TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The IRS's Cybersecurity Program Was Not Effective for Fiscal Year 2025

September 10, 2025
Report Number: 2025-200-037

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

HIGHLIGHTS: The IRS's Cybersecurity Program Was Not Effective for Fiscal Year 2025

Final Audit Report issued on September 10, 2025 **Report Number 2025-200-037**

Why TIGTA Did This Audit

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

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

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 2024, the IRS collected nearly $5.1 trillion in gross taxes and processed almost 266.6 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.

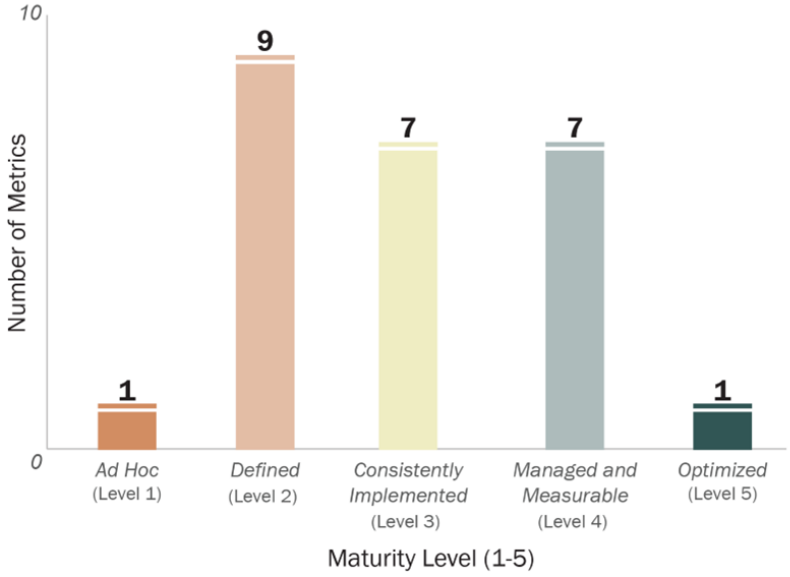
Within the IRS, the Information Technology organization's Cybersecurity function is responsible for protecting taxpayer information and electronic systems, and services from internal, and external, cybersecurity related threats. It does this by implementing security practices in planning, implementation, management, and operations.

What TIGTA Found

The IRS's Cybersecurity Program was considered not effective because three function areas were not at an acceptable maturity level. Specifically, the IDENTIFY, PROTECT, and DETECT function areas were rated 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 2025, we tested the 20 core reporting metrics, 5 new 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.

68 Percent of the Metrics Were Rated at Maturity Level 3 or Lower



We determined that the IRS needs to take further steps to improve its security program deficiencies and fully implement all security program components in compliance with FISMA requirements. For example, [redacted] 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 achieved by the IRS using the guidelines for the applicable evaluation period.

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 10, 2025

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

FROM: Diana M. Tengesdal
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The IRS's Cybersecurity Program Was Not Effective for Fiscal Year 2025 (Audit No.: 2025200001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Modernization Act of 2014 evaluation of the Internal Revenue Service (IRS) for Fiscal Year 2025.[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 and practices. This review is included in our Fiscal Year 2025 Annual Audit Plan and addresses the major management and performance challenge of *Protection of Taxpayer Data and IRS Resources*.

The Treasury Inspector General for Tax Administration made no recommendations as part of our results of the work performed during this evaluation. However, IRS officials had the opportunity to review the draft report prior to the issuance of this report.

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, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

[1] 44 U.S.C. §§ 3551-3558 (2018).

Table of Contents

Background ..... Page 1

Results of Review ..... Page 4

The IRS's Cybersecurity Program Was Not Effective in Three of the Six Cybersecurity Function Areas ..... Page 4

Appendices

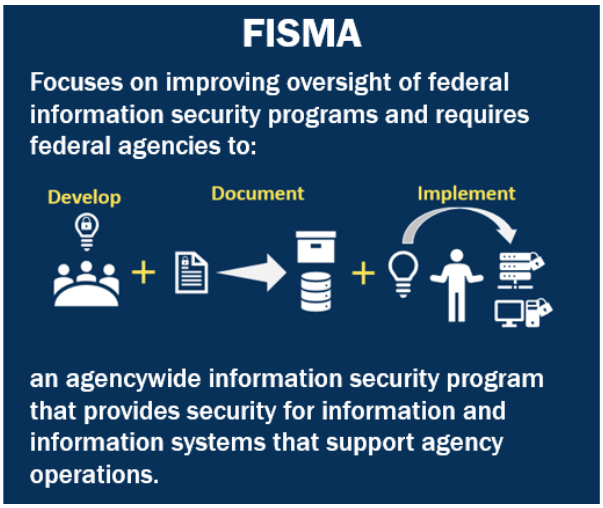
Appendix I – Detailed Objective, Scope, and Methodology ..... Page 24

Appendix II – Information Technology Security-Related Audits Considered During Our Fiscal Year 2025 Evaluation and the Metrics to Which They Apply ..... Page 26

Appendix III – Abbreviations ..... Page 27

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 provided or managed by contractors. 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 information 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. These independent evaluations are performed by the agency Inspector General, or an independent external auditor as determined by the Inspector General. 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 2024, the IRS collected nearly $5.1 trillion in gross taxes and processed almost 266.6 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.

[1] 44 U.S.C. §§ 3551-3558 (2018).

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. It does this by implementing security practices in planning, implementation, management, and operations. The Cybersecurity function also preserves the confidentiality, integrity, and availability of IRS systems and its data.

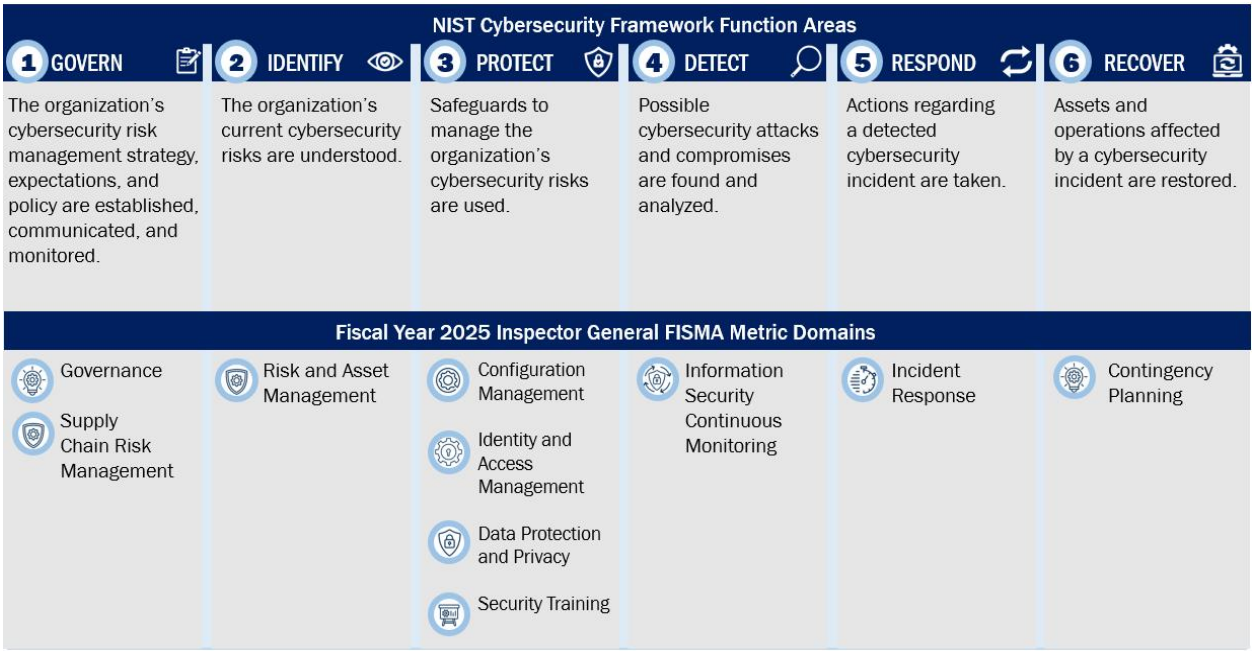
FISMA reporting metrics

Representatives from the OMB and the Council of the Inspectors General on Integrity and Efficiency coordinated to develop the *Fiscal Year 2025 Inspector General FISMA Reporting Metrics*. This year's FISMA guidance included several significant changes. Specifically, it included:

- A major update to the *NIST Cybersecurity Framework* (hereafter referred to as the Cybersecurity Framework).[2] The updated Cybersecurity Framework added a sixth new function area called Govern and realigned the Supply Chain Risk Management domain underneath it.
- Five new supplemental metric questions to contribute to the overall evaluation of the security program effectiveness.

Figure 1 presents the six Cybersecurity Framework function areas and aligns each with the associated security program components (or metric domains).

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 value controls that must be evaluated annually. Specifically, these core metrics align with the Executive

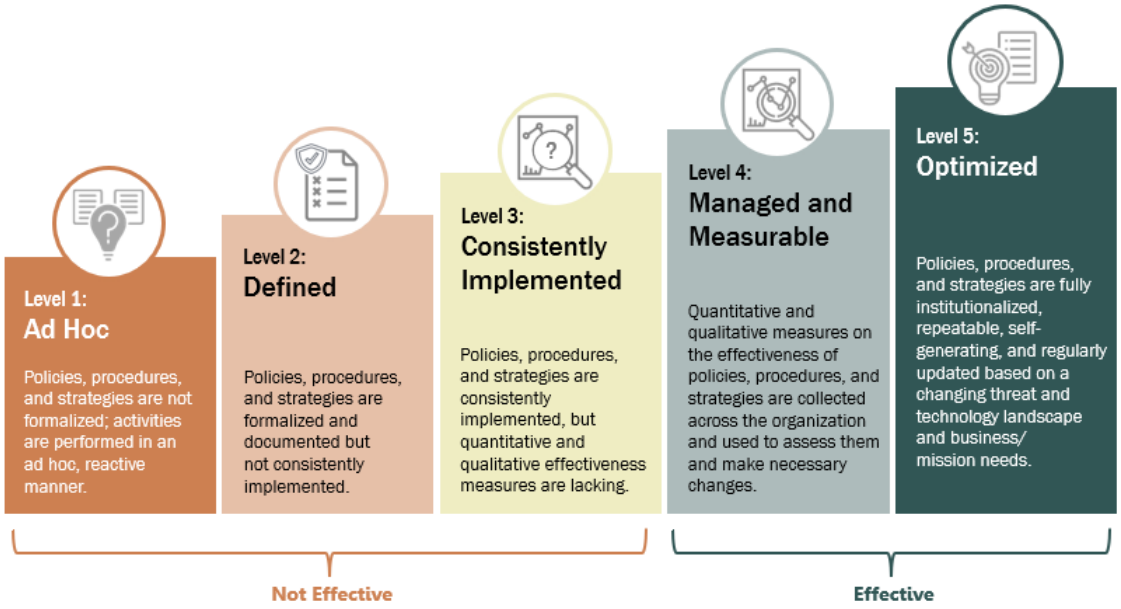
[2] *Fiscal Year 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.*0 (April 2025), and NIST, *Cybersecurity Framework (CSF) 2.0* (February 2024).

Order, *Improving the Nation's Cybersecurity*, and OMB cybersecurity guidance.[3] In addition, five new supplemental metrics were added to contribute to the overall evaluation of the security program 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 averaged 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. For example, the foundational levels (*i.e.*, Ad Hoc and Defined) ensure that agencies develop sound policies and procedures. Whereas the 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

[3] Executive Order 14028, *Improving the Nation's Cybersecurity* (May 2021) and OMB Memoranda: M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 2021); 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).

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 2025, the IRS's Cybersecurity Program was considered not effective because three function areas were not at an acceptable 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 2025 Cybersecurity Framework Assessment Results

FUNCTION AREA	CORE	SUPPLEMENTAL	ASSESSED MATURITY
GOVERN	4.0	3.3	EFFECTIVE
IDENTIFY	2.8	1.0	NOT EFFECTIVE
PROTECT	2.4	N/A	NOT EFFECTIVE
DETECT	3.0	3.0	NOT EFFECTIVE
RESPOND	4.0	N/A	EFFECTIVE
RECOVER	4.0	N/A	EFFECTIVE
OVERALL MATURITY			NOT EFFECTIVE

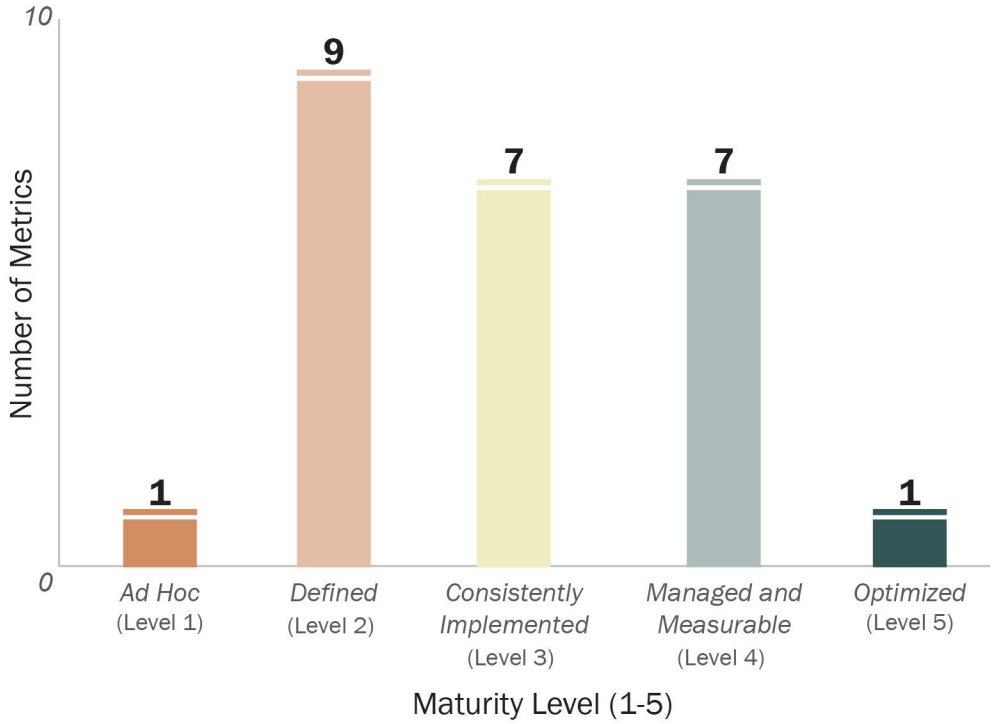
Source: Evaluation of security program metrics.

For Fiscal Year 2025, we tested all 20 core reporting metrics and 5 new supplemental metrics. In determining the overall effectiveness of the IRS's information security program, we focused on the results of the Fiscal Year 2025 core metrics and used the supplemental metrics to support the overall function level effectiveness.

We determined that the IRS needs to take further steps to improve its security program deficiencies and 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: 68 Percent of the Metrics Were Rated at Maturity Level 3 or Lower



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 were 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 2025 GOVERN Function Area Assessment Results

METRIC	DOMAIN	METRIC TYPE	RATING
1	GOVERNANCE	SUPPLEMENTAL	2
2	GOVERNANCE	SUPPLEMENTAL	4
3	GOVERNANCE	SUPPLEMENTAL	4
5	SCRM	CORE	4
CORE AVERAGE	4	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 profile(s) that includes, 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 profile(s) (*e.g.*, entity level, division level, process level, system level).	• The IRS has Internal Revenue Manual policies that support risk management. • The IRS has not developed detailed standard operating procedures to support the development of cybersecurity profiles. • The IRS did not provide evidence to demonstrate that the scope of the cybersecurity profiles has been determined.
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	None.

systems established in the organization's enterprise risk management strategy.	
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.	• The IRS can monitor qualitative and quantitative performance measures on the effectiveness of its cybersecurity risk management roles, policies, and practices as well as cybersecurity objectives in performance assessments. • For the first nine months, the IRS maintained adequate resources at the cybersecurity risk strategy leadership level. • The IRS is developing a reorganization plan that will streamline the Information Technology function during this FISMA cycle. • The IRS is currently reassessing roles and responsibilities to ensure that it continues to have adequate resources that are allocated commensurate with its cybersecurity risk strategy.
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 2025 FISMA cycle, the IRS: • Established a Cybersecurity Risk Management Strategy to communicate its cyber risk management objectives, priorities, constraints, risk appetite, and tolerance to inform organizational risk decision making. • Implemented enhancements to its Plan of Action and Milestones (POA&M) Analysis Dashboard to improve reporting capabilities. • Expanded database scanning coverage by 20 percent, providing consistent, accurate, and actionable database vulnerability scan results. Despite these achievements, the IRS's governance program can improve by: • Finalizing and formally approving standard operating procedures to support the development of cybersecurity profiles. • Working towards automating security assessments to reduce manual effort and provide continuous visibility into control implementation and system risks.	

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 2025 FISMA cycle, the IRS:

- Increased its maturity level rating from Defined (Level 2) to Managed and Measurable (Level 4) over a two-year period. To achieve these results, the IRS completed the following:
  - In October 2023, the IRS implemented its SCRM Program which included the procurement and implementation of an automated third-party risk management analysis tool to conduct risk assessments and continuous monitoring of its suppliers. The SCRM team completed 47 Supply Chain Risk Assessments for suppliers and another 17 assessments for proposed third-party vendor procurements by February 2024. As a result, we upgraded the maturity level rating to Consistently Implemented (Level 3) in the Fiscal Year 2024 FISMA report.
  - The SCRM team implemented an additional automated third-party risk management analysis tool and established a baseline quality control checklist to standardize reporting. The SCRM Program implemented the formal quality control effort in January 2025. In addition, the SCRM team provided examples of recurring supplier risk assessments to demonstrate that it has incorporated supplier risk evaluations into its continuous monitoring practices to maintain situational awareness into supply chain risks. As a result, we upgraded the maturity level rating to Managed and Measurable (Level 4) in the Fiscal Year 2025 FISMA report.

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

- Looking at ways to automate the current manual SCRM assessment and reporting process to improve efficiency and reduce the risk of data entry error.

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 2.8 and a supplemental maturity level of 1.0, which we considered not effective. Figure 6 presents the maturity level ratings for the assessed metrics.

Figure 6: Fiscal Year 2025 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	1
11	RISK AND ASSET MANAGEMENT	CORE	4
12	RISK AND ASSET MANAGEMENT	CORE	3
CORE AVERAGE	2.8	SUPPLEMENTAL AVERAGE	1
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 to maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems), and system interconnections.	• The IRS made progress addressing the findings from our prior report to ensure that its inventory systems were consistent despite potential system name differences.[4] • The owners of the authoritative inventory system regularly engaged stakeholders that maintain other inventory systems to discuss integration and address inventory discrepancies. • The IRS cannot produce a comprehensive and accurate inventory of all systems. Specifically, we compared the May 2025

[4] See Appendix II for a list of information technology security-related audits considered during our Fiscal Year 2025 evaluation.

	cloud inventory reports from two of its inventory systems and identified three cloud systems that were not in the IRS's authoritative inventory system. We cannot support a Managed and Measurable rating until we can validate that the IRS can provide a comprehensive and accurate inventory that does not have missing systems that qualify to be in the authoritative inventory system.

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 implemented a hardware management tool to maintain an up-to-date inventory of hardware assets. • [redacted] This POA&M has a revised due date of December 2025.

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 policies and procedures to develop and maintain an up-to-date inventory of software assets and licenses. • [redacted] • [redacted]

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**
Ad Hoc (Level 1) – The organization has not 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 started to develop Data and Metadata Inventory Standard Operating Procedures. However, the standard operating procedures lacked detail and were in draft status as of April 2025.
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**
Consistently Implemented (Level 3) – The organization consistently implements an automated solution across the enterprise that provides a centralized, enterprise-wide view of cybersecurity risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of cybersecurity risk	• The IRS developed an automated solution across the enterprise for cybersecurity risk management activities and is currently developing other reports to provide a centralized view of cybersecurity risks across the enterprise. • The IRS has configuration compliance and vulnerability scanning tools; however, these tools were not integrated into the

information are integrated into the solution.	enterprise-wide Governance Risk Compliance tool.[5] • The IRS is developing dashboards and reports to include Business Impact Analyses and Information Security Continuity Planning processes which will increase the timeliness of the data presented in the recently implemented Governance Risk Compliance tool.
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 2025 FISMA cycle, the IRS: • Provided an updated and signed Interconnections Systems Agreement to address an issue reported in the Fiscal Year 2024 FISMA review. • Made progress implementing a unique system identifier for its information systems. • Transitioned to a new system which contains comprehensive POA&M information. It also uses an online Risk-Based Decision tool to manage information security risks. Despite these achievements, the IRS's risk and asset management program has areas that need improvement, as follows: • Identify a plan to remediate open recommendations from our prior audit report. These recommendations include ensuring that controls are in place to verify assets are properly assigned to established groups and to reconcile assets to avoid duplicate accounting. • Make progress transitioning to existing tools which will help it verify [redacted] in a timely manner.	

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 2.4, which we considered not effective. The PROTECT function area did not have any supplemental metrics assigned for this FISMA cycle. Figure 7 presents the maturity level ratings for the assessed metrics.

[5] Software applications that can be used to manage policies, assess risk, control user access, and streamline compliance.

Figure 7: Fiscal Year 2025 PROTECT Function Area Assessment Results

METRIC	DOMAIN	METRIC TYPE	RATING
14	CONFIGURATION MANAGEMENT	CORE	2
15	CONFIGURATION MANAGEMENT	CORE	2
17	IDENTITY AND ACCESS MANAGEMENT	CORE	2
18	IDENTITY AND ACCESS MANAGEMENT	CORE	2
19	IDENTITY AND ACCESS MANAGEMENT	CORE	4
21	DATA PROTECTION AND PRIVACY	CORE	3
22	DATA PROTECTION AND PRIVACY	CORE	2
24	SECURITY TRAINING	CORE	2
CORE AVERAGE			2.4
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**
Defined (Level 2) – The organization has developed, documented, and disseminated its policies and procedures for configuration settings/common secure configurations. In addition, the organization has developed, documented, and disseminated common secure configurations (hardening guides) that are tailored to its environment. Further, the organization has established a deviation process.	• The IRS has defined configuration settings and common secure configurations. • Three of the seven sample information systems had overdue vulnerabilities or open POA&Ms for issues with configuration management. • [redacted]

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 prior to implementation, installing security relevant updates and patches within organizational-defined timeframes, 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. The IRS remediated 97 percent of the critical vulnerabilities within 30 days, as required. • [redacted] The IRS is required to use vendor supported versions for all critical software to attain a Consistently Implemented (Level 3) maturity level rating. • In September 2024, we reported that an [redacted] contained overdue vulnerabilities, and these recommendations were 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 2025 FISMA cycle, some of the IRS's noteworthy accomplishments include:

- Six of the seven sampled systems did not have any overdue configuration vulnerabilities.
- Evidence that the IRS uses lessons learned to make improvements to the flaw remediation process.

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

- [redacted]

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**
Defined (Level 2) – The organization has planned for the use of strong authentication mechanisms for non-privileged users of the organization's physical and logical assets [organization-defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.	• The IRS did not meet the OMB's goal for systems to use phishing resistant multifactor authentication to access applications used in its work by the end of Fiscal Year 2024. • In January 2025, the IRS reported a 3 percent increase and is projected to be at a 92 percent compliance rate by the end of September 2025.
18. To what extent has the organization implemented phishing-resistance 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**
Defined (Level 2) – The organization has planned for the use of strong authentication mechanisms for privileged users of the organization's physical and logical assets [organization-defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.	• The IRS did not meet the Fiscal Year 2024 deadline for systems to use phishing resistant multifactor authentication enterprise-managed identities to access the applications used in its work. • In addition, two of the seven sampled systems were not compliant with the multifactor authentication requirements.
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**
Managed and Measurable (Level 4) – The organization employs automated mechanisms (*e.g.*, machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.	None.

Further, the organization is meeting privileged identity and credential management logging requirements at maturity Event Logging 2, in accordance with OMB Memorandum M-21-31.	

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 2025 FISMA cycle, the IRS:

- Made progress addressing an open TIGTA recommendation on installing multifactor authentication card readers by upgrading 113 (62 percent) of 182 buildings to be Federal Identity, Credential, and Access Management compliant as of April 2025. The IRS stated that it is on track to be fully compliant by September 2025.
- Made progress addressing an open GAO recommendation on implementing and enforcing the use of Personal Identity Verification credentials when accessing the mainframe.
- [redacted]

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

- The IRS should work to close the open program level POA&M related to multifactor authentication dating back to October 2019.
- The IRS should prioritize resources to achieve the Treasury-wide goal of being 95 percent phishing resistant multifactor authentication compliant by September 2025. Phishing resistant multifactor authentication is designed to detect and prevent disclosure of information to a website or application posing as a legitimate system.

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 site, 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	• The IRS had 72 (19 percent) of 380 systems without current plans for data-at-rest encryption as of April 2025. • The IRS initially developed a two-phased approach to implement encryption of these systems. However, in June 2025, the IRS informed us that the Data at Rest Encryption program had been cancelled due to changing priorities.

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.	• [redacted]

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 2025, less than one percent of IRS assets are operating in an internet protocol version 6-only environment. OMB requires 80 percent of assets on federal networks to be operating in an internet protocol version 6-only environment by the end of Fiscal Year 2025. • [redacted]

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 2025 FISMA cycle, the IRS:

- [redacted]

Despite this, the IRS's data protection and privacy program needs improvement, as follows:

- [redacted]

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 current information technology skills assessment is several years old and has not been updated to account for a changing risk environment. • The IRS has an open recommendation from a prior GAO report to fully implement information technology workforce planning practices.
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 2025 FISMA cycle, the IRS: • Reported a 99 percent compliance status on mandatory Cybersecurity Awareness Training and Insider Threat briefings, and a 100 percent compliance for Specialized Information Technology Security Role-Based Training as of July 2025. Despite this, the IRS's security training program needs improvement, as follows: • The IRS has not provided evidence that it addresses identified knowledge, skills, and ability gaps through training or talent acquisition.	

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 3.0, which we considered not effective. Figure 8 presents the maturity level ratings for the assessed metrics.

Figure 8: Fiscal Year 2025 DETECT Function Area Assessment Results

METRIC	DOMAIN	METRIC TYPE	RATING
26	ISCM	CORE	3
27	ISCM	SUPPLEMENTAL	3
28	ICSM	CORE	3
CORE AVERAGE	3	SUPPLEMENTAL AVERAGE	3
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.	• The IRS is consistently implementing its ISCM policies and strategies. This provides awareness of vulnerabilities, threat information, and impact to its mission. However, the IRS has not fully deployed its solution for real-time and continuous monitoring of security controls. • The IRS uses lessons learned to improve existing policies and procedures.
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**
Consistently Implemented (Level 3) – The organization consistently analyzes the data it collects on potentially adverse events to better understand associated activities. The agency consistently implements monitoring and enforcement mechanisms to identify and manually disconnect or isolate non-compliant devices and virtual assets. The agency employs network monitoring capabilities based on known indicators of compromise to develop situational awareness and correlates telemetry from multiple sources for analysis and monitoring.	• The IRS consistently analyzes the data it collects on potentially adverse events to better understand associated activities. • The IRS currently does not have [redacted] capabilities installed on two of the seven sampled systems. • [redacted]

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 developed and implemented policies for system level continuous monitoring. • We reviewed the seven sampled systems and determined that each contained an updated security plan and security controls assessment that demonstrates that the systems undergo continuous monitoring of their security posture. • The IRS provided evidence that some control automations were in place; however, control automation across the enterprise is still being implemented and will continue to mature.

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 2025 FISMA cycle: • We conducted a review of selected security controls for the seven sampled systems identified and determined that these controls were implemented. • The IRS developed the capability to aggregate security information from multiple sources to support analysis and monitoring requirements. 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.

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 2025 RESPOND Function Area Assessment Results

METRIC	DOMAIN	METRIC TYPE	RATING
30	INCIDENT RESPONSE	CORE	3
31	INCIDENT RESPONSE	CORE	5
CORE AVERAGE			4
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-21-31.	• The organization consistently implements enterprise-wide policies, procedures, and processes for incident detection and analysis. • The IRS reported that 53 (14 percent) of 389 IRS systems containing Personally Identifiable Information or Federal Tax Information do not have audit logs that meet OMB requirements.

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 2025 FISMA cycle:

- The IRS Computer Security Incident Response Center has a reconfiguration request process in place to create temporary or permanent rules for security access measures. In addition to its traditional reconfiguration method, the Advanced Threat Analysis Cell team compliments with a more robust method of gathering intelligence and constantly tracking potential threats in real-time to proactively make security updates as needed.

Despite this, we identified an area that needs improvement:

- The IRS Computer Security Incident Response Center leverages an enterprise security tool to capture data logs across the IRS enterprise level and demonstrate compliance with OMB logging requirements at a platform level. However, the IRS has not fully implemented the same capability to demonstrate compliance with OMB logging requirements at the system level. According to the IRS, completing the work to validate audit log compliance is a labor intensive and time-consuming effort and it currently lacks the resources to perform the necessary work for all systems.

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 2025 RECOVER Function Area Assessment Results

METRIC	DOMAIN	METRIC TYPE	RATING
33	CONTINGENCY PLANNING	CORE	4
34	CONTINGENCY PLANNING	CORE	4
CORE AVERAGE			4
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 2025 FISMA cycle, the IRS: • Started to automate the contingency planning program in a cloud-based tool. The tool will allow for more comprehensive reporting features and streamlined data collection processes that allow for more accurate and real-time reporting. The IRS stated that it is planning to complete development of the ServiceNow Business Continuity Module by July 2025. Despite this, we identified an area that needs improvement, as follows: • The IRS plans to further integrate its asset management processes to improve risk identification as processes and data continue to mature.	

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the effectiveness of the IRS's information security program and practices. 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 IRS 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 January 2025, the inventory contained 189 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 Assessment, Authorization, and Risk Governance system reports with 1,623 active POA&Ms as of April 2025. 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 during the FISMA evaluation period of March 2024 through June 2025. 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 organization's Cybersecurity function located in the New Carrollton Federal Building in Lanham, Maryland during the period January through June 2025. 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) ensuring that the information was legible and contained

alphanumeric characters; 2) reviewing required data elements; and 3) reviewing the data to detect obvious errors, duplicate values, and missing data. We determined the data were sufficiently reliable for the purpose of the 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: Executive Order 14028; OMB Memoranda; NIST Special Publication 800 series; and Internal Revenue Manual policies related to information technology security 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 2025 Evaluation and the Metrics to Which They Apply

1. TIGTA, Report No. 2024-200-057, *Security Vulnerability Management and Configuration Compliance of a General Support System and Major Application Need Improvement* (September 2024) – Metrics 13 and 15.
2. TIGTA, Report No. 2025-200-009, *Systems Hosting Sensitive Data Lack Consistent Inventory Standards* (March 2025) – Metrics 7 and 13.
3. GAO, GAO-19-176, *Strategic Human Capital Management is Needed to Address Serious Risks to IRS's Mission* (March 2019) – Metric 24.
4. GAO, GAO-20-411R, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls* (May 2020) – Metric 20.
5. GAO, GAO-24-106653SU, *Security of Taxpayer Information: IRS Needs to Improve Information System Controls* (July 2024) – Metrics 14, 20, 21, and 23.

Appendix III

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 www.tigta.gov/form/suggestions.

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