FISCAL YEAR 2022 AUDIT OF THE FEDERAL TRADE COMMISSION INFORMATION SECURITY PROGRAM AND PRACTICES

Office of Inspector General
Federal Trade Commission

November 14, 2022

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

MEMORANDUM November 14, 2022

FROM: Andrew Katsaros
Inspector General

TO: Lina M. Khan, Chair

SUBJECT: Fiscal Year 2022 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) 2022.

The Office of Inspector General (OIG) contracted with RMA Associates, LLC (RMA) to conduct an independent audit to meet the FY 2022 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 November 14, 2022, and the conclusions expressed therein. We do not express an opinion on the FTC's compliance with FISMA or conclusions on other matters.

RMA identified one needed improvement, in the area of supply chain risk management. RMA made no recommendations for FY 2022.

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

A public version of this report will be posted on the OIG's website pursuant to sections 4 and 8M of the Inspector General Act of 1978, as amended (5 U.S.C. App., §§ 4 and 8M).

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 Reform;
- 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, or by email at akatsaros@ftc.gov.

RMA | Associates
Auditors. Consultants. Advisors.

Federal Trade Commission

Federal Information Security Modernization Act of 2014

Audit Report for Fiscal Year 2022

RMA Associates, LLC
1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
Fax: (703) 852-7272
www.rmafed.com

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

November 14, 2022

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

Ref: Federal Trade Commission (FTC) Federal Information Security Modernization Act of 2014 (FISMA) Audit Report for Fiscal Year (FY) 2022

Dear Mr. Katsaros:

RMA Associates, LLC is pleased to submit our FTC FISMA audit report for FY 2022. The objective of this audit was to evaluate the effectiveness of the FTC's information security program and practices for the period October 1, 2021, to July 31, 2022.

We conducted the audit in accordance with the Government Auditing Standards, issued by the Comptroller General of the United States, and relevant information security standards established by the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology (NIST). We have also prepared the FY 2022 Core IG FISMA Metrics (April 2022), as shown in Appendix B. These metrics provide reporting requirements across the NIST cybersecurity framework functional areas, which are to be addressed in the independent assessment of agencies' information security programs.

In summary, we found the FTC's information security program and practices were effective for the period October 1, 2021, to July 31, 2022.

We very much appreciate the opportunity to serve your organization and will be pleased to discuss any questions you may have.

Sincerely,

Reza Mahbod
President

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Inspector General
Federal Trade Commission

RMA Associates LLC (RMA) conducted a performance audit of the Federal Trade Commission's (FTC) information security program and practices for fiscal year (FY) 2022 in accordance with the *Federal Information Security Modernization Act of 2014* (FISMA). FISMA[1] requires Federal agencies to have 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.

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 outlined in the *FY 2022 Core IG FISMA Metrics.*

For this year's review, OMB required inspectors' generals to assess 20 of the 66 metrics from *FY 2021 IG FISMA Reporting Metrics v1.1* (May 12, 2021). The FY 2022 Core Inspectors General (IG) Metrics were aligned with the five following Cybersecurity Framework security functions areas: Identify, Protect, Detect, Respond, and Recover to determine the effectiveness of agencies' information security program. The FY 2022 Core IG Metrics classifies information security programs and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

The audit included an assessment of FTC's information security program and practices consistent with FISMA and reporting instructions issued by OMB. We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), as specified in the most current version of the Government Accountability Office's Government Auditing Standards (GAO "Yellow Book" / GAGAS), as well as guidelines established by the OMB DHS, and National Institute of Standards and Technology (NIST) guidance. 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 audit objective. We believe that the evidence obtained provides a reasonable basis for determining the maturity level for the core metrics and conclusions based on our audit objective. We also assessed selected security controls outlined in *NIST Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations*, for a sample of three (3) internal systems out of a total of 5 (five) FISMA reportable systems from FTC's FISMA inventory of information systems.

RMA conducted a FISMA audit for the period of October 1, 2021, to July 31, 2022. The audit fieldwork covered FTC's headquarters located in Washington, DC, from February 28 to [redacted].

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

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

We concluded that FTC implemented an effective information security program by achieving an overall Managed and Measurable maturity level based on the FY 2022 Core IG FISMA Metrics. Our tests of the information security program found no findings.

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 risks that conditions may materially change from their status. The information included in this report was obtained from FTC on or before [redacted]. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to [redacted].

Additional information on our findings and recommendations are included in the accompanying report. We are submitting this report to the Federal Trade Commission Office of Inspector General.

Sincerely,

RMA Associates

RMA Associates, LLC
Arlington, VA

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Table of Contents

Introduction 1
Summary Audit Results 1
Background 2
Key Changes to the Fiscal Year (FY) 2022 Core IG FISMA Metrics 2
Objective 5
Audit Results 6
Scope and Methodology 14
Criteria 15
Acronyms 18
Appendix A – Management's Response 19
Appendix B – FY 2022 IG Core FISMA Metrics 20

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Introduction

This report presents the results of our independent audit of the Federal Trade Commission's (FTC) information security program and practices. The *Federal Information Security Modernization Act of 2014* (FISMA) requires Federal agencies to have an annual independent audit performed 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: *Fiscal Year (FY) 2022 Core Inspector General Federal Information Security Modernization Act of 2014 Metrics* (Core FISMA Metrics). We also considered applicable OMB and the National Institute of Standards and Technology (NIST) policies, standards, and guidelines to perform the audit.

FISMA requires the agency Inspector General (IG) or an independent external auditor, as determined by the IG, to perform the annual audit. Consequently, the FTC Office of Inspector General (OIG) engaged RMA Associates LLC (RMA) to conduct an annual audit of the FTC's information security program and practices in support of the FISMA requirements. The objective of the audit was to evaluate the effectiveness of the FTC's information security program and practices for the period October 1, 2021, to July 31, 2022.

Summary Audit Results

We concluded 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 Functions[2] and nine FISMA Metric Domains.[3] The overall maturity level of the FTC's information security program was determined as Managed and Measurable, as described in this report. Accordingly, we found the FTC's information security program and practices were effective for the period October 1, 2021, to July 31, 2022.

We provided the FTC a draft of this report for comment; however, no internal control weakness was noted. In a written response, management concurs with the results of our audit. See *Management's Response* in Appendix A for the FTC's response in its entirety.

[2] 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*.

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

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

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 make certain those controls are operating as intended to safeguard the confidentiality, integrity, and availability (CIA) of information.

Key Changes to the Fiscal Year (FY) 2022 Core IG FISMA Metrics

One of the annual FISMA audit goals is to assess agencies' progress toward achieving outcomes that strengthen Federal cybersecurity, including implementing the Administration's priorities and best practices. The OMB Office of the Federal Chief Information Officer published Core Metrics, which is geared to the President's agenda, on April 13, 2021. The OMB issued Memorandum M-22-05[4], which provides guidance on Federal Information Security and Privacy Management Requirements. The metrics are based on coordinated discussions between (and the consensus opinion of) representatives from OMB, Council of the Inspectors General on Integrity and Efficiency (CIGIE), Federal Civilian Executive Branch Chief Information Security Officers and its staff, and the Intelligence Community. Research, interviews, and IG survey data provided quantitative and qualitative information to formulate these guidelines. The core metrics consist of 20 of the 66 FISMA questions from FY 2021 IG FISMA Reporting Metrics v1.1 (May 12, 2021).

[4] M-22-05 *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, December 6, 2021.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

The FY 2022 Core IG Metrics were chosen based on alignment with Executive Order (EO) 14028 (May 12, 2021), *Improving the Nation's Cybersecurity,* as well as recent OMB guidance to agencies in furtherance of the modernization of Federal cybersecurity, including:

- *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (M-22-09) – OMB and Cybersecurity & Infrastructure Security Agency (CISA) solicited public feedback on strategic and technical guidance documents meant to move the U.S. Government towards a zero-trust architecture. OMB's Federal Zero Trust Strategy aims to accelerate agencies towards a baseline of early zero trust maturity.
- Multifactor Authentication (MFA) and Encryption (EO 14028) – Per the EO, agencies were required to fully adopt MFA and encryption for data at rest and in transit by November 8, 2021. For agencies that were unable to meet these requirements within 180 days of the date of the order, the agency head was directed to provide a written rationale to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the Assistant to the President and National Security Advisor.
- *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (M-21-31) – This memorandum provides specific requirements for log management. It includes a maturation model, prioritizing the most critical log types and requirements, to build a roadmap to success.
- *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (M-22-01) – On October 8, 2021, this memorandum was issued for agencies to focus on improving early detection capabilities, creating "enterprise-level visibility" across components and sub-agencies, and requires agencies to deploy an Endpoint Detection and Response solution.
- Software Supply Chain Security & Critical Software – Section 4 of EO 14028 tasks OMB, NIST, and other Federal entities with developing new guidelines and frameworks to improve the security and integrity of the technology supply chain. In collaboration with industry and other partners, this effort provides frameworks and guidelines on how to assess and build secure technology, including open-source software.

Additionally, OMB Memorandum M-22-05 adjusts the timeline for the IG audit of agency effectiveness to align the results of the audit with the budget submission cycle. Historically, the audit of agency effectiveness by IGs finished in October. However, for FY 2022 the IG audit completion (submission to the Cyber Scope system) deadline has shifted from October to July to better align the release of IG assessments with the development of the President's Budget as mentioned in OMB M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements.* The previous timeline limited agency leadership's ability to request resources in the next Budget Year submissions to provide for remediations. The expectation is this change will reduce the time between issue identification, resource request, and allocation.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Federal Information Security Modernization Act of 2014

Title III of the *E-Government Act*, entitled the *Federal Information Security Management Act of 2002*, requires 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 result in less overall reporting, strengthened use of continuous monitoring in systems, and increased focus on the agencies for compliance and reporting that is more focused 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* (known as the Clinger-Cohen Act), explicitly emphasizes a risk-based policy for cost-effective security. In support of this legislation, OMB, through Circular No. A-130, *Managing Federal Information as a Strategic Resource*, requires executive agencies within the Federal Government to:

- Plan for security;
- Ensure appropriate officials are assigned security responsibility;
- Periodically review the security controls in their systems; and
- Authorize system processing prior to operations and periodically thereafter.

These management responsibilities presume responsible agency officials understand the risks and other factors that could adversely affect their 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 to make informed judgments and investments that 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.

NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems.

NIST also developed an integrated Risk Management Framework that effectively brings together all FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Core FISMA Metrics

We evaluated the effectiveness of the information security program and practices on a maturity model spectrum in which the foundation levels ensure the development of sound policies and procedures. The Core FISMA Metrics classify 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, represents an effective level of security:

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 to assess 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.

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 20 Core FISMA Metrics in Appendix B reflect the results of our testing of the FTC's information security program and practices.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

This audit also had an objective to review corrective actions taken by the Office of the Chief Information Officer to implement OIG's prior audit recommendations. FTC has implemented all OIG's prior audit recommendations.

Audit Results

We determined the maturity level for each FISMA domain based on the responses to the questions contained in the Core FISMA Metrics and testing for each domain. We determined the FTC's overall maturity level for its security program as Managed and Measurable based upon a simple majority of the component scores for each domain's maturity level. Our testing of the information security program found no significant control issues and concluded that the FTC's security program controls were effective.

We have presented the maturity level for the nine domains below:

Table 2: The FTC's FY 2022 Maturity Levels

Function	Maturity Level	
Function 1: Identify		Managed and Measurable (Level 4)
• Risk Management	Managed and Measurable (Level 4)	
• Supply Chain Risk Management	Consistently Implemented (Level 3)	
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**

Below is the maturity level for each domain.

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.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Information security measures facilitate decision-making and improve performance and accountability by collecting, analyzing, and reporting relevant performance-related data. The measures also provide the means for assessing the efficiency and effectiveness of security controls. The FTC uses performance measures as a management tool in its internal improvement efforts and links the implementation of its information security program to agency-level strategic planning efforts.

We determined the FTC's overall maturity level for the risk management program is 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. Additionally, the agency has risk management policies, procedures, and strategies, including methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk. Furthermore, the FTC maintained comprehensive and accurate hardware and software inventories. Lastly, the agency evaluated risks associated with its assets and determined it had no high-value assets.[5]

The FTC had a process for identifying and prioritizing internal and external threats using a common vulnerability scoring system that identifies network vulnerabilities and the potential likelihood of business impacts of threats. The agency consistently managed its Plans of Action & Milestones to identify and track weaknesses at the enterprise level and monitor system-specific weaknesses at the system level.

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

Supply Chain Risk Management (SCRM)

The supply chain infrastructure is the integrated set of components (hardware, software, and processes) within the organizational boundary that composes the environment in which a system is developed or manufactured, tested, deployed, maintained, and retired/decommissioned. The supply chain consists of multiple layers of system integrators, external service providers, and suppliers. The supply chain risks include the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware (e.g., global positioning system tracking devices, computer chips, etc.), and poor manufacturing and development practices in the supply chain.

We determined the FTC's overall maturity level for the SCRM program was Consistently Implemented. FTC defined and communicated policies and procedures to ensure that products, system components, systems, and services adhere to its cybersecurity and SCRM requirements. FTC identified and prioritized externally provided systems, system components, and services and

[5] 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.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

maintained awareness of its upstream suppliers. FTC integrated its acquisition processes, including contractual agreements stipulating appropriate cyber measures for external providers.

FTC's SCRM implemented sufficient controls to be assessed at the Consistently Implemented level. FTC was in the process of implementing some of its SCRM controls. To reach the Managed and Measurable level, and for the control to be effective, FTC must complete implementing the controls and show their effectiveness. As such, the FTC's SCRM controls were not operating as intended and were not effective.

Area of Improvement: To increase the cybersecurity maturity level for FISMA DHS Question 14[6] to Managed and Measurable (Level 4), the FTC should continue its effort to complete implementing the SCRM controls. Specifically, FTC needs to demonstrate how to utilize qualitative and quantitative performance metrics to measure, report on, and monitor the information security and SCRM performance of organizationally defined products, systems, and services provided by external providers. In addition, FTC needs to incorporate supplier risk evaluations, based on criticality, into its continuous monitoring practices to maintain situational awareness of the supply chain risks.

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, the establishment of a decision-making structure, and configuration management training.

We determined the FTC's overall maturity level for the configuration management program is Managed and Measurable. The FTC consistently implemented an organization-wide configuration management plan, and the plan was 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. 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.

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 Security Content Automation Protocol 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.

[6] FY 2022 Core IG FISMA Metrics

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

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

Identity and Access Management

ICAM is the means of verifying the identity of a user or device, 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 it is the basis for most types of access control and for establishing user accountability. Access control often requires the system to be able to identify and differentiate between users. For example, access control is usually based on 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 determined the FTC's overall maturity level for the ICAM program is Managed and Measurable. The FTC established an identification and authentication policy[7] that defines processes of managing, monitoring, and securing access to protected resources. In addition, the FTC's access control policy[8] assigns responsibilities and defines requirements pertaining to developing and managing system access controls. Also, FTC held stakeholders accountable for carrying out their roles and responsibilities effectively by having its employees adhere to the two ICAM policies referenced above. Its managers used task orders and gathered lessons learned from its processes to hold employees accountable.

The FTC used automation to manage and review user access agreements for privileged and non-privileged users. Additionally, FTC conducted [redacted] reviews of privileged user access.

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

Data Protection and Privacy

Data Protection and Privacy refer to a collection of activities focused on the security objective of confidentiality, information access restrictions, and 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

[7] [redacted]
[8] [redacted]

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

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

We determined the FTC's overall maturity level for the data protection and privacy program is Managed and Measurable. The FTC protected PII through a combination of measures, including operational safeguards, privacy-specific safeguards, and security controls. The FTC used a risk-based approach to protect the confidentiality of PII. The FTC's Privacy Program Plan[9] requires a Privacy Steering Committee and a Chief Privacy Officer (CPO). The Privacy Steering Committee comprises an internal agency advisory group of representatives from bureaus and offices within the FTC. Its mission is to help implement an effective agency-wide privacy program and ensure sound practices and controls are integrated into the FTC's operations. The committee also acts as a consulting board for the agency and offers solutions and feedback on privacy matters across the organization.

The CPO advises the Chair and other senior officials on internal privacy issues, including the protection of PII. The CPO's duties include overseeing the agency's privacy compliance efforts, reviewing all agency privacy policies, performing assessments and monitoring, directing privacy training for all the FTC employees and contractors, and promoting privacy awareness amongst the FTC staff.

Moreover, the FTC dedicated significant resources to its privacy program. It maintained an inventory of the collection and use of PII, conducted, and maintained privacy impact assessments, and system of records notices for all applicable systems.

The FTC has defined and communicated its data breach response plan, 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, FTC monitored and analyzed quantitative and qualitative performance measures on the effectiveness of its privacy activities.

Our testing of the data protection and privacy program found no exceptions and concluded 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 be focused on the organization's entire 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.

[9] [redacted]

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

We determined the FTC's overall maturity level for the security training program is Managed and Measurable. The FTC developed, documented, and disseminated comprehensive policies and procedures[10] 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 has three main parts. The first is mandatory, annual training for every current employee and new hire, to gain or maintain access to the FTC information systems. The second part is auditing the training for all employees through fake phishing emails delivered into their accounts to test their application of training concepts during their everyday job. 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.

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

Information Security Continuous Monitoring

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 determined the FTC's overall maturity level for the ISCM program is 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, FTC has updated ISCM policies that cover the areas related to FTC's overall ISCM program

Additionally, FTC analyzed quantitative and quantitative performance measures on the effectiveness of its ISCM policies and procedures through monthly, quarterly, and yearly continuous monitoring reports. FTC used the results of security control assessments and monitoring to maintain ongoing authorizations of information systems.

Our testing of the ISCM program found no exceptions and concluded the FTC's ISCM program

[10] [redacted]

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

controls in place were 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 not only more numerous and diverse but also more 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 for rapidly detecting incidents, minimizing loss and destruction, mitigating exploited weaknesses, and restoring IT services.

We determined the FTC's overall maturity level for the Incident Response program is Managed and Measurable. The FTC has published Incident Response policies and procedures[11] 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 found the FTC personnel reported potential incidents to the CSIRT, which handled reported incidents in accordance with the plan. In addition, the FTC used several software tools to detect suspected incidences and used a ticketing system to track incidences, mitigate the threat, and determine whether the threat affected other systems. Also, the ticketing system keeps track of reported incident response activities sent to the United States Computer Emergency Response Team (US-CERT).

The FTC utilized Tenable security center dashboards to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. Through this capability, the FTC was able to detect and prevent potential compromises.

Our testing of the incident response program found no exceptions and concluded that the FTC's incident response program controls were 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;

[11] [redacted]

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

- 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.

We determined the FTC's overall maturity level for the contingency planning program is Managed and Measurable. The FTC developed, maintained, and integrated system contingency planning through policies, procedures, and strategies. The policies and procedures defined the roles and responsibilities of stakeholders involved in information systems contingency planning.

Additionally, the FTC prepared a Business Impact Assessment and used the results to guide contingency planning efforts and inform senior-level decision-making. Moreover, our testing noted that FTC performed an annual tabletop exercise of its information system contingency planning processes and adequately documented lessons learned to improve the plan. The information system contingency plans and performance of recovery activities were disseminated and communicated to relevant stakeholders via the utilization of the Cyber Security Assessment and Management system.

Our testing of the contingency planning program found no exceptions and concluded that the FTC's contingency Planning program controls were effective.

Overall Conclusion

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, we concluded that the FTC's information security program and practices were established and have been maintained for the five Cybersecurity Functions and nine FISMA Metric Domains. Additionally, we found the FTC's information security program and practices were effective from October 1, 2021, to July 31, 2022. The overall maturity level of the FTC's information security program was Managed and Measurable.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Scope and Methodology

Scope

The scope of the FISMA 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 2022 as of July 31, 2022. Our 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 20 IG Core FISMA Metrics issued by DHS.

Methodology

We conducted this audit in accordance with Government Auditing Standards. The audit is 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 audit objectives. We also conducted this audit in accordance with Generally Accepted Government Auditing Standards (also known as the Yellow Book) issued by the Comptroller General of the United States. These standards require 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 objectives.

The overall strategy of our audit considered the NIST Special Publication (SP*)* 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* NIST SP 800-53A Revision 5, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations,* the Core FISMA Metrics from the Council of the Inspectors General on Integrity and Efficiency (CIGIE), OMB, and DHS, and the Council's policies and procedures. Our testing procedures were developed from NIST SP 800-53A. We determined the overall maturity level of each of the nine domains by a simple majority of the competent scores of the maturity level of each question within the domain, in accordance with the Core FISMA Metrics.

For testing the operating effectiveness of the security controls, we exercised statistical analysis and methods in determining the number of items to select for testing and the method to be used 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.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Criteria

We focused our FISMA 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 2022 FISMA audit:

NIST Federal Information Processing Standards (FIPS) and Special Publications

- 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 3, *Guide to Enterprise Patch Management Technologies*
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
- 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 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*

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

- NIST SP 800-161, *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 (ERM)*

OMB Policy Directives

- OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*
- OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*
- 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 (CISP) for the Federal Civilian Government*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*

DHS

- FY 2022 Core IG FISMA Metrics
- DHS Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- DHS Emergency Directive 21-04, *Mitigate Windows Print Spooler Service Vulnerability*
- DHS Emergency Directive 21-03, *Mitigate Pulse Connect Secure Product Vulnerabilities*

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

- 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 DNS Server Vulnerability from July 2020 Patch Tuesday*
- DHS Emergency Directive 20-02, *Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday*
- 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 Emergency Directive 19-01, *Mitigate DNS Infrastructure Tampering*
- 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*

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Acronyms

CIA.....Confidentiality, Integrity, and Availability
CIGIE.....Council of the Inspectors General on Integrity and Efficiency
CPO.....Chief Privacy Officer
CSIRT.....Computer Security Incident Response Team
DHS.....Department of Homeland Security
ERM.....Enterprise Risk Management
FIPS.....Federal Information Processing Standards
FISMA.....Federal Information Security Modernization Act of 2014
FTC.....Federal Trade Commission
FY.....Fiscal Year
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
RMA.....RMA Associates LLC
SCRM.....Supply Chain Risk Management
SP.....Special Publication
US-CERT.....United States Computer Emergency Readiness Team

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Appendix A – Management's Response

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

MEMORANDUM

DATE: November 8, 2022

FROM: Raghav Vajjhala, Chief Information and Chief Data 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) 2022 *("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 22 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 Supply Chain Risk Management. 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 FTC is committed to continually improving its Information Security and Privacy Program through continued partnership with the OIG.

RAGHAV VAJJHALA
Digitally signed by RAGHAV VAJJHALA
Date: 2022.11.09 10:10:09 -05'00'

Raghav Vajjhala, Chief Information Officer and Chief Data Officer

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Appendix B – FY 2022 IG Core FISMA Metrics

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