Federal Trade Commission

Office of Inspector General

Fiscal Year 2025 Audit of the FTC's Information Security Program and Practices

FINAL REPORT—REDACTED—FOR PUBLIC RELEASE

Sensitive information on the FTC's information technology security systems, policies, and practices determined to be restricted from public release has been redacted from this document.

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of Inspector General

December 19, 2025

MEMORANDUM

FROM: Marissa Gould Marissa Gould
Acting Inspector General

TO: Andrew Ferguson, Chairman

SUBJECT: Fiscal Year 2025 Audit of the FTC's Information Security Program and Practices

As required by the Federal Information Security Modernization Act of 2014 (P.L. 113-283) (FISMA), attached is the report on the annual independent evaluation of the Federal Trade Commission's (FTC) Information Security Program and Practices for Fiscal Year (FY) 2025.

The Office of Inspector General (OIG) contracted with RMA Associates, LLC (RMA) to conduct an independent audit to meet the FY 2025 FISMA requirements. The objective of the audit was to evaluate the effectiveness of FTC's information security program and practices and determine the maturity level FTC achieved for each of the core metrics and supplemental metrics outlined in the *FY 2025 Inspector General (IG) FISMA Reporting Metrics v2.0*. The contract required that the audit be performed in accordance with U.S. generally accepted government auditing standards, applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines.

RMA concluded that the FTC's information security program and practices were **effective**.

RMA is responsible for the attached auditor's report dated December 18, 2025, and the conclusions expressed therein. We do not express an opinion on the FTC's compliance with FISMA or conclusions on other matters.

RMA made **no new recommendations** in the FY 2025 report.

The FTC's response to the draft report is included as Appendix II.

A public version of this report will be posted on the OIG's website pursuant to section 420(b) of the Inspector General Act of 1978, as amended. The OIG redacted portions of the public version of this report at the agency's request.

RMA | Associates
Auditors. Consultants. Advisors.

Federal Trade Commission

Federal Information Security Modernization Act of 2014

Audit Report for Fiscal Year 2025

RMA Associates, LLC
4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
Fax: (703) 852-7272
www.rmafed.com

RMA | Associates
Auditors. Consultants. Advisors.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

December 18, 2025

Marissa Gould, Acting Inspector General
Federal Trade Commission
Room CC-5206
600 Pennsylvania Ave., NW
Washington, DC 20580

Re: Federal Trade Commission Federal Information Security Modernization Act of 2014 Audit Report for Fiscal Year 2025

Dear Ms. Gould:

RMA Associates, LLC is pleased to submit our performance audit report on the effectiveness of the Federal Trade Commission's (FTC) information security program and practices for Fiscal Year (FY) 2025. In accordance with the *Federal Information Security Modernization Act of 2014* (FISMA), the objective of this performance audit was to evaluate the effectiveness of FTC's information security program and practices and determine the maturity level FTC achieved for each of the core metrics and supplemental metrics outlined in the *FY 2025 Inspector General (IG) FISMA Reporting Metrics v2.0*. We conducted our performance audit for FY 2025 as of August 1, 2025. The performance audit fieldwork was conducted in Washington, DC, from March 10, 2025, to August 1, 2025.

Based on the results of our performance audit, we determined that the FTC's information security program and practices were effective for FY 2025, as the criteria assessed for the FTC's information security program met the maturity level of Managed and Measurable. Our assessment of the information security program identified no new findings associated with the 10 FISMA Metric Domains. There was one area for improvement in the [redacted] domain, and one finding [redacted] from a prior FISMA performance audit had not been resolved. As such, we are not making a new recommendation in the FY 2025 FISMA audit.

Our report includes **Appendices I**: Status of Prior Year Recommendations, **II**: Management Response, **III**: Evaluation of Management Response, and **IV**: FY 2025 IG FISMA Reporting Metrics. Further details of our findings and recommendations are included in the accompanying report.

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.

The performance audit included assessing the FTC's information security program and practices consistent with FISMA and reporting instructions issued by the Office of Management and Budget (OMB). We considered the guidelines established by the OMB, Department of Homeland Security (DHS), and National Institute of Standards and Technology (NIST). We assessed three judgmentally selected systems out of a total of six FISMA reportable systems from the FTC's FISMA inventory of information systems.

For FY 2025, OMB required Inspector Generals to assess 25 metrics from FY *2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025, including both core and supplemental metrics. These metrics are coordinated and agreed upon by the Council of the Inspectors General on Integrity and Efficiency, the Chief Information Security Officer, OMB, and the Cybersecurity & Infrastructure Security Agency. This approach is aligned with NIST *Cybersecurity Framework 2.0*, which underscores the essential role of governance in managing cybersecurity risks and integrating cybersecurity into an organization's overall enterprise risk management strategy. The FY 2025 IG Metrics were aligned with the following Cybersecurity Framework function areas: Govern, Identify, Protect, Detect, Respond, and Recover to determine the effectiveness of agencies' information security program. The *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025, classifies information security programs and practices into five maturity levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

We have also prepared responses to the OMB's M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* guidance, encouraging agencies to shift towards a continuous assessment process for their annual independent assessment using *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025 and the submission of evaluations via CyberScope. These metrics provide reporting requirements across function areas to be addressed in the independent assessment of agencies' information security programs.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. We caution that projecting the results of our performance audit to future periods is subject to the risk that conditions may change significantly from their current status. The information included in this report was obtained from the FTC on or before August 1, 2025. We are not obligated to update our report or revise the information contained therein to reflect events occurring after August 1, 2025.

We greatly appreciate the opportunity to serve your organization and the assistance provided by your staff and the FTC. We will be happy to answer any questions you may have concerning the report.

Sincerely,

Reza Mahbod

RMA Associates, LLC
Arlington, VA

Table of Contents

Introduction

This report presents the results of RMA Associates, LLC (RMA) 's independent performance audit of the Federal Trade Commission's (FTC) information security program and practices. The *Federal Information Security Modernization Act of 2014* (FISMA)[1] requires Federal agencies to conduct an annual independent evaluation to assess their information security program and practices to determine the effectiveness of such programs and practices and to report the results of the audits to the Office of Management and Budget (OMB). OMB delegated its responsibility to the Department of Homeland Security (DHS) for the collection of annual FISMA responses. DHS prepared the FISMA questionnaire to collect the responses, which is provided in **Appendix IV – FY 2025 IG FISMA Reporting Metrics**. We also considered applicable OMB and the National Institute of Standards and Technology (NIST) policies, standards, and guidelines to perform the audit.

The FTC's Office of Inspector General engaged RMA to conduct an annual performance audit of FTC's information security program and practices in support of the FISMA performance audit requirement. The objective of this performance audit was to evaluate the effectiveness of FTC's information security program and practices and determine what maturity level FTC achieved for each of the core metrics and Fiscal Year (FY) 2025 supplemental metrics outlined in the *FY 2025 Inspectors General (IG) FISMA Reporting Metrics v2.0* (April 2025).

As part of our performance audit, we responded to the FY 2025 20 core and five supplemental metrics specified in OMB's *FY 2025 IG FISMA Reporting Metrics v2.0* (April 2025).[2] These metrics provide reporting requirements across the functional areas to be addressed in the independent assessment of agencies' information security programs.[3] We also considered applicable FTC and OMB policy and guidelines, and the NIST standards.

Summary Performance Audit Results

We determined that, consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, the FTC's information security program and practices were established and maintained for the six NIST Cybersecurity Framework function areas[4] and 10 FISMA metric domains.[5] The overall maturity level of the FTC's information security program was determined as Managed and Measurable, as described in this report. Our tests of the

[1] Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014 (Dec. 18, 2014).

[2] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the Inspector General FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council.

[3] Refer to the section titled, *Objective, Scope, and Methodology,* for more details.

[4] OMB, DHS, and CIGIE developed the FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. The 10 FISMA Metric Domains were aligned with the six functions: (1) govern, (2) identify, (3) protect, (4) detect, (5) respond, and (6) recover as defined in the NIST *Cybersecurity 2.0*.

[5] As described in the FISMA Reporting Metrics, the 10 FISMA Metric Domains are: (1) Cybersecurity Governance, (2) Cybersecurity Supply Chain Risk Management, (3) Risk and Asset Management, (4) Configuration Management, (5) Identity and Access Management, (6) Data Protection and Privacy, (7) Security Training, (8) Information Security Continuous Monitoring, (9) Incident Response, and (10) Contingency Planning.

information security program identified no new findings associated with the 10 FISMA Metric Domains. There was one area for improvement in the cybersecurity supply chain risk management domain, and one finding that fell within the incident response domain from a prior FISMA performance audit had not been resolved. As such, we are not making a new recommendation in the FY 2025 FISMA audit.

We assessed that the FTC's information security program and practices were effective from October 1, 2024, to August 1, 2025.

We provided FTC with a draft of this report for their review and comment. In a written response, management agreed with the results of our performance audit (refer to **Appendix II – Management's Response** for the FTC's response in its entirety, and **Appendix III – Evaluation of Management's Response** for our assessment of management's response).

Background

Federal Trade Commission

The FTC is a bipartisan Federal agency with a unique dual mission to protect consumers and promote competition. Moreover, the agency is dedicated to advancing consumer interests while encouraging innovation and competition in a dynamic, global economy.

The FTC develops policy and research tools through hearings, workshops, and conferences. Additionally, the FTC collaborates with law enforcement partners across the country and around the world to advance consumer protection and competition missions. Furthermore, the FTC cooperates with international agencies and organizations to protect consumers in the global marketplace.

As it relates to information technology (IT), the FTC relies extensively on information systems and the sharing of information to accomplish its mission. Information systems with effective security controls reduce risk and strengthen management's oversight of information, property, and finances to protect information systems and their shared data. Improving the overall management and security of IT resources and stakeholder information must be a top priority for the FTC. While technology enables and enhances the ability to share information instantaneously among stakeholders through computers and networks, increased connectivity also makes an organization's networks and IT resources vulnerable to malicious activity and exploitation by internal and external sources. Insiders with malicious intent, recreational and institutional hackers, and attacks by foreign intelligence organizations are significant threats to the FTC's critical systems. Therefore, the operational effectiveness of security controls must be periodically assessed to ensure those controls operate as intended to safeguard the confidentiality, integrity, and availability of information.

Key Changes to the FY 2025 IG FISMA Metrics

One of the goals of the annual FISMA audits is to assess agencies' progress toward achieving objectives that strengthen Federal cybersecurity. The IG FISMA Reporting Metrics have been updated to determine agency progress in achieving the objectives, as follows:

- NIST *Cybersecurity Framework 2.0*: NIST published Cybersecurity Framework (CSF) Version 2.0, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's broader enterprise risk management strategy. A new IG FISMA function area (Govern) was created that includes a new domain (Cybersecurity Governance). In addition, new supplemental metrics were designed to assess the maturity of an organization's:
  - Use of cybersecurity profiles to understand, tailor, assess, prioritize, and communicate cybersecurity objectives.
  - Cybersecurity risk management strategy, which establishes an organization's priorities, constraints, risk tolerance and appetite statements and is used to support operational risk decisions.
  - Processes and authorities to foster cybersecurity accountability, performance assessment, and continuous improvement.

  In addition, to align with the CSF 2.0, the supply chain risk management (SCRM) domain was moved from the Identify function area to the Govern function area and renamed to Cybersecurity SCRM (C-SCRM) to better reflect the cybersecurity environment. Furthermore, a new domain in the Identify function area (Risk and Asset Management) was established to group metrics on system inventory and hardware, software, and data management.

- Zero Trust Architecture (ZTA) Implementation: The FY 2025 metrics include two new supplemental metrics critical to achieving ZTA objectives. These new metrics assess the maturity of an organization's (1) data management capabilities, and (2) ability to monitor and measure the integrity and security posture of all owned and associated assets.

- Supplemental metrics for FY 2025: Five supplemental metrics, including metric numbers 1, 2, 3, 10, and 27, were in scope for the FY 2025 IG FISMA audit.

- Information System Level Risk Management: The core metric on information system level risk management (Metric 11, formerly Metric 5) was revised to focus on the maturity of agencies' implementation of the NIST risk management framework.

For FY 2025, the IG audit had a deadline of August 1, 2025, for FISMA reporting to OMB and the DHS. This allowed agencies more time to incorporate the necessary changes identified by the IG audits in their budget submissions.

Federal Information Security Modernization Act of 2014

Title III of the *E-Government Act*, entitled the *Federal Information Security Management Act of 2002*, required each Federal agency to develop, document, and implement an agency-wide program to provide security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources. FISMA amended the *Federal Information Security Management Act of 2002* and provided several modifications that modernize Federal security practices to address evolving security concerns. These changes resulted in less overall reporting, strengthened the use of continuous monitoring in systems, and increased focus on the agencies for compliance and reporting that is more concentrated on the issues caused by security incidents.

FISMA, along with the *Paperwork Reduction Act of 1995* and the *Information Technology Management Reform Act of 1996* (also known as the Clinger-Cohen Act), explicitly emphasizes a risk-based approach to cost-effective security. In support of and reinforcing this legislation, OMB, through Circular No. A-130, *Managing Information as a Strategic Resource*, requires executive agencies within the Federal government to:

- Plan for security;
- Ensure that appropriate officials are assigned security responsibilities;
- Periodically review the security controls in its systems; and
- Authorize system processing prior to operations and periodically after that.

These management responsibilities presume that responsible agency officials understand the risks and other factors that could adversely affect the organization's missions. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information and systems, and make informed judgments and investments that appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct the Commission's day-to-day operations and accomplish its stated mission with adequate security or security commensurate with risk, including the magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information.

FISMA provided OMB with oversight authority over agency security policies and practices and authorized the implementation of agency policies and practices for information systems to DHS.[6]

FISMA required the Secretary of DHS to develop and oversee the implementation of operational directives that require agencies to implement OMB standards and guidelines for safeguarding Federal information and systems from known or reasonably suspected information security threats, vulnerabilities, or risks. FISMA directed the Secretary to consult with and consider guidance developed by NIST to ensure operational directives do not conflict with NIST information security

[6] FISMA, Pub. L. No. 113-283, 128 Stat. 3073, December 2014, https://www.congress.gov/bill/113th-congress/senate-bill/2521.

standards.[7] FISMA authorized the Director of OMB to revise or repeal operational directives not in accordance with the Director's policies.[8]

Additionally, FISMA directed Federal agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General of the U.S. Government Accountability Office. The reports are required to include: (1) threats and threat actors, vulnerabilities, and impacts of the incidents; (2) risk assessments of affected systems before the incidents; (3) the status of system compliance at the time of the incidents; (4) detection, response, and remediation actions; (5) total number of incidents; and (6) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information.[9]

Core and FY 2025 Supplemental IG Metrics

OMB's *FY 2025 IG FISMA Reporting Metrics v2.0* (April 2025) specified 20 Core and five Supplemental IG Metrics. It directed IGs to report the assessed maturity levels of these metrics in CyberScope[10] no later than August 1, 2025. The FY 2025 FISMA IG Metrics were aligned with the six function areas in the NIST *Cybersecurity Framework 2.0* as follows:

- Govern, includes metrics pertaining to Cybersecurity Governance and Cybersecurity Supply Chain Risk Management;
- Identify, includes metrics pertaining to Risk and Asset Management;
- Protect, includes metrics pertaining to Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training;
- Detect, includes metrics pertaining to Information Security Continuous Monitoring;
- Respond, includes metrics pertaining to Incident Response; and
- Recover, includes metrics pertaining to Contingency Planning.

We assessed the effectiveness of information security programs and practices on a maturity model spectrum, in which the foundation levels ensure the development of sound policies and procedures. The FY 2025 IG Metrics classifies information security programs and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. Within the context of the maturity model, Level 4 (Managed and Measurable) and Level 5 (Optimized) represent an effective level of security. **Table 1: IG Audit Maturity Levels** explains the five maturity model levels.

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] CyberScope is a web-based platform to streamline the reporting of information security practices required under FISMA. As mandated by OMB and DHS, federal agencies must collect FISMA performance metrics data and upload the results into CyberScope.

Table 1: IG Audit Maturity Levels

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

For FY 2025, IGs continued to focus on a calculated weighted average approach, wherein the average of the metrics in a particular domain was used by IGs to determine the effectiveness of individual function areas (govern, identify, protect, detect, respond, and recover) and the overall program. To provide IGs with additional flexibility and encourage evaluations based on agencies' risk tolerance and threat models, calculated averages were not automatically rounded (i.e., rounded up or down based on mathematical rules) to a particular maturity level. In the FY 2025 calculated average scoring model, core metrics and supplemental metrics were calculated independently to determine a domain's maturity calculation and provide data points for assessing program and function area effectiveness. For example, if the calculated core metric maturity of two of the function areas is Level 3 (Consistently Implemented) and the calculated core metric maturity of the remaining three function areas is Level 4 (Managed and Measurable), then the information security program rating would average a 3.60.[11]

We focused on the results of the core metrics to determine maturity levels. We used the calculated averages of the supplemental metrics as a data point to support our risk-based determination of overall program and function level effectiveness. The DHS computed average of the maturity level was 4.09, the Managed and Measurable level. As a result, FTC's overall assessed maturity level was effective.

FTC's FY 2025 calculated core metric, supplemental metric, assessed maturity averages, and assessed maturity level by function are presented in **Table 2: Overall Calculated Averages Maturity Calculation in FY 2025.**

[11] *FY 2025 IG FISMA Reporting Metrics v2.0*, April 3, 2025.

Table 2: Overall Calculated Averages Maturity Calculation in FY 2025

Function	Core Metrics	Supplemental Metrics[12]	Assessed Maturity Average[13]	Assessed Maturity
Govern[14]	3.00	4.33	4.14	Managed and Measurable
Identify	4.00	4.00	4.00	Managed and Measurable
Protect	4.38	N/A	4.38	Managed and Measurable
Detect	4.00	4.00	4.00	Managed and Measurable
Respond	4.00	N/A	4.00	Managed and Measurable
Recover	4.00	N/A	4.00	Managed and Measurable
Overall Maturity	**3.9**	**4.11**	**4.09**	**Managed and Measurable**

Audit Results

We assessed the FTC's overall maturity level for its security program as Managed and Measurable. However, there was one area for improvement in the [redacted] domain, and one finding that fell within the [redacted] from a prior FISMA performance audit had not been resolved. [redacted] We assessed that FTC implemented an effective information security program, considering the agency's unique mission, resources, and challenges.

The maturity level for the 10 domains is presented below in **Table 3: FTC's FY 2025 Maturity Levels.**

Table 3: FTC's FY 2025 Maturity Levels

Function	Maturity Level	
Function 1: Govern		Managed and Measurable (Level 4)
• Cybersecurity Governance	Managed and Measurable (Level 4)	
• [redacted]	[redacted]	
Function 2: Identify – Risk and Asset Management		Managed and Measurable (Level 4)
Function 3: Protect		Managed and Measurable (Level 4)
• Configuration Management	Managed and Measurable (Level 4)	
• Identity and Access Management	Managed and Measurable (Level 4)	
• Data Protection and Privacy	Managed and Measurable (Level 4)	
• Security Training	Optimized (Level 5)	

[12] Protect, Respond, and Recover function areas only consist of core metrics.
[13] For FY 2025, the assessed maturity average was computed by averaging the core and supplemental metrics.
[14] The Govern function area was introduced in FY 2025.

Function	Maturity Level
Function 4: Detect—Information Security Continuous Monitoring	Managed and Measurable (Level 4)
Function 5: Respond—Incident Response	Managed and Measurable (Level 4)
Function 6: Recover—Contingency Planning	Managed and Measurable (Level 4)
Overall	**Managed and Measurable (Level 4)**
Overall	**Effective**

The following paragraphs provide more details on each domain's assessed maturity level and offer recommendations to the Chief Information Officer to remediate deficiencies.

Cybersecurity Governance

We assessed the FTC's overall maturity level for the cybersecurity governance program as Managed and Measurable.

The FTC identified its current and target cybersecurity profiles in alignment with the CSF 2.0 and assessed the gaps between its profiles. It then created and implemented a prioritized action plan through the Plan of Action and Milestones (POA&M) process, as well as corrective action plans initiated from Enterprise Risk Management. FTC consistently implemented its risk management strategy, evaluating and adjusting it based on its threat environment and agency-wide cyber and privacy risk assessments. Roles, responsibilities, and authorities related to cybersecurity risk management were established and communicated. Stakeholders were held accountable for carrying out their roles and responsibilities effectively.

Our testing of the cybersecurity governance program found no exceptions and determined that the FTC's cybersecurity governance program controls in place were effective.

Cybersecurity Supply Chain Risk Management

We assessed the FTC's overall maturity level for the C-SCRM program as Consistently Implemented.

The FTC defined and communicated policies and procedures to ensure that products, system components, systems, and services adhere to its cybersecurity and C-SCRM requirements. The FTC identified and prioritized externally provided systems, system components, and services, maintaining awareness of its upstream suppliers. Additionally, the FTC integrated its acquisition processes, including contractual agreements that stipulate appropriate cybersecurity measures for external providers.

[redacted]

[redacted]

[redacted]

Risk and Asset Management

We assessed the FTC's overall maturity level for the risk and asset management program as Managed and Measurable.

The FTC defined priority levels for its IT systems and implemented continuous monitoring processes that considered risks associated with supporting business functions and the impact on its mission, helping its leadership make informed risk management decisions. The FTC used performance measures as a management tool in its internal improvement efforts and linked the implementation of its information security program to agency-level strategic planning efforts. In addition, the FTC implemented its security architecture across the enterprise, business process, and system levels to help leadership make informed risk management decisions. Those risk management decisions helped improve and update FTC's risk management policies, procedures, and strategy, including methodologies for categorizing risk, developing a risk profile, assessing risk, determining risk appetite or tolerance levels, responding to risk, and monitoring risk. Additionally, FTC consistently captured and shared lessons learned on the effectiveness of risk management processes and activities to update the program. Information system inventory, hardware, and software asset inventory were maintained comprehensively and accurately. The agency evaluated risks associated with its assets and determined it had no high-value assets.[15]Lastly, FTC consistently maintained a comprehensive and accurate inventory of its data and corresponding metadata for each data type, ensuring that the data and metadata in its inventories were subject to the monitoring processes defined within the FTC's Information Security Continuous Monitoring (ISCM) strategy.

Our testing of the risk and asset management program found no exceptions and determined that the FTC's risk and asset management program controls in place were effective.

Configuration Management

We assessed that the FTC's overall maturity level for the configuration management program as Managed and Measurable.

The FTC consistently implemented an organization-wide configuration management plan integrated into risk management and continuous monitoring processes. The FTC utilized various automated mechanisms to detect unauthorized hardware, software, and firmware on its network

[15] A high-value asset is information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to this system would have serious impact on the organization's ability to perform its mission or conduct business.

and take immediate actions to limit any security impact. The FTC utilized the Security Content Automation Protocol, which allowed scanners to identify network vulnerabilities and maintain an up-to-date, comprehensive, accurate, and readily available view of the security configuration for all system components connected to its network. The FTC applied standard baselines to control hardware and software configurations, centrally managed its flaw remediation process, and applied software patches.

Our testing of the configuration management program found no exceptions and determined that the FTC's configuration management program controls in place were effective.

Identity and Access Management (IDAM)

We assessed the FTC's overall maturity level for the IDAM program as Managed and Measurable.

The FTC established an identification and authentication policy that defines processes of managing, monitoring, and securing access to protected resources. Additionally, the FTC's access control policy assigned responsibilities and defined requirements for developing and managing system access controls. FTC implemented a third-party identity management cloud service for its enterprise-wide single sign-on solution. All of the FTC's systems interfaced with the solution to oversee employees, enabling the central management of non-privileged and privileged users' accounts, as well as the reporting of effectiveness in near real-time. The FTC used automation to manage and review user access agreements for privileged and non-privileged users. Additionally, the FTC conducted monthly reviews of privileged user access. [redacted] in accordance with OMB Memorandum M-21-31, "*Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*."

Our testing of the IDAM program found no exceptions and determined that the FTC's IDAM controls in place were effective.

Data Protection and Privacy

We assessed the FTC's overall maturity level for the data protection and privacy program as Managed and Measurable.

The FTC dedicated significant resources to its privacy program. It maintained an inventory of Personally Identifiable Information (PII) collection and use, conducting privacy impact assessments and system of records notices for all applicable systems. FTC ensured that security controls for safeguarding PII and other sensitive agency data were diligently monitored throughout the data lifecycle. FTC defined and communicated policy related to encryption of data at rest, encryption of data in transit, limitation of transfer to a removable drive, and sanitization of the removable drive before reuse or disposal for the protection of PII and other sensitive information. Additionally, the FTC monitored and analyzed quantitative and qualitative performance measures to assess the effectiveness of its privacy activities. The FTC conducted an independent review of its privacy program and made necessary improvements. FTC also conducted exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses.

[redacted]

Our testing of the data protection and privacy program found no exceptions and determined that the FTC's data protection and privacy program controls in place were effective.

Security Training

We assessed the FTC's overall maturity level for the security training program as Optimized.

The FTC developed, documented, and disseminated comprehensive policies and procedures for security awareness and specialized security training. The FTC defined the roles and responsibilities of individuals executing duties serving the security awareness and training program. The FTC performed roles and responsibilities related to security training, completed a workforce assessment, and conducted annual security training. Additionally, the FTC effectively allocated resources in a risk-based manner, allowing stakeholders to implement security awareness training consistently. The FTC also demonstrated the ability to monitor and analyze qualitative and quantitative performance measures of its security awareness and training strategies and plans, and addressed its identified knowledge, skills, and ability gaps through talent acquisition. Data supporting the metrics were obtained accurately and consistently in a reproducible format.

Our testing of the security training program found no exceptions and determined that the FTC's security training program controls in place were effective.

Information Security Continuous Monitoring

We assessed the FTC's overall maturity level for the ISCM program as Managed and Measurable.

The FTC's ISCM strategy established a general approach to maintain awareness of the FTC's cybersecurity posture to support risk management decisions and establish guidelines for granting ongoing authorizations. In addition to the ISCM strategy, the FTC updated ISCM policies that cover the areas related to the FTC's overall ISCM program. Additionally, the FTC consistently updated its authorization package and conducted annual system-level security assessments. The FTC analyzed qualitative and quantitative performance measures to assess the effectiveness of its ISCM policies and procedures through monthly, quarterly, and yearly continuous monitoring reports. The security control assessments and monitoring results were used to maintain ongoing authorizations of information systems. Furthermore, the FTC documented and implemented lessons learned to enhance the continuous monitoring process, instructing employees to record, analyze, and revise control activities on a cyclical basis to continuously improve the FTC's security posture, as defined in the Security Continuous Monitoring Plan. FTC utilized security tools and dashboards to enhance detection accuracy and characterize threat actors, their methods, and indicators of compromise. Manual reviews were conducted for technologies that cannot be sufficiently monitored through automation. We also noted that FTC automated its inventory collection and anomaly detection to detect unauthorized devices.

Our testing of the ISCM program found no exceptions and determined that the FTC's ISCM program controls in place were effective.

Incident Response

We assessed the FTC's overall Incident Response program maturity level as Managed and Measurable.

The FTC published Incident Response policy and procedures that establish the FTC's level of its Incident Response program, outlining containment strategies, consideration for potential damage to and theft of resources, evidence preservation, service availability, and the time, resources, and duration of the solution. Also, the FTC centralized its incident response function by establishing the Computer Security Incident Response Team (CSIRT), which comprises incident handlers within the Continuous Assurance Branch and other agency security officials. We assessed that the FTC personnel reported potential incidents to the CSIRT, which handled the reported incidents in accordance with the plan. [redacted]

[redacted]

[redacted]

Although the FTC did not address a prior year's finding regarding EL requirements, the incident response controls were operating as intended. We assessed that the FTC's incident response program controls in place were effective.

Contingency Planning

We assessed the FTC's overall maturity level for the contingency planning program as Managed and Measurable.

[redacted]

Our testing of the contingency planning program found no exceptions and determined that the FTC's contingency planning program controls in place were effective.

Overall Conclusion

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, we assessed that the FTC's information security program and practices were established and maintained for the six Cybersecurity Framework function areas and 10 FISMA Metric Domains. Additionally, we evaluated that the FTC's information security program, and practices were effective from October 1, 2024, to August 1, 2025, and the overall maturity level of the FTC's information security program was Managed and Measurable. Our assessment of the information security program identified no new findings associated with the 10 FISMA Metric Domains. There was one area for improvement in the [redacted]

[redacted]

Objective, Scope, and Methodology

Objective

The objective of this performance audit was to evaluate the effectiveness of the FTC's information security program and practices, and to determine the maturity level achieved by the FTC for each of the core metrics and supplemental metrics outlined in FY *2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025. Specifically, the performance audit determined whether the FTC implemented an effective information security program by evaluating the six Cybersecurity Framework function areas as divided into 10 FISMA Metric Domains:

- **Govern**, includes metrics pertaining to cybersecurity governance and cybersecurity supply chain risk management;
- **Identify**, includes metrics pertaining to risk and asset management;
- **Protect**, includes metrics pertaining to configuration management, identity and access management, data protection and privacy, and security training;
- **Detect**, includes metrics pertaining to information security continuous monitoring;
- **Respond**, includes metrics pertaining to incident response; and
- **Recover**, includes metrics pertaining to contingency planning.

The answers to the core metrics and the FY 2025 supplemental metrics in **Appendix IV – FY 2025 IG FISMA Reporting Metrics** reflect the results of our testing of the FTC's information security program and practices.

Scope

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.

The scope of the FISMA performance audit work was agency-wide for the FTC, and the review covered FY 2025 as of August 1, 2025. We assessed three judgmentally selected systems out of a total of six FISMA reportable systems from the FTC's inventory of information systems. The performance audit fieldwork was conducted at the FTC's headquarters in Washington, DC, between March 10, 2025, and August 1, 2025. This performance audit included steps to follow up on prior-year FISMA-related recommendations. **Appendix I – Status of Prior Year's Recommendations** summarizes the status of recommendations from the prior years.

Methodology

The overall strategy of our performance audit considered the following: (1) NIST SP 800-53, Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*;

(2) NIST SP 800-53A, Revision 5.1.1, *Assessing Security and Privacy Controls in Information Systems and Organizations*; (3) *FY 2025 IG FISMA Reporting Metrics v2.0*; and (4) the FTC's policies and procedures.

We conducted interviews with the FTC officials and reviewed the legal and regulatory requirements stipulated in FISMA. We also examined documents supporting the information security program and practices. Where appropriate, we compared documents, such as the FTC's information technology policies and procedures, to requirements stipulated in NIST Special Publications. Additionally, we conducted tests of system processes to assess the design and operating effectiveness of these controls.

We applied the following criteria for performing the FTC's FY 2025 FISMA audit.

NIST Federal Information Processing Standards (FIPS) and SPs

- *NIST Cybersecurity Framework (CSF 2.0)*
- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS Publication 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-40, Revision 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*
- NIST SP 800-53, Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-53A, Revision 5.1.1, *Assessing Security and Privacy Controls in Information Systems and Organizations*
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*
- NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61, Revision 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*
- NIST SP 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-83, Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*

- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-161, Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
- NIST SP 800-181, Revision 1, *Workforce Framework for Cybersecurity* (*NICE Framework)*
- NIST SP 800-207, *Zero Trust Architecture*
- NIST SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1, Recommendations for Mitigating the Risk of Software Vulnerabilities*
- NIST Interagency Report 8011, *Automation Support for Security Control Assessments: Volume 1: Overview*
- NIST Interagency Report 8011, *Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management*
- NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*

OMB Policy Directives

- *FY 2025 IG FISMA Reporting Metrics v2.0*
- OMB Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*
- OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*
- OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*
- OMB Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures*
- OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*
- OMB Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*
- OMB Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*
- OMB Memorandum M-17-09, *Management of Federal High Value Assets*

- OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CISP) for the Federal Civilian Government*
- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*

Government Accountability Office

- Standards for Internal Control in the Federal Government, September 2014

Cybersecurity and Infrastructure Security Agency

- Binding Operational Directive (BOD) 25-01, *Implementing Secure Practices for Cloud Services*
- BOD 23-02, *Mitigating the Risk from Internet-Exposed Management Interfaces*
- BOD 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*
- BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy*
- BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*
- BOD 18-02, *Securing High Value Assets*
- BOD 18-01, *Enhance Email and Web Security*
- BOD 17-01, *Removal of Kaspersky-Branded Products*
- BOD 16-03, *2016 Agency Cybersecurity Reporting Requirements*
- BOD 16-02, *Threat to Network Infrastructure Devices*
- Emergency Directive (ED) 24-02*, Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System*
- ED 24-01 *Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*
- ED 22-03 *Mitigate VMware Vulnerabilities*
- ED 21-04, *Mitigate Windows Print Spooler Service Vulnerability*
- ED 21-03, *Mitigate Pulse Connect Secure Product Vulnerabilities*
- ED 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*
- ED 21-01, *Mitigate SolarWinds Orion Code Compromise*
- ED 20-04, *Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday*
- ED 20-03, *Mitigate Windows DNS Server Remote Code Execution Vulnerability from July 2020 Patch Tuesday*
- ED 20-02, *Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday*
- ED 19-01, *Mitigate DNS Infrastructure Tampering*

Abbreviations

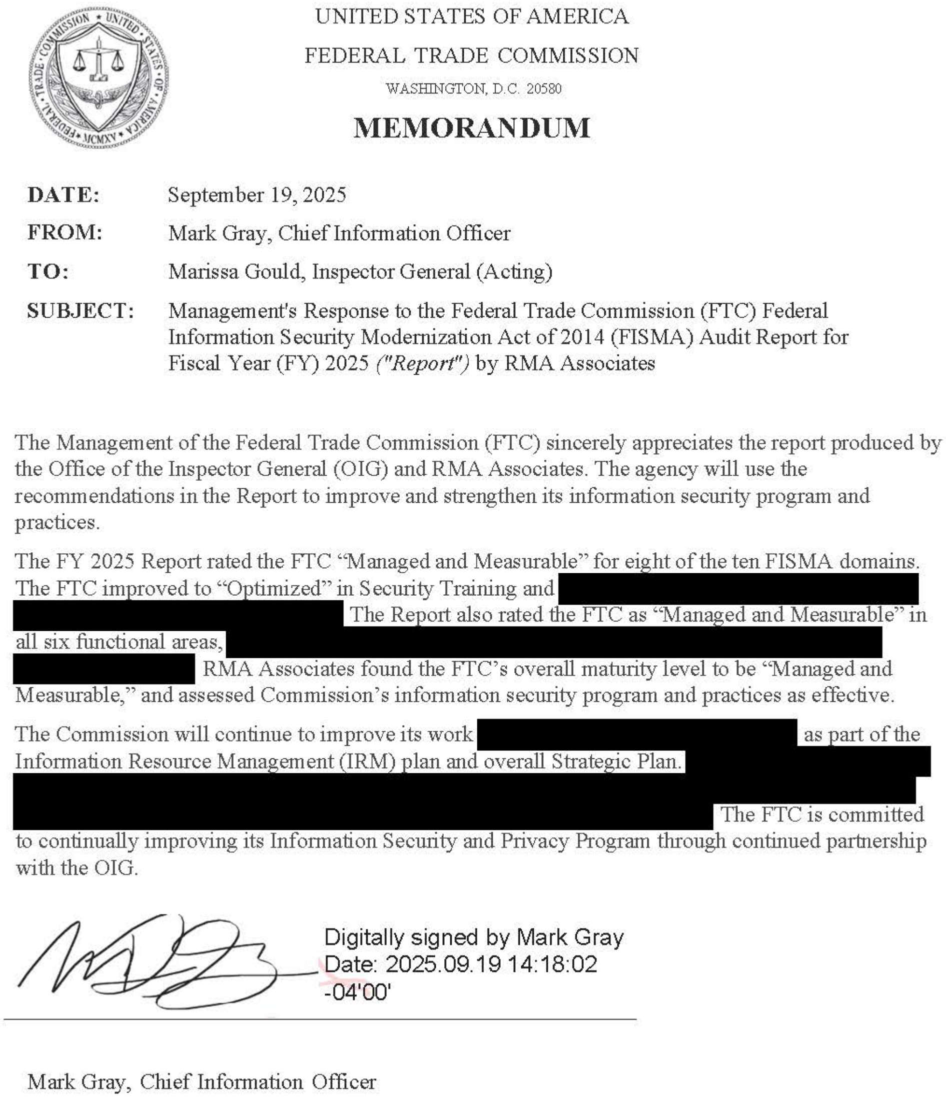
BIA	Business Impact Analysis
BOD	Binding Operational Directive
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CSF	Cybersecurity Framework
C-SCRM	Cybersecurity Supply Chain Risk Management
CSIRT	Computer Security Incident Response Team
DNS	Domain Name System
DHS	Department of Homeland Security
ED	Emergency Directive
EDR	Endpoint Detection and Response
EL	Event Logging
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FTC	Federal Trade Commission
FY	Fiscal Year
IDAM	Identity and Access Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plans of Action & Milestones
RMA	RMA Associates LLC
SCRM	Supply Chain Risk Management
SP	Special Publication
ZTA	Zero Trust Architecture

Appendix I – Status of Prior Year's Recommendations

[redacted]

[redacted]	[redacted]	[redacted]
	[redacted]	
1	[redacted]	[redacted]

Appendix II – Management's Response



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

MEMORANDUM

DATE: September 19, 2025

FROM: Mark Gray, Chief Information Officer

TO: Marissa Gould, Inspector General (Acting)

SUBJECT: Management's Response to the Federal Trade Commission (FTC) Federal Information Security Modernization Act of 2014 (FISMA) Audit Report for Fiscal Year (FY) 2025 *("Report")* by RMA Associates

The Management of the Federal Trade Commission (FTC) sincerely appreciates the report produced by the Office of the Inspector General (OIG) and RMA Associates. The agency will use the recommendations in the Report to improve and strengthen its information security program and practices.

The FY 2025 Report rated the FTC "Managed and Measurable" for eight of the ten FISMA domains. The FTC improved to "Optimized" in Security Training and [redacted] The Report also rated the FTC as "Managed and Measurable" in all six functional areas, [redacted] RMA Associates found the FTC's overall maturity level to be "Managed and Measurable," and assessed Commission's information security program and practices as effective.

The Commission will continue to improve its work [redacted] as part of the Information Resource Management (IRM) plan and overall Strategic Plan. [redacted] The FTC is committed to continually improving its Information Security and Privacy Program through continued partnership with the OIG.

Digitally signed by Mark Gray
Date: 2025.09.19 14:18:02
-04'00'

Mark Gray, Chief Information Officer

Appendix III – Evaluation of Management's Response

After reviewing the FTC's response, we consider them to be responsive to our recommendation and the action taken and planned should resolve the issues identified in the report. Therefore, the prior year recommendation will remain open until the FTC provides documentation to verify appropriate actions have been taken.

Appendix IV – FY 2025 IG FISMA Reporting Metrics

The subsequent section of the report "Appendix IV" is not being publicly released due to the sensitive security content.