

Federal Trade Commission

OFFICE OF INSPECTOR GENERAL

October 28, 2024



Fiscal Year 2024 Audit of the FTC's Information Security Program and Practices

FINAL REPORT REDACTED FOR PUBLIC RELEASE

Sensitive information on the FTC's information technology (IT) 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

October 28, 2024

MEMORANDUM

FROM: Andrew Katsaros
Inspector General

A handwritten signature in black ink, appearing to read "Andrew Katsaros".

TO: Lina M. Khan, Chair

SUBJECT: Fiscal Year 2024 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) 2024.

The Office of Inspector General (OIG) contracted with RMA Associates, LLC (RMA) to conduct an independent audit to meet the FY 2024 FISMA requirements. The objective of the audit was to evaluate the status of the FTC's overall information technology security program and practices. 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 October 14, 2024, 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 2024 report.

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

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.

FINAL REPORT—REDACTED—FOR PUBLIC RELEASE

Pursuant to FISMA and implementation guidance from OMB, the FTC will submit its annual FISMA reports to the Chairperson and Ranking Member of the following Congressional committees:

- House Committee on Oversight and Accountability;
- House Committee on Homeland Security;
- House Committee on Science, Space, and Technology;
- Senate Committee on Homeland Security and Governmental Affairs;
- Senate Committee on Commerce, Science, and Transportation; and
- The appropriate authorization and appropriations committees of the House and Senate.

Additionally, the FTC must provide a copy of its reports to the Comptroller General of the United States, OMB, and the Department of Homeland Security.

The OIG greatly appreciates the cooperation and courtesies extended to RMA and to us by the Office of the Chief Information Officer, Chief Privacy Officer, Financial Management Office, and Office of the Executive Director throughout the FISMA audit.

If you have any questions or concerns regarding this report, please contact me at (202) 326-3527.

Federal Trade Commission

Federal Information Security Modernization Act of 2014

Audit Report for Fiscal Year 2024



RMA Associates, LLC

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

October 14, 2024

Andrew Katsaros, Inspector General
Federal Trade Commission
Room CC-5206
600 Pennsylvania Ave., NW
Washington, DC 20580

Ref: Federal Trade Commission Federal Information Security Modernization Act of 2014 Audit Report for Fiscal Year 2024

Dear Mr. Katsaros:

RMA Associates, LLC is pleased to submit our Federal Trade Commission (FTC) Federal Information Security Modernization Act of 2014 (FISMA) performance audit report for Fiscal Year (FY) 2024. The objective of this performance audit was to evaluate the effectiveness of the FTC's information security program and practices for the period from October 1, 2023, to July 31, 2024. In accordance with the FISMA, the objective of this performance audit was to evaluate the effectiveness of the FTC's information security program and practices and determine what maturity level FTC achieved for each of the core metrics and FY 2024 supplemental metrics outlined in the *FY 2023 - 2024 Inspectors General (IG) FISMA Reporting Metrics*.

Based on the results of our performance audit, we assessed the FTC's information security program and practices as effective for FY 2024, as FTC's information security program met the criteria required to be evaluated at a maturity level of Managed and Measurable. Our tests of the information security program identified one area for improvement in the [REDACTED] domain and one finding that fell in the [REDACTED] domain. There was one recommendation from a prior FISMA performance audit that remains open to address this specific finding. As such, we are not making a new recommendation in the FY 2024 FISMA audit.

Our report includes **Appendix A – Management's Response** and **Appendix B – FY 2024 IG FISMA Reporting Metrics**.

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, which 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 performance audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our performance audit objectives.

We have also prepared the answers to the Office of Management and Budget's FY 2024 Inspector General Metrics (February 2023). These metrics provide reporting requirements across functional areas to be addressed in the independent assessment of agencies' information security programs.

In summary, we assessed the FTC's information security program and practices and determined that they were effective for the period October 1, 2023, to July 31, 2024.

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

Sincerely,



Reza Mahbod
President

Inspector General
Federal Trade Commission

RMA Associates LLC (RMA) conducted a performance audit of the effectiveness of the Federal Trade Commission's (FTC) information security program and practices for fiscal year (FY) 2024. We conducted our performance audit for the period of October 1, 2023, to July 31, 2024. The audit fieldwork covered FTC's headquarters located in Washington, DC, from April 9 to July 25, 2024.

In accordance with the *Federal Information Security Modernization Act of 2014* (FISMA)¹, the objective of this performance audit was to evaluate the effectiveness of the FTC's information security program and practices and determine what maturity level FTC achieved for each of the core metrics and FY 2024 supplemental metrics outlined in the *FY 2023 - 2024 Inspectors General (IG) FISMA Reporting Metrics*.

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards (GAGAS)*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our conclusions based on our performance audit objective. We believe that the evidence obtained provides a reasonable basis for determining the maturity level for the core and supplemental metrics and conclusions based on our performance audit objective.

The performance audit included assessing 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) guidance, and we assessed selected security controls outlined in NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*. We assessed three internal and external systems out of a total of six FISMA reportable systems from FTC's FISMA inventory of information systems.

For FY 2024, OMB required Inspector Generals to assess 37 of the 66 metrics from *FY 2021 IG FISMA Reporting Metrics v1.1* (May 12, 2021), including the core metrics and supplemental metrics for FY 2024, a combination of metrics that must be evaluated on a two-year calendar basis and agreed to by the Council of the Inspectors General on Integrity and Efficiency (CIGIE), the Chief Information Security Officer, OMB, and Cybersecurity & Infrastructure Security Agency (CISA). The FY 2024 IG Metrics were aligned with the five following Cybersecurity Framework security functions: Identify, Protect, Detect, Respond, and Recover, to determine the effectiveness of the agencies' information security program. The FY 2024 IG Metrics classifies information security programs and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

We assessed that FTC implemented an effective information security program by achieving an overall Managed and Measurable maturity level based on the *FY 2023 - 2024 IG FISMA Reporting*

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

Metrics. Our tests of the information security program identified one area for improvement in the [REDACTED] domain and one finding that fell in the [REDACTED] domain. There was one recommendation from a prior FISMA performance audit that remains open to address this specific finding. As such, we are not making a new recommendation in the FY 2024 FISMA audit.

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. RMA cautions that projecting the results of our performance audit to future periods is subject to the risk that conditions may materially change from their status. The information included in this report was obtained from FTC on or before July 31, 2024. We are not obligated to update our report or revise the information contained therein to reflect events occurring subsequent to July 31, 2024.

Additional information on our findings and recommendations are included in the accompanying report.

Sincerely,

RMA Associates

RMA Associates, LLC
Arlington, VA

Table of Contents

Introduction.....	1
Summary Performance Audit Results.....	1
Background.....	2
Key Changes to the IG FISMA Metrics	3
Objective.....	6
Audit Results.....	7
Scope and Methodology	17
Criteria	18
Appendix A – Management's Response	22
Appendix B – FY 2024 IG FISMA Reporting Metrics	23

Introduction

This report presents the results of RMA Associates, LLC (RMA) independent performance audit of the Federal Trade Commission's (FTC) information security program and practices. The *Federal Information Security Modernization Act of 2014* (FISMA)² requires Federal agencies to conduct an annual independent performance audit or evaluation of 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 B – FY 2024 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.

FTC's Office of Inspector General (OIG) 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 DFC achieved for each of the core metrics and Fiscal Year (FY) 2024 supplemental metrics outlined in the *FY 2023 - 2024 Inspectors General (IG) FISMA Reporting Metrics*.

As part of our performance audit, we responded to the FY 2024 20 core and 17 supplemental metrics specified in OMB's *FY 2023 – 2024 IG FISMA Reporting Metrics*, dated February 10, 2023.³ These metrics provide reporting requirements across the functional areas to be addressed in the independent assessment of agencies' information security programs.⁴ We also considered applicable FTC and OMB policy and guidelines, and the National Institute of Standards and Technology (NIST) standards.

Summary Performance Audit Results

We assessed 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 five NIST Cybersecurity Framework Functions⁵ and nine FISMA Metric Domains.⁶ The overall maturity level of the FTC's information security program

² Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014 (Dec. 18, 2014).

³ 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.

⁴ Refer to the section titled, *Objective, Scope, and Methodology*, for more details.

⁵ Office of Management and Budget (OMB), Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the FISMA Reporting Metrics in consultation with the Federal Chief Information Officers Council. The nine FISMA Metric Domains were aligned with the five functions: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover as defined in the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.

⁶ As described in the FISMA Reporting Metrics, the nine FISMA Metric Domains are: (1) risk management, (2) supply chain risk management (3) configuration management, (4) identity and access management, (5) data protection and

was determined as Managed and Measurable, as described in this report. Our tests of the information security program identified one area for improvement in the [REDACTED] domain and one finding that fell in the [REDACTED] domain. There was one recommendation from a prior FISMA performance audit that remains open to address this specific finding. As such, we are not making a new recommendation in the FY 2024 FISMA audit. We assessed that the FTC's information security program and practices were effective from October 1, 2023, to July 31, 2024.

We provided the FTC with a draft of this report for comment. In a written response, management concurred with the results of our audit. See management's response in **Appendix A – Management's Response** for the FTC's response in its entirety.

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 (CIA) of information.

privacy, (6) security training, (7) information security continuous monitoring, (8) incident response, and (9) contingency planning.

Key Changes to the IG FISMA Metrics

One of the annual FISMA evaluation goals was to assess agencies' progress toward achieving outcomes that strengthen Federal cybersecurity, including implementing the Administration's priorities and best practices. OMB issued Memorandum M-24-04,⁷ *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, on December 4, 2023, which among other areas such as directs Federal agencies to increase their Continuous Diagnostics and Mitigation implementation efforts, and provides agencies with FY 2024 reporting guidance and deadlines in accordance with FISMA.⁸

As a representation of this guidance, on February 10, 2023, the final *FY 2023 – 2024 IG FISMA Reporting Metrics* were released,⁹ which included the 20 core metrics plus an additional 17 supplemental metrics to be assessed in the FY 2024 review cycle. The FY 2024 IG Metrics are based on coordinated discussions between (and the consensus opinion of) representatives from OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), Federal Civilian Executive Branch Chief Information Security Officers (CISO) and their staff, the Intelligence Community, and among other OIGs throughout the Federal government included in an established working group.¹⁰

OMB Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, also solidifies the timeline adjustment for the IG evaluation of agency effectiveness to align the results with the budget submission cycle. Historically, IG's evaluation of agency effectiveness finished in October until FY 2022, when the deadline shifted to July 31st of each year unless an extension was granted to September 30, 2022. For FY 2024, the IG evaluation has a deadline of July 31, 2024, for FISMA reporting to OMB and DHS to align the release of IG assessments to better facilitate the timely funding for the remediation of problems identified. The previous timing limited agency leadership's ability to request resources in the next Budget Year submissions for remediations.

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 information 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.

⁷ M-24-04 *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, December 4, 2023.

⁸ 44 U.S.C. §§ 3551 et seq.

⁹ *FY 2023 – 2024 IG FISMA Reporting Metrics* (February 10, 2023).

¹⁰ CISO Council FISMA Metrics Subcommittee.

FISMA, along with the *Paperwork Reduction Act of 1995* and the *Information Technology Management Reform Act of 1996* (known as the Clinger-Cohen Act), explicitly emphasizes a risk-based policy for 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 responsible agency officials understand the risks, and other factors, that could adversely affect its missions. Moreover, these officials must understand the current status of its security programs, and the security controls planned or in place, to protect its information and systems to make informed judgments and investments which appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions 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 oversight authority of agency security policies and practices and provided authority for implementing agency policies and practices for information systems to DHS.¹¹

FISMA required the Secretary of DHS to develop and oversee the implementation of operational directives requiring agencies to implement OMB's standards and guidelines for safeguarding federal information and systems from a known or reasonably suspected information security threat, vulnerability, or risk. FISMA directed the Secretary to consult with and consider guidance developed by NIST to ensure operational directives do not conflict with NIST information security standards.¹² It authorized the Director of OMB to revise or repeal operational directives not in accordance with the Director's policies.¹³

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 (GAO). 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 compliance of the systems at the time of the incidents; (4) detection, response, and remediation actions; (5) the 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.¹⁴

¹¹ FISMA, Pub. L. No. 113-283, 128 Stat. 3073 (December 2014). <https://www.congress.gov/bill/113th-congress/senate-bill/2521>.

¹² Ibid.

¹³ Ibid.

¹⁴ Ibid.

Core and FY 2024 Supplemental IG Metrics

OMB's *FY 2023 – 2024 IG FISMA Reporting Metrics* Version 1.1, dated February 10, 2023, specified the FY 2024 20 Core and 17 Supplemental IG Metrics. It directed IGs to report the assessed maturity levels of these metrics in CyberScope no later than July 31, 2024.

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 2024 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.

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.

In FY 2024, a calculated average scoring model was used, where core and supplemental metrics were averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. For example, if the calculated core metric maturity of two of the function areas is Level 3: Consistently Implemented (i.e., 3.0) and the computed core metric maturity of the remaining three function areas is Level 4: Managed and Measurable (i.e., 4.0), the information security program rating would average to be a 3.60 (i.e., $(3+3+4+4+4)/5$).

RMA focused on the results of the core metrics to determine maturity levels and 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. Although the DHS computed average of the maturity level was 3.95, the Consistently Implemented level, we rounded up to maturity level 4.0 and assessed the maturity level as Managed and Measurable. FTC control processes were operational and generated information that supported control monitoring and decision-making, thus exceeding the maturity level of Consistently Implemented. The Consistently Implemented level would not accurately depict FTC's control environment. As a result, FTC's overall maturity level was Managed and Measurable and is effective.

FTC's FY 2024 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 2024**.

Table 2: Overall Calculated Averages Maturity Calculation in FY 2024

Function	Core Metrics	FY 2024 Supplemental Metrics	FY 2024 Assessed Maturity Average ¹⁵	FY 2024 Assessed Maturity
Identify	3.83	3.33	3.58	Consistently Implemented
Protect	4.25	4.13	4.19	Managed and Measurable
Detect	4.00	4.00	4.00	Managed and Measurable
Respond	4.00	4.00	4.00	Managed and Measurable
Recover	4.00	4.00	4.00	Managed and Measurable
Calculated Maturity	4.02	3.89	3.95	Consistently Implemented
Assessed Maturity	4.02	3.89	4.00	Managed and Measurable

Objective

The objective of this audit was to evaluate the status of the FTC's overall IT security program and practices by evaluating the five NIST Cybersecurity Framework Functions:

- **Identify**, which includes questions pertaining to risk management and supply chain risk management (SCRM);
- **Protect**, which includes questions pertaining to configuration management, identity and access management (ICAM), data protection and privacy, and security training;
- **Detect**, which includes questions pertaining to information security continuous monitoring (ISCM);
- **Respond**, which includes questions pertaining to incident response; and
- **Recover**, which includes questions pertaining to contingency planning.

The answers to the core metrics and the FY 2024 supplemental metrics in **Appendix B – FY 2024 IG FISMA Reporting Metrics** reflect the results of our testing of the FTC's information security program and practices.

¹⁵ The FY 2024, the assessed maturity average was computed by averaging the core and supplemental metrics and the calculated averages were not rounded to determine the maturity level. In determining maturity levels and the overall effectiveness of FTC's information security program, RMA focused on the results of the core metric and made a risk-based assessment of the overall program and function level effectiveness.

Audit Results

We assessed the FTC's overall maturity level for its security program as Managed and Measurable. While the calculated average of the maturity levels was 3.95, we evaluated that FTC's control processes were effective based on their unique mission, resources, and challenges.

However, we did identify weaknesses [REDACTED]

[REDACTED] We did not issue a new recommendation for this finding due to an outstanding recommendation from a prior FISMA pending addressing by management. We assessed that FTC implemented an effective information security program, considering the agency's unique mission, resources, and challenges.

The maturity level for the nine domains is presented below in **Table 3: The FTC's FY 2024 Maturity Levels**.

Table 3: The FTC's FY 2024 Maturity Levels

Function	Maturity Level		
Function 1: Identify	Consistently Implemented (Level 3)		
• Risk Management			Managed and Measurable (Level 4)
[REDACTED]	[REDACTED]		
Function 2: Protect	Managed and Measurable (Level 4)		
• Configuration Management			Managed and Measurable (Level 4)
• Identity Management			Managed and Measurable (Level 4)
• Data Protection and Privacy			Managed and Measurable (Level 4)
• Security Training	Managed and Measurable (Level 4)		
Function 3: Detect—Information Security Continuous Monitoring	Managed and Measurable (Level 4)		
Function 4: Respond—Incident Response	Managed and Measurable (Level 4)		
Function 5: 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 provide the Chief Information Officer (CIO) with recommendations to remediate deficiencies.

IDENTIFY FUNCTION

The Identify Function relates to developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effectively using the Cybersecurity Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks

enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.¹⁶ The domains included under this function are Risk Management and SCRM. We assessed the Identity Function's maturity level as Consistently Implemented, and not effective.

Risk Management

Managing information system-related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization, from senior leaders providing the strategic vision, top-level goals, and objectives for the organization to mid-level leaders planning and managing projects to individuals on the front lines developing, implementing, and operating the systems supporting the organization's core missions and business processes. Federal guidance views risk management as a holistic activity fully integrated into every aspect of the organization.

Information security measures facilitate decision-making and improve performance and accountability by collecting, analyzing, and reporting relevant performance-related data. The measures also provide a means for assessing the efficiency and effectiveness of security controls. 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.

We assessed the FTC's overall maturity level for the risk management program was Managed and Measurable. The FTC defined the priority levels for its IT systems and implemented continuous monitoring processes that considered risks from the supporting business functions and mission impacts to help its leadership make informed risk management decisions. 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/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. Lastly, the agency evaluated risks associated with its assets and determined it had no high-value assets.¹⁷

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

¹⁶ NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (April 16, 2018).

¹⁷ 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.

SCRM

The supply chain infrastructure consists of the integrated set of components (hardware, software, and processes) within the organizational boundary, forming the environment where a system is developed, manufactured, tested, deployed, maintained, and retired/decommissioned. Each agency is required to train its personnel to identify, report, and mitigate counterfeit risks effectively.

Anti-counterfeit training for IT components includes essential topics to prepare personnel for these tasks. Training begins with understanding the types and significance of counterfeit components, including visual inspection, electrical testing, and non-destructive methods. Emphasis is placed on supply chain security, vendor qualification, and authentication methods. Through hands-on exercises, participants also learn risk management, explore technological advances, and practice interdepartmental coordination.

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

During the fieldwork, we noted that the FTC was

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

PROTECT FUNCTION

The Protect Function relates to developing and implementing appropriate safeguards to ensure the delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.¹⁸ The domains included under this function are Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training. We assessed the Protect Function's maturity level as Managed and Measurable, and effective.

Configuration Management

Configuration management comprises a collection of activities focused on establishing and maintaining the integrity of software and hardware systems through control of the processes for installing, initializing, changing, and monitoring the configurations of those systems. Procedures cover employee roles and responsibilities, change control and system documentation requirements, establishing a decision-making structure, and configuration management training.

We assessed that the FTC's overall maturity level for the configuration management program was Managed and Measurable. The FTC consistently implemented an organization-wide configuration management plan integrated into risk management and continuous monitoring processes. The FTC identified configuration management roles and responsibilities that described specific functions to be performed by officials and established an Enterprise Change Advisory Board to approve and manage all configuration changes.

We selected a sample of configuration changes that occurred in FY 2024 and determined FTC consistently followed its change control policies and procedures, and all changes made in FY 2024 were approved, as appropriate. The FTC monitored, analyzed, and reported qualitative and quantitative performance measures on the effectiveness of its change control activities and documented lessons learned on the effectiveness of its change control activities. Data supporting the metrics were obtained accurately, consistently, and in a reproducible format, ensuring that the Agency's Change Control Board is involved in the process.

The FTC utilized various automated mechanisms to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit any security impact. The FTC employed the Security Content Automation Protocol, which enabled scanners to detect network vulnerabilities and maintain an up-to-date, complete, 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 the FTC's configuration management program controls in place were effective.

¹⁸ NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (April 16, 2018).

ICAM

ICAM verifies a user's or device's identity, typically as a prerequisite for granting access to resources in an information system. For most systems, identification and authentication are the first lines of defense. Identification and authentication are technical measures that prevent unauthorized individuals or devices from entering a system. These defenses are critical building blocks of information security since they are the basis for most types of access control and for establishing user accountability. Access control often requires the system to identify and differentiate between users. For example, access control is usually based on the least privilege, which grants users only those accesses required to perform their duties. User accountability requires linking activities on a system to specific individuals and, therefore, requires the system to identify users. If the user is identified and authenticated through security controls, the user may be granted access to the user's permissions settings.

We assessed the FTC's overall maturity level for the ICAM program was Managed and Measurable. The FTC established an identification and authentication policy¹⁹ that defines processes of managing, monitoring, and securing access to protected resources. In addition, the FTC's access control policy²⁰ assigns responsibilities and defines requirements pertaining to developing and managing system access controls. Also, FTC ensured all personnel were assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically. FTC implemented a third-party identity management cloud service for its enterprise-wide single sign-on solution. All of the organization's systems interface with the solution to oversee employees, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on the effectiveness on a near real-time basis. The FTC used automation to manage and review user access agreements for privileged and non-privileged users. Additionally, FTC conducted monthly reviews of privileged user access. Further, FTC met privileged identity and credential management logging requirements at maturity EL2 (intermediate) in accordance with OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident* (OMB M-21-31).

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

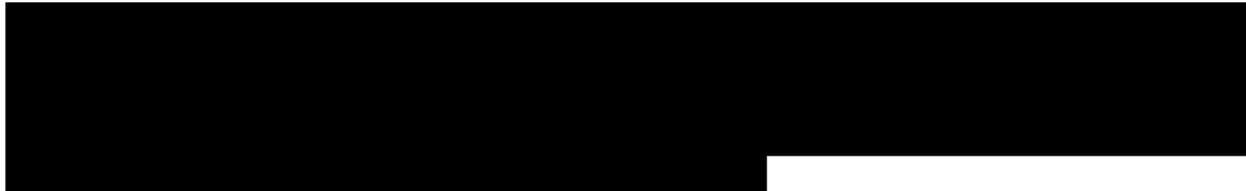
Data Protection and Privacy

Data Protection and Privacy refers to a collection of activities focused on the security objective of confidentiality, information access restrictions, personal privacy and proprietary information protection. Individual trust in the privacy and security of Personally Identifiable Information (PII) is strengthened through the effective implementation of information security controls. PII can range from an individual's name or email address to an individual's financial and medical records or criminal history. Unauthorized access, use, or disclosure of PII can seriously harm individuals and organizations by contributing to identity theft, blackmail, or embarrassment. Organizations



must identify and protect PII located within an organization's environment, assign PII impact levels, and select safeguards, respectively.

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 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. The FTC defined and communicated its data breach response plan²¹, including its processes and procedures for data breach notification. The breach response team participates in tabletop exercises and uses lessons learned to improve the plan. In addition, the FTC monitored and analyzed quantitative and qualitative performance measures to determine 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.



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

Security Awareness Training

A successful IT security program consists of 1) developing an IT security policy that reflects the business needs to be tempered by known risks; 2) informing users of their IT security responsibilities, as documented in agency security policy and procedures; and 3) establishing processes for monitoring and reviewing the program. Security awareness and training should focus on the organization's user population. Management should set an example of proper IT security behavior within an organization and an awareness program aimed at all levels of the organization, including senior and executive managers. The effectiveness of this effort will usually determine the effectiveness of the awareness and training program.

We assessed the FTC's overall maturity level for the security training program was Managed and Measurable. The FTC developed, documented, and disseminated comprehensive policies and procedures²² 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. In addition, the FTC's security training program consisted of three main parts. The first was mandatory annual training for every current employee and new hire to gain or maintain access to the FTC information systems. The second part was auditing the training for all employees



through phishing emails delivered to their accounts to test their application of training concepts during their everyday jobs. Finally, the third part is role-based/specialized training, which is deployed to individuals in specific roles or duties (system owners, authorizing officials, etc.) to enhance their understanding of the challenges faced during their roles/duties. FTC performed roles and responsibilities for security training, completed workforce assessment, and annual security training. Additionally, FTC effectively allocated resources in a risk-based manner so that stakeholders could implement security awareness training consistently. FTC also demonstrated the ability to monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans and addressed its identified knowledge, skills, and abilities 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.

DETECT FUNCTION

The Detect Function relates to the development and implementation of appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables the timely discovery of cybersecurity events.²³ The domain included under this function is Information Security and Continuous Monitoring. We assessed the Detect Function's maturity level as Managed and Measurable and effective.

ISCM

ISCM is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. An ISCM program is established to collect information in accordance with pre-established metrics, using information readily available in part through implemented security controls. Organizational officials gather and analyze the data regularly and as often as needed to manage risks appropriate for each organizational tier. This process involves the entire organization, from senior leaders providing governance and strategic vision to individuals developing, implementing, and operating individual systems supporting the organization's core missions and business processes. Subsequently, determinations are made from an organizational perspective on whether to conduct mitigation activities or reject, transfer, or accept risk.

We assessed the FTC's overall maturity level for the ISCM program was 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 strategy²⁴, the FTC updated ISCM policies²⁵ that cover the areas related to the FTC's overall ISCM program. Additionally, the FTC consistently updated its authorization package and conducted system-level security assessments annually. FTC

²³ NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (April 16, 2018).

analyzed quantitative and qualitative performance measures on 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. Further, FTC documented and implemented lessons learned to enhance the continuous monitoring process to instruct employees to record, analyze, and revise control activities on a cyclical basis to continuously improve FTC security posture as defined in the Security Continuous Monitoring Plan.

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

RESPOND FUNCTION

The Respond Function relates to developing and implementing appropriate activities to take action regarding a detected cybersecurity incident.²⁶ The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. The domain included under this function is Incident Response. We assessed the Respond Function's maturity level as Managed and Measurable, and effective.

Incident Response

Computer security incident response has become an essential component of IT programs. New types of security-related incidents emerge frequently. Cybersecurity-related attacks have become more numerous, diverse, damaging, and disruptive. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. Therefore, an incident response capability is necessary to rapidly detect incidents, minimize loss and destruction, mitigate exploited weaknesses, and restore IT services.

We assessed the FTC's overall Incident Response program maturity level as Managed and Measurable. The FTC has published Incident Response policies and procedures²⁷ that establish the FTC level of its Incident Response program, which outlines containment strategies, consideration for potential damage to and theft of resources, evidence preservation, service availability, 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.



²⁶ Ibid.



[REDACTED]

[REDACTED]

[REDACTED] the incident response controls were operating as intended. We assessed the FTC's incident response program controls in place were effective.

RECOVER FUNCTION

The Recover Function relates to developing and implementing appropriate activities to maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact of a cybersecurity incident.²⁹ The domain included under this function is Contingency Planning. We assessed the Recover Function's maturity level as Managed and Measurable, and effective.

Contingency Planning

Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. Contingency planning generally includes one or more of the following approaches to restore disrupted services:

- Restoring information systems using alternate equipment;
- Performing some or all the affected business processes using alternate processing (manual means (typically acceptable for only short-term disruptions));
- Recovering information systems operations at an alternate location (usually acceptable for only long-term disruptions or those physically impacting the facility) and
- Implementing appropriate contingency planning controls based on the information system's security impact level.

²⁹ NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (April 16, 2018).

We assessed the FTC's overall maturity level for the contingency planning program was Managed and Measurable. FTC consistently implemented an annual information system contingency plan testing/exercise and coordinated plan testing [REDACTED]

[REDACTED]

[REDACTED]

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 five Cybersecurity Functions and nine FISMA Metric Domains. Additionally, we evaluated that the FTC's information security program, and practices were effective from October 1, 2023, to July 31, 2024, and the overall maturity level of the FTC's information security program was Managed and Measurable. Our tests of the information security program identified one area for improvement in the [REDACTED] domain and one finding that fell in the [REDACTED] domain.

[REDACTED]

[REDACTED]

Scope and Methodology

Scope

The scope of the FISMA performance audit evaluated the overall information security program and practices of the FTC's unclassified systems to determine the effectiveness of such programs and practices for FY 2024 as of July 31, 2024. Our performance audit tested the effectiveness of the agency's information security policies, procedures, and practices of the FTC information systems to ascertain if it enabled the protection of the CIA of information. RMA answered the FY 2024 20 Core and 17 FY 2024 Supplemental IG Metrics issued by DHS.

Methodology

We conducted this performance audit in accordance with Government Auditing Standards. The performance audit was designed to determine whether the FTC implemented selected security controls for selected information systems in support of FISMA.

We obtained evidence that provided a reasonable basis for our findings and conclusions based on our performance audit objectives. We also 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 performance audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our performance audit objectives.

The overall strategy of our performance audit considered the NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53A Revision 5, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, the FISMA Metrics from the CIGIE, OMB, and DHS, and the FTC's policies and procedures. Our testing procedures were developed from NIST SP 800-53A. We assessed the overall maturity level of each of the nine domains by a calculated average scoring model, where the core and supplemental metrics were averaged independently for each maturity level of each question within the domain in accordance with the FISMA Metrics.

To test the operating effectiveness of the security controls, we exercised statistical analysis and methods to determine the number of items to select for testing and the method to select items. We also considered the relative risk and the significance or criticality of the specific items in achieving the related control objectives, along with the severity of a deficiency related to the control activity.

Criteria

We focused our FISMA performance audit approach on Federal information security guidelines developed by NIST, OMB, DHS, and the FTC. NIST SPs provide guidelines that were considered essential to developing and implementing the FTC's security programs. The following is a listing of the criteria used in the performance of the FY 2024 FISMA performance audit:

NIST Federal Information Processing Standards (FIPS) and SPs

- 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 800-50, *Building an Information Technology Security Awareness and Training Program*
- 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 2, *Computer Security Incident Handling Guide*
- 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 Federal Information Systems and Organizations*
- NIST SP 800-181, Revision 1, *Workforce Framework for Cybersecurity (NICE Framework)*
- NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management*

OMB Policy Directives

- OMB Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*
- 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-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*
- 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 (CSIP) for the Federal Civilian Government*
- OMB Circular A-123 - *Management's Responsibility for Internal Control*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*

GAO

- Standards for Internal Control in the Federal Government (September 2014)

DHS

- *FY 2023 – 2024 IG FISMA Reporting Metrics*
- DHS Binding Operational Directive 23-01, *Implementation Guidance for Improving Asset Visibility and Vulnerability Detection on Federal Networks*

- DHS Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- DHS Binding Operational Directive 20-01, *Develop and Publish Vulnerability Disclosure Policy*
- DHS Binding Operational Directive 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*
- DHS Binding Operational Directive 18-02 *Securing High Value Assets*
- DHS Binding Operational Directive 18-01, *Enhance Email and Web Security*
- DHS Binding Operational Directive 17-01, *Removal of Kaspersky-branded Products.*
- DHS Binding Operational Directive 16-03, *2016 Agency Cybersecurity Reporting Requirements*
- DHS Binding Operational Directive 16-02, *Threat to Network Infrastructure Devices*
- DHS Emergency Directive 21-04, *Mitigate Windows Print Spooler Service Vulnerability*
- DHS Emergency Directive 21-03, *Mitigate Pulse Connect Secure Product Vulnerabilities*
- DHS Emergency Directive 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*
- DHS Emergency Directive 21-01, *Mitigate SolarWinds Orion Code Compromise*
- DHS Emergency Directive 20-04, *Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday*
- DHS Emergency Directive 20-03, *Mitigate Windows Domain Name System (DNS) Server Vulnerability from July 2020 Patch Tuesday*
- DHS Emergency Directive 20-02, *Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday*
- DHS Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*

Abbreviations

BIA.....	Business Impact Analysis
CIA.....	Confidentiality, Integrity, and Availability
CIGIE.....	Council of the Inspectors General on Integrity and Efficiency
CIO.....	Chief Information Officer
CISA.....	Cybersecurity & Infrastructure Security Agency
CISO.....	Chief Information Security Officer
CSIRT.....	Computer Security Incident Response Team
DNS.....	Domain Name System
DHS.....	Department of Homeland Security
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
GAGAS.....	Generally Accepted Government Auditing Standards
GAO.....	Government Accountability Office
ICAM.....	Identity and Access Management
IG.....	Inspector General
ISCM.....	Information Security Continuous Monitoring
IT.....	Information Technology
NIST.....	National Institute of Standards and Technology
OIG.....	Office of Inspector General
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
TIC.....	Trusted Internet Connections

Appendix A – Management's Response



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

MEMORANDUM

DATE: September 23, 2024
FROM: Mark Gray, Chief Information Officer
TO: Andrew Katsaros, Inspector General
SUBJECT: Management's Response to the Federal Trade Commission (FTC) Federal Information Security Modernization Act of 2014 (FISMA) Audit Report for Fiscal Year (FY) 2024 ("*Report*") by RMA Associates

Federal Trade Commission (FTC) Management appreciates the report produced by the Office of the Inspector General (OIG) and RMA Associates. The agency will use the RMA recommendations to improve and strengthen its Information Security Program.

The FY 24 Report recognizes that the Information Security Program of the Federal Trade Commission is effective as indicated by ratings of "Managed and Measurable" for eight of the nine FISMA domains and by noting improvement to "Consistently Implemented" for [REDACTED]. The agency will incorporate further areas of improvement from the report for Supply Chain Risk Management into the agency's Information Resource Management (IRM) plan and overall Strategic Plan. The agency will continue to work on the Corrective Action Plan to address Event Logging and we expect to identify solutions and associate a budget by FY26.

The FTC is committed to continually improving its Information Security and Privacy Program through continued partnership with the OIG.

A handwritten signature in black ink, appearing to read "Mark Gray".

Digitally signed by MARK GRAY
Date: 2024.09.23 15:10:48 -04'00'

Mark Gray, Chief Information Officer

Appendix B – FY 2024 IG FISMA Reporting Metrics

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