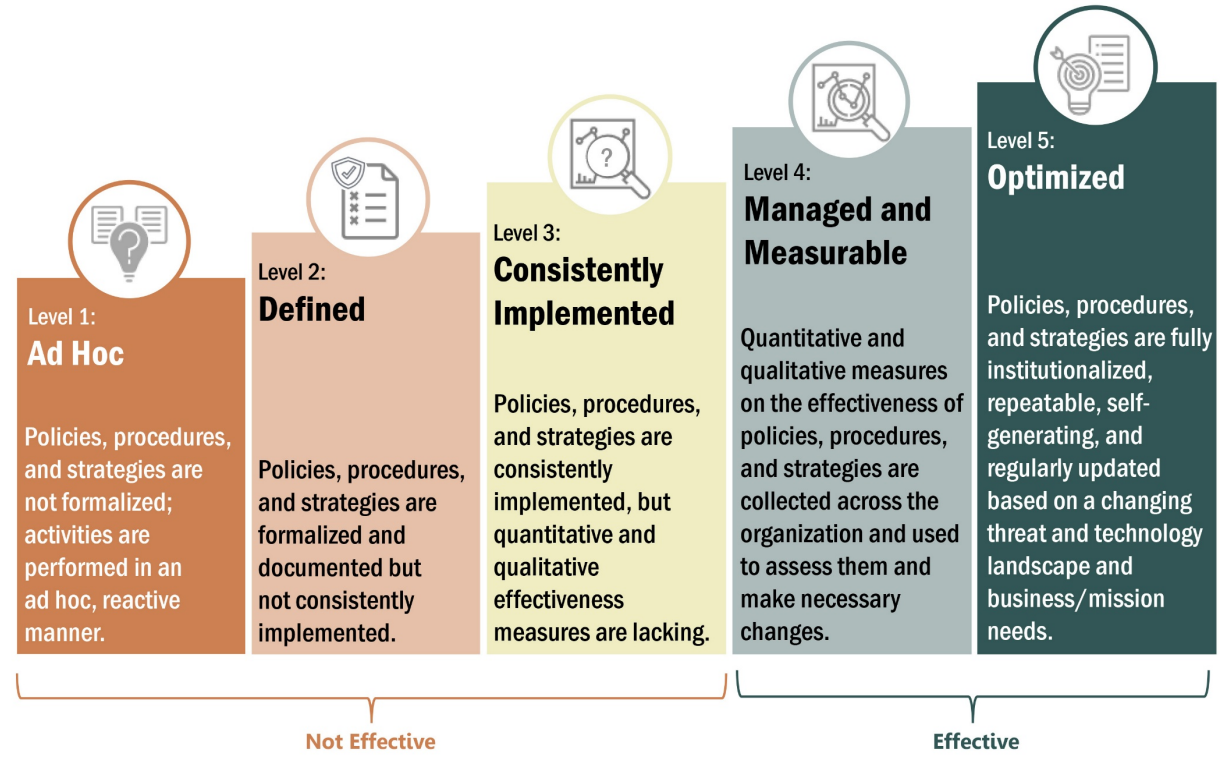
Inspectors General are required to assess the effectiveness of the information security program based on a maturity model spectrum.

[2] *Improving the Nation's Cybersecurity*, E.O. 14028, Fed. Reg. 26633 (May 12, 2021). OMB Memoranda: M-26-14, *Ensuring Effective and Efficient Logging and Network Visibility to Defend Against Evolving Cyber Threats* (May 2026); M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems Through Endpoint Detection and Response* (October 2021); M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 2022); and M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (September 2022).

- Foundational levels (*i.e.*, *Ad Hoc* and *Defined*) ensure that agencies develop sound policies and procedures.
- Advanced levels (*i.e.*, *Consistently Implemented* through *Optimized*) capture the extent that agencies implement those policies and procedures.

Maturity levels range from *Ad Hoc* for not having formalized policies, procedures, and strategies, to *Optimized* for fully institutionalizing sound policies, procedures, and strategies across the agency. Figure 2 details the five maturity levels: *Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized*. The scoring methodology defines "effective" as being at a maturity Level 4, *Managed and Measurable*, or above.

Figure 2: FISMA Assessment Maturity Levels



Source: FISMA reporting metrics.

Per the FISMA reporting metrics, the Inspectors General should use the calculated averages of the supplemental metrics to support their risk-based determination of overall program and function level effectiveness. The evaluation is completed using the results of cybersecurity evaluations, (*i.e.*, system security control reviews, vulnerability scanning, and penetration testing); the progress made by agencies to address outstanding Inspector General recommendations; and reported security incidents during the review period.

Results of Review

The Cybersecurity Program Was Not Effective in Three of the Six Cybersecurity Function Areas

We determined that for Fiscal Year 2026, the IRS's Cybersecurity Program was considered not effective because three function areas were not at an acceptable overall maturity level. Specifically, the IDENTIFY, PROTECT, and DETECT function areas were rated not effective. However, the remaining three function areas, GOVERN, RESPOND, and RECOVER were rated effective. Figure 3 includes the overall Cybersecurity Framework function area ratings averaged independently to determine the assessed maturity.

Figure 3: Fiscal Year 2026 Cybersecurity Framework Assessment Results

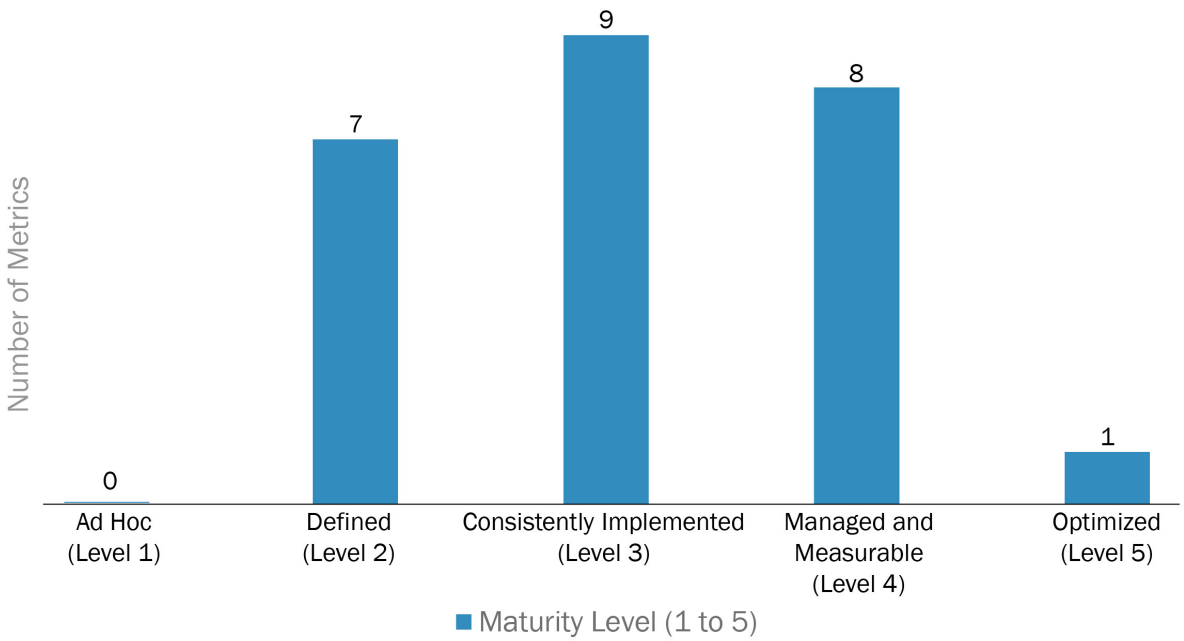
Function Area	Core	Supplemental	Assessed Maturity
GOVERN	4.0	3.3	Effective
IDENTIFY	3.0	2.0	Not Effective
PROTECT	2.6	N/A	Not Effective
DETECT	3.0	4.0	Not Effective
RESPOND	4.0	N/A	Effective
RECOVER	4.0	N/A	Effective
Overall Assessment	**Not Effective**		

Source: Evaluation of security program metrics.

For Fiscal Year 2026, we tested all 20 core reporting metrics and 5 supplemental metrics, and 10 editorial metrics. In determining the overall effectiveness of the IRS's information security program, we focused on the results of the Fiscal Year 2026 core metrics and used supplemental metrics to support the overall function level effectiveness. The editorial metrics provide additional information on the IRS's Cybersecurity program areas not previously discussed.

While the IRS has made some improvements over last fiscal year's reported maturity level ratings, we determined that the IRS needs to take further steps to improve its security program deficiencies. IRS Cybersecurity management needs to fully implement all security program components in compliance with FISMA requirements to protect taxpayer data from inappropriate and undetected use, modification, or disclosure. A summary of the IRS's maturity level distribution is provided in Figure 4.

Figure 4: 72 Percent of the Metrics Were Rated at Advanced Levels (Levels 3, 4, or 5)



Source: Evaluation of security program metrics.

The detailed results of our evaluation of the maturity level for each of the *Fiscal Year 2025 Inspector General Reporting Metrics* are provided below. We can use our discretion to determine if the IRS is effective in each of the Cybersecurity Framework function areas, even if it does not achieve a maturity Level 4, *Managed and Measurable*. In these instances, we have provided comments to explain our determinations. The effectiveness rating for core metrics and supplemental metrics averages was calculated independently based on the Cybersecurity Framework function areas. However, we also considered other factors to determine the final ratings, as instructed by the *Fiscal Year 2025 Inspector General FISMA Reporting Metrics*.

The GOVERN function area was effective

We found that the GOVERN function area and the respective domains, Governance and Supply Chain Risk Management (SCRM), met a core maturity level of 4.0 and a supplemental maturity level of 3.3, which we considered effective. Figure 5 presents the maturity level ratings for the assessed metrics.

Figure 5: Fiscal Year 2026 GOVERN Function Area Assessment Results

Metric	Domain	Metric Type	Rating
1	Governance	SUPPLEMENTAL	2
2	Governance	SUPPLEMENTAL	4
3	Governance	SUPLEMENTAL	4
5	SCRM	CORE	4
Core Average	**4.0**	**Supplemental Average**	**3.3**
Overall Assessment	**Effective**		

Source: Evaluation of security program metrics associated with the Cybersecurity Framework GOVERN function area.

Govern Function Area – Cybersecurity Governance	
1. To what extent does the organization develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize, and communicate its cybersecurity objectives?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Defined (Level 2) – The organization has defined policies and procedures for developing and maintaining current and target profiles that include, at a minimum, consideration of the organization's mission objectives, threat landscape, resources (including personnel), and constraints. The organization has determined the scope of its profiles (*e.g.*, entity level, division level, process level, system level).	• The IRS has not developed formal written procedures for developing and maintaining cybersecurity profiles. However, the IRS conducted biweekly reporting that tracked the current and target state cybersecurity profiles.
2. To what extent does the organization use a cybersecurity risk management strategy to support operational risk decisions?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Managed and Measurable (Level 4) – The organization uses qualitative and quantitative data to assess cybersecurity risk management effectiveness. Metrics, dashboards, and automated tools inform adjustments to the strategy. The organization's cyber risk management strategy integrates security and privacy programs with the management control systems established in the organization's enterprise risk management strategy.	None.
3. To what extent do cybersecurity roles, responsibilities, and authorities foster accountability, performance assessment, and continuous improvement?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Managed and Measurable (Level 4) – The organization has adequate resources that are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, policies, and profiles. The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its cybersecurity risk management roles, policies, and practices, and makes updates as appropriate. Cybersecurity objectives are included in the performance assessment process of those with significant cybersecurity responsibilities.	None.

4. Provide any additional information on the effectiveness (positive or negative) of the organization's cybersecurity governance program that was not noted in the questions above.

TIGTA COMMENTS

For the Fiscal Year 2026 FISMA cycle, the IRS:

- Reorganized the Information Technology division and developed a new Cybersecurity Strategic Plan in January 2026. In April 2026, the IRS formalized the first report request for the updated cybersecurity profiles.
- Established the Risk Executive function as a governance structure to view and analyze risk organization-wide.

Despite these achievements, the IRS's governance program can improve by:

- Formalizing a written process for developing and maintaining cybersecurity profiles. We also reported this as an area of improvement in the IRS Fiscal Year 2025 FISMA report.

Govern Function Area – Cybersecurity SCRM

5. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?

MATURITY LEVEL AND NARRATIVE	TIGTA COMMENTS
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 the Cybersecurity SCRM performance of organizationally defined products, systems, and services provided by external providers. In addition, the organization has incorporated supplier risk evaluations, based on criticality, into its continuous monitoring practices to maintain situational awareness into the cyber-related supply chain risks.	None.

6. Provide any additional information on the effectiveness (positive or negative) of the organization's SCRM Program that was not noted in the question above.

TIGTA COMMENTS

For the Fiscal Year 2026 FISMA cycle, the IRS:

- Made progress towards the final implementation of the SCRM process established in 2023. It plans to complete the first three comprehensive risk assessments by January 2027.

Despite these achievements, the IRS's SCRM program can improve by:

- Applying lessons learned from the comprehensive risk assessment pilot project to improve their processes.

The IDENTIFY function area was not effective

We found that the IDENTIFY function area and the respective domain, Risk and Asset Management, met a core maturity level of 3.0 and a supplemental maturity level of 2.0, which we considered not effective. Figure 6 presents the maturity level ratings for the assessed metrics.

Figure 6: Fiscal Year 2026 IDENTIFY Function Area Assessment Results

Metric	Domain	Metric Type	Rating
7	Risk and Asset Management	CORE	3
8	Risk and Asset Management	CORE	2
9	Risk and Asset Management	CORE	2
10	Risk and Asset Management	SUPPLEMENTAL	2
11	Risk and Asset Management	CORE	4
12	Risk and Asset Management	CORE	4
Core Average	**3.0**	**Supplemental Average**	**2.0**
Overall Assessment	**Not Effective**		

Source: Evaluation of security program metrics associated with the Cybersecurity Framework IDENTIFY function area.

Identify Function Area – Risk and Asset Management	
7. To what extent 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 AND NARRATIVE	**TIGTA COMMENTS**
Consistently Implemented (Level 3) – The organization consistently implements its policies, procedures, and processes for developing and maintaining an accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems) and system interconnections.	• In March 2025, we reported that the IRS should improve its annual validation process to ensure that all systems with Personally Identifiable Information and Federal Tax Information are consistently designated across multiple inventory systems, and that system owners are communicating changes to impacted groups. This recommendation is still open.[3] • In March 2026, the Government Accountability Office (GAO) reported that the IRS's artificial intelligence inventory did not always contain quality information and omitted use cases. The recommendations to mitigate these weaknesses are still open.

[3] See Appendix II for a list of information technology security-related audits considered during our Fiscal Year 2026 evaluation.

8. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including Government Furnished Equipment, Internet of Things, and Bring Your Own Device mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Defined (Level 2) – The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) with the detailed information necessary for tracking and reporting.	• The IRS has an open program level Plan of Action and Milestones (POA&M) for not having a tool that can detect the presence of unauthorized hardware assets and notifying appropriate organizational officials. We included a similar comment in the IRS Fiscal Year 2025 FISMA report.

9. 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 AND NARRATIVE	**TIGTA COMMENTS**
Defined (Level 2) – The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for executive order critical, cloud, and mobile software and applications used in the organization's environment with the detailed information necessary for tracking and reporting.	• The IRS has open program level POA&Ms for the following deficiencies. Specifically, the IRS does not have a tool that: ○ Prevents the execution of unauthorized programs on the network. ○ Administers the rules authorizing the terms and conditions of authorized software program usage. ○ Detects the presence of unauthorized software assets and notifies appropriate organizational officials. • According to the January 2026 Cybersecurity Strategic Plan, the IRS plans to implement a solution to prevent unauthorized software from operating on the network and strengthen overall network integrity and compliance posture by June 2027.

10. To what extent does the organization develop and maintain inventories of data and corresponding metadata for designated data types, as appropriate throughout the data lifecycle?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Defined (Level 2) – The organization has defined its policies, procedures, processes, and roles and responsibilities for developing and maintaining a comprehensive and accurate inventory data and corresponding metadata for its data types, as appropriate. This includes data obtained from third-party providers.	• The IRS's maturity level rating improved from *Ad Hoc* to *Defined* since the last FISMA review. • The IRS has not fully implemented metadata tagging for the six of seven sampled systems. For the remaining sampled system, metadata discovery scans are in progress.
11. To what extent does the organization ensure that information system security risks are adequately managed?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Managed and Measurable (Level 4) – The organization consistently monitors the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level. The organization ensures that information in cybersecurity risk registers is obtained accurately, consistently, and in a reproducible format and is used to: • Quantify and aggregate security risks. • Normalize cybersecurity risk information across organizational units. • Prioritize operational risk response.	None.
12. To what extent does the organization use technology/automation to provide a centralized, enterprise-wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Managed and Measurable (Level 4) – The IRS ensures that cybersecurity risk management information is integrated into enterprise management reporting tools (such as a governance, risk management, and compliance tool), as appropriate.	• The IRS's maturity level rating improved from *Consistently Implemented* to *Managed and Measurable* since the last review. • The IRS has an open program level POA&M for not having adequate procedures to assure that system owners consistently and timely create POA&Ms for identified weaknesses. However, the IRS demonstrated that it has a tool to provide an enterprise view of risk information that includes

	information on configuration compliance, vulnerability status, and risk registers.

13. Provide any additional information on the effectiveness (positive or negative) of the organization's risk and asset management program that was not noted in the questions above.

TIGTA COMMENTS

For the Fiscal Year 2026 FISMA cycle, the IRS:

- Added a unique system identifier to the IRS's FISMA master inventory, enterprise audit trail, and enterprise risk compliance tool inventory repositories. The addition of the system identifier will simplify reconciliation efforts to the authoritative inventory repository.
- Incorporated cybersecurity risk information into a centralized reporting tool.

Despite these achievements, the IRS's risk and asset management program has areas that need improvement, as follows:

- Strengthening commitment with owners of the various inventory management systems used to identify, and address or resolve discrepancies in a timely manner.
- Implementing corrective actions to close the open program level POA&Ms referenced in Metrics 8 and 9.

The PROTECT function area was not effective

We found that the PROTECT function area and the respective domains, Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training met a core maturity level of 2.6 that we considered not effective. The PROTECT function area did not have any supplemental metrics assigned for this FISMA cycle. Figure 7 represents the maturity level ratings for the assigned metrics.

Figure 7: Fiscal Year 2026 PROTECT Function Area Assessment Results

Metric	Domain	Metric Type	Rating
14	Configuration Management	CORE	3
15	Configuration Management	CORE	2
17	Identity and Access Management	CORE	3
18	Identity and Access Management	CORE	3
19	Identity and Access Management	CORE	3
21	Data Protection and Privacy	CORE	3
22	Data Protection and Privacy	CORE	2
24	Security Training	CORE	2
Core Average	**2.6**		
Overall Assessment	**NOT EFFECTIVE**		

Source: Evaluation of security program metrics associated with the Cybersecurity Framework PROTECT function area.

Protect Function Area – Configuration Management	
14. To what extent does the organization use configuration settings/common secure configurations for its information systems?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**

Consistently Implemented (Level 3) – The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on the principle of least functionality. Further, the organization consistently uses security content automation protocol-validated software assessing (scanning) capabilities against all systems on the network (in accordance with the Department of Homeland Security Binding Operational Directive 23-01) to assess and manage both code-based and configuration-based vulnerabilities.[4] The organization uses lessons learned in implementation to make improvements to its secure configuration policies and procedures.	• The IRS's maturity level rating improved from *Defined* to *Consistently Implemented* since the last FISMA review.
	• The IRS has defined configuration settings and common secure configurations.
	• 71 percent (5 of 7) of the 7 sampled systems were compliant with configuration settings. The compliance status of the remaining two systems was not verified. Cloud service providers manage these systems, and we were unable to obtain and review the required documentation due to timing constraints.
	• The IRS has six significantly overdue configuration settings POA&Ms that are not related to our sampled systems.
	• The IRS has open recommendations from our prior audit reports.
	  ○ In September 2021, we reported that configuration compliance controls were insufficient.
	  ○ In September 2024, we reported that the IRS should resolve configuration compliance settings in accordance with federal and IRS policies.

[4] Cybersecurity and Infrastructure Security Agency, BOD 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks* (October 2022).

15. To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management to manage software vulnerabilities on all network addressable internet protocol assets?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Defined (Level 2) – The organization has developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices. Policies and procedures include processes for: identifying, validating, reporting, and correcting information system flaws, testing software and firmware updates before implementation, installing security relevant updates and patches within organizational-defined time frames, and incorporating flaw remediation into the organization's configuration management processes.	• The IRS has policies and procedures to support flaw remediation and demonstrated the capability to scan for vulnerabilities for the seven sampled systems. • 86 percent (6 out of 7) of the sampled information systems had critical vulnerabilities that were not remediated within 30 days, as required. • The IRS did not provide an inventory of its critical software. Therefore, we were unable to determine if all critical software used vendor supported versions. • In September 2025, we reported that the IRS should timely remediate General Support Service Big Data Analytics vulnerabilities in accordance with IRS policies. This recommendation is still open.

16. Provide any additional information (positive or negative) of the organization's configuration management program that was not noted in the questions above.
TIGTA COMMENTS
For the Fiscal Year 2026 FISMA cycle, the IRS: • Achieved a 95 percent enterprise configuration compliance rate. Despite this achievement, the IRS's configuration management program can be improved by: • Prioritizing the remediation of vulnerabilities within required time frames, especially ones that are at a critical severity level or are known exploited vulnerabilities. • Establishing and implementing a repeatable process to ensure that it maintains an inventory of critical software.

Protect Function Area – Identity and Access Management	
17. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (*e.g.*, Personal Identity Verification, Fast Identity Online 2, or web authentication) for non-privileged users to access the organization's physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Consistently Implemented (Level 3) – The organization has consistently implemented strong authentication mechanisms for non-privileged users of the organization's physical and logical assets [organization-defined entry/exit points] and networks, including for remote access, in accordance with federal targets. For instances where it would be impractical to use the Personal Identity Verification card, the organization uses an alternative token (derived Personal Identity Verification credential) which can be implemented and deployed with mobile devices. Further, for public-facing systems that support multifactor authentication, users are provided with the option of using phishing-resistant multifactor authentication.	• The IRS's maturity level rating improved from *Defined* to *Consistently Implemented* since the last FISMA review. • As of March 2026, 93 percent (314 of 336) of systems were compliant with phishing-resistant multifactor authentication requirements. • In May 2026, the IRS reported that it completed 79 percent (329 of 417) of the required Enterprise Physical Access Control system installations.
18. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (*e.g.*, Personal Identity Verification, Fast Identity Online 2, or web authentication) for privileged users to access the organization's physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access.	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**

Consistently Implemented (Level 3) – The organization has consistently implemented strong authentication mechanisms for privileged users of the organization's physical and logical assets [organization-defined entry/exit points] and networks, including for remote access, in accordance with federal targets. For instances where it would be impractical to use the Personal Identity Verification card, the organization uses an alternative token (Derived Personal Identity Verification credential) which can be implemented and deployed with mobile devices.	• The IRS's maturity level rating improved from *Defined* to *Consistently Implemented* since the last FISMA review.
	• As of March 2026, 93 percent (314 of 336) of systems were compliant with phishing-resistant multifactor authentication requirements.
	• In April 2026, the GAO reported that the IRS did not:
	  ○ Have an effective process to recertify user access authorization for access to several systems.
	  ○ Consistently revoke user access authorization in a tool used to request and document user access to

	systems/application for employees placed on administrative leave. o Timely revoke network access privileges for employees placed on administrative leave.
19. 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 AND NARRATIVE	**TIGTA COMMENTS**
Consistently Implemented (Level 3) – The organization ensures that its process for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. The organization limits the functions that can be performed when using privileged accounts, limits the duration that privileged accounts can be logged in and ensures that privileged use activities are logged and periodically reviewed.	• The IRS's maturity level was lowered from *Managed and Measurable* to *Consistently Implemented* since the last FISMA review. • According to IRS Cybersecurity management, it has not fully migrated service accounts to a privileged account management system. As of June 2026, the IRS reported that it has 841 privileged service accounts spanning 313 systems that are managed outside of the IRS's privileged account management system. • In May 2026, we reported that the IRS: o Did not use a privileged account management system to manage privileged user accounts. o Had one privileged user with access to taxpayer data without approved access.
20. Provide any additional information (positive or negative) of the organization's identity and access management program that was not noted in the questions above.	
TIGTA COMMENTS	
For the Fiscal Year 2026 FISMA cycle, the IRS: • Continues to implement a physical access control system to selectively authorize or restrict access to facilities by March 2028 in response to Homeland Security Presidential Directive-12.[5] Despite these achievements, the IRS's identity and access management program has areas that need improvement, as follows: • Remediate 3 (11 percent) of the 27 public-facing systems that the IRS reported are not phishing-resistant multifactor authentication compliant.	

[5] Department of Homeland Security, *Homeland Security Presidential Directive-12* (August 2004).

Protect Function Area – Data Protection and Privacy	
21. To what extent has the organization implemented the following security controls to protect the confidentiality, integrity, and availability of its Personally Identifiable Information and other agency sensitive data, as appropriate, throughout the data lifecycle? This includes encryption of data at rest and in transit, sanitization of digital media before disposal or reuse, and access to personal email, external file sharing and storage sites, and personal communication applications are blocked, as appropriate.	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Consistently Implemented (Level 3) – The organization's policies and procedures have been consistently implemented for the specified areas, including (i) use of Federal Information Processing Standards-validated encryption of Personally Identifiable Information and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, (iii) destruction or reuse of media containing Personally Identifiable Information or other sensitive agency data, (iv) backups of Personally Identifiable Information, including protection and testing of backups, and (v) access to personal email, external file sharing and storage sites, and personal communication applications are blocked, as appropriate.	The IRS set an internal goal of implementing data at rest encryption for the full portfolio of IRS critical systems by the end of Fiscal Year 2024. However, as of April 2026, IRS Cybersecurity management reported that it has not fully implemented data at rest encryption on its systems. According to the IRS, the procurement and acquisition process will extend the completion timeline to Fiscal Year 2027.
22. To what extent has the organization implemented security controls (*e.g.*, Data Loss Prevention, Intrusion Detection and Prevention Systems, Cloud Access Security Broker, User and Entity Behavior Analytic tools, Security Information and Event Management, and Endpoint Detection and Response) to prevent data exfiltration and enhance network defenses?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Defined (Level 2) – The organization has defined and communicated policies and procedures for data exfiltration, endpoint detection and response, enhanced network defenses, email authentication processes, and mitigation against domain name system infrastructure tampering.	• As of May 2026, less than 1 percent of IRS assets are operating in an Internet Protocol Version 6-only environment. The OMB required 80 percent of assets on federal networks to operate in an Internet Protocol Version 6-only environment by the end of Fiscal Year 2025. However, the Department of the Treasury Chief Information Officer has directed the IRS to delay transitioning to Internet Protocol Version 6-only to avoid disruption of public services. • The IRS uses enterprise endpoint security controls to provide malware protection

	across supported platforms. However, the IRS currently does not have endpoint detection and response capabilities installed on 29 percent (2 of 7) high value asset systems.
23. Provide any additional information (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above.	
TIGTA COMMENTS	
For the Fiscal Year 2026 FISMA cycle, the IRS: • Closed all recommendations from our prior report on actions needed to be taken to improve its data loss prevention solution and reduce the risk of data exfiltration. Despite this, the IRS's data protection and privacy program needs improvement, as follows: • The IRS should establish a target date for compliance with the OMB requirement for its assets to operate in an Internet Protocol Version 6-only environment.	
PROTECT FUNCTION AREA – SECURITY TRAINING	
24. To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide specialized security training within the functional areas of: govern, identify, protect, detect, respond, and recover?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Defined (Level 2) – The organization has defined its processes for assessing the knowledge, skills, and abilities of its workforce to determine its specialized training needs and periodically updating its assessment to account for a changing risk environment.	• The IRS has defined its processes for assessing the knowledge, skills, and abilities of its workforce. However, the IRS is required to assess its entire information technology workforce every two years. The last assessment was conducted in Fiscal Year 2023. However, in June 2026, the IRS initiated the Fiscal Year 2026 skills assessment.
25. Provide any additional information (positive or negative) of the organization's security training program that was not noted in the questions above.	
TIGTA COMMENTS	
For the Fiscal Year 2026 FISMA cycle, the IRS: • Closed an open recommendation in July 2025 from a prior GAO report to fully implement information technology workforce planning practices. Despite this, the IRS's security training program needs improvement, as follows: • The IRS needs to complete the Fiscal Year 2026 skills assessments.	

The DETECT function area was not effective

We found that the DETECT function area and the respective domain, Information Security Continuous Monitoring (ISCM), met a core maturity level of 3.0 and a supplemental maturity level of 4.0, which we considered not effective. Figure 8 presents the maturity level ratings for the assessed metrics.

Figure 8: Fiscal Year 2026 DETECT Function Area Assessment Results

Metric	Domain	Metric Type	Rating
26	ISCM	CORE	3
27	ISCM	SUPPLEMENTAL	4
28	ISCM	CORE	3
Core Average	**3.0**	**Supplemental Average**	**4.0**
Overall Assessment	**Not Effective**		

Source: Evaluation of security program metrics associated with the Cybersecurity Framework DETECT function area.

DETECT FUNCTION AREA – ISCM	
26. To what extent does the organization use ISCM policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Consistently Implemented (Level 3) – The organization's ISCM policies and strategy are consistently implemented at the organization, business process, and information system levels. In addition, the strategy supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captures lessons learned to make improvements to the ISCM policies and strategy.	• Due to the recent reorganization, the IRS was unable to maintain an updated organization-wide ISCM strategy. It plans to update the organization-wide strategy in FISMA Fiscal Year 2027.
27. To what extent does the organization monitor and measure the integrity and security posture of all owned and associated assets?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Managed and Measurable (Level 4) – The organization uses up-to-date cyber threat intelligence in log analysis tools to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise. Further, manual reviews are conducted for technologies that cannot be sufficiently monitored through automation. The organization automates both inventory collection (including endpoint monitoring on all standard user devices) and anomaly detection to detect unauthorized devices.	• The IRS's maturity level rating improved from *Consistently Implemented* to *Managed and Measurable* since the last FISMA review.

28. To what extent does the organization perform ongoing (continuous monitoring) information system assessments to grant system authorizations, including developing and maintaining system security plans, and monitoring system security controls?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Consistently Implemented (Level 3) – The organization consistently implements its system level continuous monitoring strategies and related processes, including performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring security controls to provide a view of the organizational security posture, as well as each system's contribution to said security posture. In conjunction with the overall ISCM strategy, all security control classes (management, operational, and technical) and types (common, hybrid, and system-specific) are assessed and monitored, and their status updated regularly (as defined in the agency's information security policy) in security plans.	• The IRS has defined its process for performing ongoing security control assessments. However, it has not fully assessed NIST, Special Publication 800-53 Rev. 5 security and privacy controls for its cloud systems.[6] IRS Cybersecurity management stated that the IRS expects to fully assess cloud systems by FISMA Fiscal Year 2027. • At the start of FISMA Fiscal Year 2026, the assessment teams began using a tool to automate completion of the security controls assessments. Using this tool, the IRS captured the assessment results on one-third of the NIST Special Publication 800-53 Rev. 5 controls. However, it has not completed assessment on the remaining two-thirds of the controls to monitor and provide a view of the organizational security posture. • The IRS has an open security program level POA&M on not having adequate procedures to reasonably assure that information system owners consistently created POA&Ms for identified weaknesses on a timely basis according to IRS policy.
29. Provide any additional information (positive or negative) on the organization's ISCM program that was not noted in the questions above.	
TIGTA COMMENTS	
For the Fiscal Year 2026 FISMA cycle: • The IRS is updating its security procedures to align with recent changes. Despite these achievements, the IRS's ISCM program needs improvement, as follows: • The IRS needs to fully establish automated analysis tools. The IRS stated that it is implementing a tool that will provide the capability to perform continuous control and system authorization. We also reported this as an area of improvement in the IRS Fiscal Year 2025 FISMA report.	

[6] NIST, Special Publication 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020).

The RESPOND function area was effective

We found that the RESPOND function area and the respective domain, Incident Response, met a core maturity level of 4.0, which we considered effective. The RESPOND function area did not have any supplemental metrics for this FISMA cycle. Figure 9 presents the maturity level ratings for the assessed metrics.

Figure 9: Fiscal Year 2026 RESPOND Function Area Assessment Results

Metric	Domain	Metric Type	Rating
30	INCIDENT RESPONSE	CORE	3
31	INCIDENT RESPONSE	CORE	5
Core Average	**4.0**		
Overall Assessment	**Effective**		

Source: Evaluation of security program metrics associated with the Cybersecurity Framework RESPOND function area.

Respond Function Area – Incident Response	
30. To what extent has the organization implemented processes related to incident detection and analysis?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Consistently Implemented (Level 3) – The organization consistently implements enterprise-wide policies, procedures, and processes for incident detection and analysis. In addition, the organization consistently uses its enterprise-wide 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 potential adverse events and indicators generated by, for example, the following enterprise-wide technologies: intrusion detection/prevention, security information and event management, antivirus and antispam software, and file integrity checking software. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident detection policies and procedures and making updates as necessary. In addition, the organization is meeting logging requirements at maturity Event Logging 1 (basic), in accordance with OMB Memorandum M-26-14.	• As of July 2026, the IRS reported that 4 percent (16 of 413) of IRS systems containing Personally Identifiable Information or Federal Tax Information are not sending audit logs to the IRS's security information and event management tool. This is an improvement from last year where we reported 53 (14 percent) of 389 IRS systems were not sending audit logs. • The IRS did not provide requested evidence to support that it maintains a comprehensive baseline of network operations and expected data flows for users and systems or use of performance metrics defined in the incident detection and analysis that is required to support a maturity level rating of *Managed and Measurable*.

31. To what extent has the organization implemented processes related to incident handling?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Optimized (Level 5) – The organization uses dynamic reconfiguration (*e.g.*, changes to router rules, access control lists, and filter rules for firewalls and gateways) to stop attacks, misdirect attackers, and to isolate components of systems.	None.
32. Provide any additional information (positive or negative) of the organization's incident response program that was not noted in the questions above.	
TIGTA COMMENTS	
For the Fiscal Year 2026 FISMA cycle: • The IRS Cyber Security Incident Response Center supports connecting incidents, assets, vulnerabilities, and risk factors to drive informed decision-making. Despite this, we identified an area that needs improvement: • The IRS does not use profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents.	

The RECOVER function area was effective

We found that the RECOVER function area and the respective domain, Contingency Planning, met a core maturity level of 4.0, which we considered effective. The RECOVER function area did not have any supplemental metrics for this FISMA cycle. Figure 10 presents the maturity level ratings for the assessed metrics.

Figure 10: Fiscal Year 2026 RECOVER Function Area Assessment Results

Metric	Domain	Metric Type	Rating
33	CONTINGENCY PLANNING	CORE	4
34	CONTINGENCY PLANNING	CORE	4
Core Average	**4.0**		
Overall Assessment	**Effective**		

Source: Evaluation of security program metrics associated with the Cybersecurity Framework RECOVER function area.

Recover Function Area – Contingency Planning	
33. To what extent does the organization ensure that the results of Business Impact Analyses are used to guide contingency planning efforts?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Managed and Measurable (Level 4) – The organization ensures that the results of organizational and system level Business Impact Analyses are integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets. As appropriate, the organization uses the results of its Business Impact Analyses in conjunction with its risk register to calculate potential losses and inform senior-level decision-making.	None.
34. To what extent does the organization perform tests/exercises of its information system contingency planning processes?	
MATURITY LEVEL AND NARRATIVE	**TIGTA COMMENTS**
Managed and Measurable (Level 4) – The organization employs automated mechanisms to test system contingency plans more thoroughly and effectively. In addition, the organization coordinates plan testing with external stakeholders (*e.g.*, Information and Communications Technology supply chain partners/providers,) as appropriate.	None.
35. Provide any additional information (positive or negative) of the organization's contingency planning program that was not noted in the questions above.	
TIGTA COMMENTS	
For the Fiscal Year 2026 FISMA cycle: • The IRS leveraged a platform for Business Impact Analyses and Information System Contingency Plans, as well as the IRS application used to assist with incident management activities. Despite this, the IRS's contingency planning has areas that need improvement. The IRS plans to: • Implement an overall Business Impact score for systems and applications in FISMA Fiscal Year 2027. The overall score will reflect the level of impact (*i.e.*, downtime of applications and systems) on the IRS's mission.	

- Update its process documentation to formally clarify the requirements of Business Impact Analyses as reflected in NIST Special Publication 800-34 Rev.1.[7] During the Initiation phase:
    - Business Impact Analyses must be completed.
    - Results of the Business Impact Analyses shall be used to develop the Information System Contingency Plan.
- Incorporate when Business Impact Analyses revision is required (*i.e.*, major application changes).

[7] NIST, Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010).

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the effectiveness of the IRS's information security program. To accomplish our objective, we:

- Evaluated the 20 core, 5 supplemental, and 10 additional editorial metric questions that pertain to the Cybersecurity Framework by reviewing program documentation and interviewing key subject matter experts. We determined the information security program rating by applying a calculated average. The FISMA reporting metrics allowed for some discretion on maturity rating based on other considerations. Some specific examples that allowed us to make these evaluations included the following:
    - Selected a representative sample of seven information systems to evaluate the implementation status of key security controls. To select the systems, we followed the selection methodology that the Treasury Office of Inspector General defined for the Treasury Department as a whole. We used the information system inventory reported in the IRS FISMA Master Inventory. As of December 2025, the inventory contained 188 systems that were considered operational with high and moderate security ratings. We used a random number generator to select information systems within this population. Generally, we excluded information systems that were selected in the past three FISMA reviews.
    - Reviewed and analyzed the IRS's Assessment, Authorization, and Risk Governance system reports with 1,473 active POA&Ms as of January 2026. In addition, we evaluated the POA&Ms that document weaknesses at the IRS program and system levels as part of the metrics assessments.
    - Assessed the status of applicable GAO and TIGTA audit recommendations that were open as of June 2026. This was done by reviewing reports generated by the Joint Audit Management Enterprise System.

Performance of This Review

This review was performed with information obtained from the Information Technology's Cybersecurity function located in the New Carrollton Federal Building in Lanham, Maryland during the period January through July 2026. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Data Validation Methodology

During this review, we relied on security documents and inventory reports. We performed tests to assess the reliability of the system documents and inventory reports obtained from the IRS.

We evaluated the data by (1) performing electronic testing of required data elements, (2) reviewing existing information about the data and the system that produced them, and (3) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for purposes of this report.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: OMB Memoranda; NIST Special Publications 800 series; Internal Revenue Manual policies and standard operating procedures related to information technology controls. We evaluated these controls by reviewing documentation provided by the Cybersecurity function and interviewing IRS subject matter experts. We compared the relevant data and evidence obtained through these interactions to the *Fiscal Year 2025 Inspector General FISMA Reporting Metrics.*

Appendix II

Information Technology Security-Related Audits Considered During Our Fiscal Year 2026 Evaluation and the Metrics to Which They Apply

1. TIGTA, Report No. 2021-20-063, **********Platform Management Needs Improvement* (September 2021) – Metric 14.[1]
2. TIGTA, Report No. 2024-200-048, *Actions Need to Be Taken to Improve the Data Loss Prevention Solution and Reduce the Risk of Data Exfiltration* (September 2024) – Metric 23.
3. TIGTA, Report No. 2024-200-057, *Security Vulnerability Management and Configuration Compliance of a General Support System and Major Application Need Improvement* (September 2024) – Metric 14.
4. TIGTA, Report No. 2025-200-009, *Systems Hosting Sensitive Data Lack Consistent Inventory Standards* (March 2025) – Metric 7.
5. TIGTA, Report No. 2025-200-038, *The Infrastructure Supporting the Big Data Analytics Platform Has Overdue and Unresolved System Vulnerabilities* (September 2025) – Metric 15.
6. TIGTA, Report No. 2025-200-037, *The IRS's Cybersecurity Program Was Not Effective for Fiscal Year 2025* (September 2025) – Metrics 4, 8, 10, 12, 14, 17, 18, 19, 27, 29, and 30.
7. TIGTA, Report No. 2026-200-010, *SharePoint Online Access and Security Controls Need Improvement* (March 2026) – Metric 19.
8. TIGTA, Report No. 2026-208-026, *The IRS Needs to Address Access Control Deficiencies for the Enterprise Data Platform* (May 2026) – Metric 19.
9. GAO, GAO-19-176, *Strategic Human Capital Management is Needed to Address Serious Risks to IRS's Mission* (March 2019) – Metric 25.
10. GAO, GAO-23-104719, *IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements* (January 2023) – Metric 8.
11. GAO, GAO-26-107522, *Artificial Intelligence: IRS Actions Needed to Address Skills Gaps, Information Quality, and Strategic Management* (March 2026) – Metric 7.
12. GAO, GAO-26-108898, *IRS Financial Reporting: Improvements Needed in Information System and Other Controls* (April 2026) – Metric 18.

[1] Redaction due to subject matter that might create a risk of circumvention of the law if publicly released.

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

August 31, 2026

MEMORANDUM FOR DIANA M. TENGESDAL
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya
Chief Information Officer
Kaschit D. Pandya
Digitally signed by Kaschit D. Pandya
Date: 2026.08.31 10:41:27 -04'00'

SUBJECT: Federal Information Security Modernization Act (FISMA) Audit 2026 Management Response
Draft Audit Report – The IRS's Cybersecurity Program Was Not Effective for Fiscal Year 2026 (Audit No.: 2026200001)

The Internal Revenue Service (IRS) appreciates the Treasury Inspector General for Tax Administration's (TIGTA) evaluation of the agency's cybersecurity program and its continued partnership in strengthening the security of IRS information systems. The IRS is committed to continuously improving its Information Security Continuous Monitoring (ISCM) program and values the observations provided through the FISMA evaluation.

While the IRS acknowledges the opportunities identified to improve documentation and traceability within certain program artifacts, the IRS assesses that the operational evidence supporting Metrics 26 and 28 demonstrates a Managed and Measurable (Level 4) maturity. The IRS offers the following perspective to provide additional context regarding the maturity of its ISCM program.

Metric 26: Information Security Continuous Monitoring Strategy

The ISCM strategy demonstrates the characteristics of a Managed and Measurable program as defined in the FY 2025 Inspector General FISMA Reporting Metrics, which were used to conduct the FY 2026 FISMA evaluation.

The ISCM Program Plan establishes an enterprise-wide continuous monitoring strategy aligned with National Institute of Standards and Technology (NIST) Special Publication 800 -137 and the NIST Risk Management Framework. The strategy defines governance responsibilities, establishes monitoring frequencies, integrates continuous monitoring with organizational risk management and ongoing authorization, and provides for recurring assessment of security controls.

The IRS further maintains quantitative performance measures through executive dashboards, FISMA reporting, ongoing authorization activities, annual and event-driven security control assessments, continuous vulnerability monitoring, and enterprise risk reporting. These activities provide measurable information that supports enterprise risk management and executive decision-making.

The IRS maintains that recent organizational changes did not require an update to the enterprise ISCM strategy. While the IRS Information Technology underwent organizational changes during the FY 2026 evaluation period, those changes did not materially alter the IRS's ISCM strategy, monitoring requirements, organizational tiers, or continuous monitoring approach. The ISCM strategy remained current, applicable, and documented within the ISCM Program Plan. The IRS's discussion of possible future documentation improvements was intended to address clarity and ease of review by potentially presenting the existing strategy in a separate document. It was not intended to convey that the strategy was outdated, incomplete, or required to be updated because of the reorganization.

Metric 28: Information System Continuous Monitoring

The ISCM capability likewise demonstrates characteristics consistent with a Managed and Measurable (Level 4) program. The IRS has implemented an enterprise continuous monitoring capability that combines automated security tools, recurring security and privacy control assessments, ongoing authorization, vulnerability management, configuration compliance monitoring, endpoint monitoring, and executive reporting to maintain ongoing awareness of organizational security posture.

Monitoring results are routinely incorporated into enterprise risk management activities, Plan of Action and Milestones management, executive dashboards, security control assessments, and remediation efforts to support continuous improvement and risk-informed decision-making. These activities provide quantitative information used to measure security performance and prioritize remediation across the enterprise. The IRS's operational implementation of its continuous monitoring program reflects mature governance, measurable performance, enterprise oversight, and continuous evaluation of security controls consistent with a Managed and Measurable program.

Closing Statement

The IRS remains committed to strengthening its cybersecurity program and appreciates TIGTA's feedback for continued improvement. The IRS will continue enhancing its governance documentation and program artifacts to improve traceability and transparency. At the same time, the IRS considers the operational capabilities of its ISCM program, including enterprise governance, quantitative performance measurement, automated monitoring, executive oversight, and continuous improvement, demonstrate a Managed and Measurable (Level 4) maturity for Metrics 26 and 28.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Houman Rasouli, Coordinating Director, Cybersecurity at (202) 317-7061.

Appendix IV

Office of Audit Comments

In its response, IRS management disagreed with our maturity level assessment for Metrics 26 (ISCM Strategy) and 28 (ISCM ongoing information system assessment). Both metrics correspond to the Cybersecurity Framework *DETECT* function area.

NIST Special Publication 800-137 requires organizations to establish a procedure for reviewing and modifying all aspects of the ISCM strategy.[1] This includes relevance of the overall strategy; accuracy in reflecting organizational risk tolerance; accuracy and correctness of measurement and applicability of metrics; reporting requirements; and monitoring and assessment frequencies.

- For Metric 26, to advance to a *Managed and Measurable* maturity level, the IRS would need to demonstrate that it updated its ISCM strategy and program plan that addresses requirements and activities within its organization. As previously stated, the IRS was unable to maintain an organization-wide strategy. The last IRS update to the strategy document was March 2025 and it references key roles that no longer exist within the IRS after its reorganization. In addition, the document includes software tools no longer used within the IRS. Based on our review of available information, the IRS has not fully met the intent of updating the ISCM strategy and program plan to support the activities in the IRS environment.
- For Metric 28, to advance to a *Managed and Measurable* maturity level, the IRS would need to demonstrate that all security and privacy controls are fully assessed and monitored to provide a view of the IRS's security posture. As previously stated, the IRS expects to fully assess the cloud systems by FISMA Fiscal Year 2027. In addition, the IRS implemented a tool to capture assessment results. However, it has not completed assessment on two-thirds of the controls. Based on our review of available information, the IRS has not fully assessed all the security and privacy controls.

[1] NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Systems and Organizations* (September 2011).

Appendix V

Abbreviations

FISMA	Federal Information Security Modernization Act
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
POA&M	Plan of Action and Milestones
SCRM	Supply Chain Risk Management
TIGTA	Treasury Inspector General for Tax Administration

To report fraud, waste, or abuse,
contact our hotline on the web at
https://www.tigta.gov/reportcrime-misconduct.

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at
TIGTACommunications@tigta.treas.gov.

Information you provide is confidential, and you may remain anonymous.