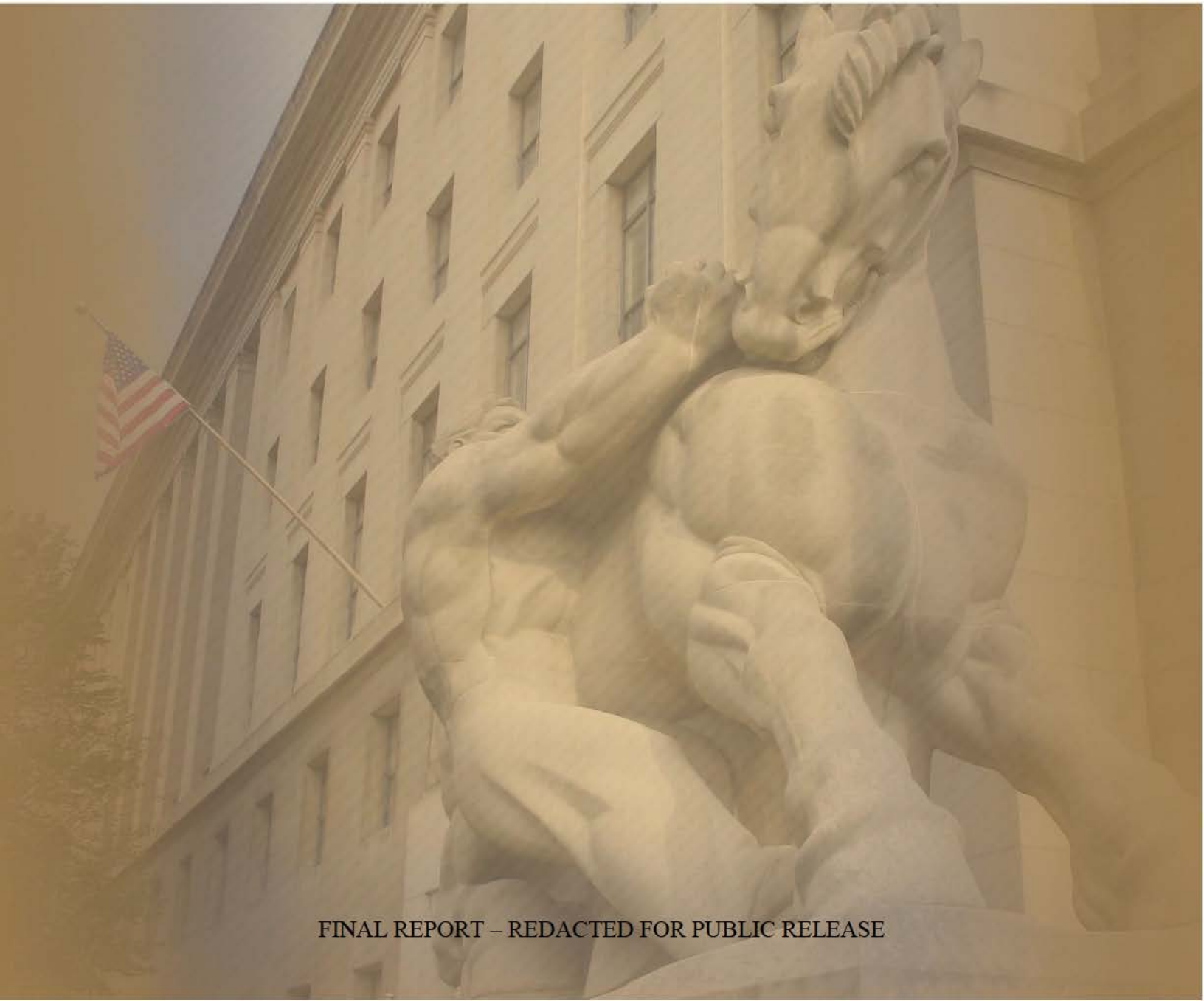
Federal Trade Commission
Office of Inspector General

Audit of Federal Trade Commission Information Security Program and Practices

OIG Report No. A-20-05 February 4, 2020



FINAL REPORT – REDACTED FOR PUBLIC RELEASE

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

Office of Inspector General

February 4, 2020

MEMORANDUM

FROM: Andrew Katsaros
Inspector General

TO: Joseph J. Simons, Chairman
Commissioner Noah Joshua Phillips
Commissioner Rohit Chopra
Commissioner Rebecca Kelly Slaughter
Commissioner Christine S. Wilson

SUBJECT: Fiscal Year 2019 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 annual independent evaluation of the Federal Trade Commission's (FTC) Information Security Program and Practices for Fiscal Year (FY) 2019.

The Office of Inspector General (OIG) contracted with RMA Associates, LLC (RMA) to conduct an independent audit to meet the FY 2019 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 February 4, 2020, and the conclusions expressed therein. We do not express an opinion on the FTC's compliance with FISMA or conclusions on other matters. The OIG's independent auditors will follow-up on the outstanding recommendations and evaluate the adequacy of corrective actions during the FY 2020 FISMA audit.

RMA identified needed improvements in the areas of risk management, configuration management, identity and access management, and contingency planning. RMA made six recommendations intended to assist the FTC in improving the overall management and security of IT resource.

The FTC's response to the draft report's findings and recommendations is included as Appendix B. The response reflects that the FTC concurred with the report's six recommendations.

Final Report - Redacted for Public Release

Please submit to us an action plan that addresses the recommendations in this report within 60 calendar days. 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 Energy and Commerce
- House Committee on Homeland Security
- House Committee on the Judiciary
- House Committee on Oversight and Reform
- House Committee on Science, Space, and Technology
- Senate Committee on Commerce, Science, and Transportation
- Senate Committee on Homeland Security and Governmental Affairs
- Senate Committee on the Judiciary
- The appropriate authorization and appropriations committees of the House and Senate

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 2019

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

February 4, 2020

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

Ref: Final Federal Trade Commission (FTC) Federal Information Security Modernization Act of 2014 (FISMA) Audit Report for Fiscal Year (FY) 2019

Dear Mr. Katsaros:

RMA Associates, LLC (RMA) is pleased to submit our final FTC FISMA audit report for FY 2019. 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 (OMB), the Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST). We have also prepared the *FY 2019 Inspector General (IG) FISMA Reporting Metrics Version 1.3* (April 9, 2019), as shown in Appendix C. 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. The objective of this audit was to evaluate the effectiveness of the Commission's information security program and practices for FY 2019.

In summary, we found FTC's information security program and practices were effective for the period October 1, 2018, to September 30, 2019.

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

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 **1**
Background **1**
FISMA 2
Key Changes to the FY 2019 IG FISMA Metrics 3
Objectives 4
Audit Results **4**
Risk Management 5
Configuration Management 7
Identity and Access Management 8
Data Protection and Privacy 10
Security Awareness Training 11
Information Security Continuous Monitoring 11
Incident Response 12
Contingency Planning 13
Scope and Methodology **14**
Scope 14
Methodology 15
Criteria 15
Appendix A: Acronyms **18**
Appendix B: Management's Response **19**
Appendix C: FY 2019 IG FISMA Reporting Metrics **23**

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 FTC's information security program and practices. FISMA requires Federal agencies to have an annual independent audit performed of their information security program and practices to determine the effectiveness of such program and practices, and to report the results of the audits to OMB. OMB delegated its responsibility to DHS for the collection of annual FISMA responses. DHS prepared the FISMA questionnaire to collect these responses, which is provided in Appendix C. We also considered applicable OMB and NIST policy, standards, and guidelines to perform the audit.

Furthermore, FISMA requires the agency's 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 to conduct an audit in support of the FISMA requirements. The objective of the audit was to evaluate the effectiveness of FTC's information security program and practices for the period October 1, 2018, to September 30, 2019.

Summary

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, FTC's information security program and practices were established and maintained for the five NIST Cybersecurity Framework Functions and eight FISMA Metric Domains. 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 FTC's information security program and practices were effective for the period October 1, 2018, to September 30, 2019.

We provided the FTC 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 B for FTC's response in its entirety.

Background

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.

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

As it relates to information technology (IT), 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

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

to ensure information systems and the data shared between them are protected. Improving the overall management and security of IT resources and stakeholder information must be a top priority for 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 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.

FISMA

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 *of 2014* 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 the 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 the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies.

Key Changes to the FY 2019 IG FISMA Metrics

One of the goals of the annual FISMA evaluations is to assess the agency's progress toward achieving outcomes that strengthen Federal cybersecurity, including implementing the Administration's priorities and best practices. The FY 2019 Chief Information Officer (CIO) FISMA Metrics, OMB Memorandum M-19-03, "Strengthening the Cybersecurity of Federal Agencies by Enhancing the High-Value Asset Program," and DHS' Binding Operational Directive 18-02, "Securing High-Value Assets," have placed additional emphasis on the enhancement of the High-Value Asset (HVA)[1] program. As such, the FISMA Reporting Metrics include additional maturity indicators and criteria references regarding the evaluation of the effectiveness of agencies' HVA programs.

Furthermore, on December 21, 2018, the Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act of 2018 (SECURE Technology Act) established new requirements for supply chain risk management. The FISMA Reporting Metrics have been updated to gauge agencies' preparedness in addressing these new requirements.

In addition, NIST has updated several of its Special Publications (SP) to enhance existing criteria, such as NIST SP 800-37 (Revision 2) and NIST SP 800-160 (Volume 1). These updates include changes to criteria that impact the FISMA reporting metrics, such as alignment with the constructs in the NIST Cybersecurity Framework and the system life cycle security engineering processes, integration of privacy risk management processes, and incorporation of supply chain risk management processes. While the updates will not go into full effect until one year after their respective publications, the criteria references in the FISMA reporting metrics have been updated to reflect these changes.

As a result of these updates and changes, 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 FISMA reporting metrics classify information security program and practices into five maturity model levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. Within the context of the maturity model,

[1] "High Value Assets" are those assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people.

Level 4, Managed and Measurable represents an effective level of security. Below is a table demonstrating the maturity model.

Table 1: FISMA Reporting Metrics Maturity Model

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 on 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.

Objectives

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

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

Our detailed audit included testing to answer the 67 IG FISMA Reporting Metrics as shown in Appendix C of this report.

Audit Results

We determined the maturity level for each FISMA domain based on the responses to the questions contained in the FISMA Reporting Metrics and testing for each domain. We determined FTC's overall maturity level for its security program as Managed and Measurable. Our testing of the

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

information security program found no significant control issues and concluded the FTC's security program controls in place were effective.

Below is a summary of 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.

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

We determined FTC's overall maturity level for the risk management program is Managed and Measurable. 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, FTC maintained comprehensive and accurate hardware and software inventories. Lastly, the agency evaluated risks associated with its assets and determined it had no HVAs.

FTC has 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 manages its Plans of Action & Milestones (POA&Ms) to identify and track weaknesses at the enterprise-level and monitor system-specific weaknesses at the system-level.

Although we found areas where FTC can improve its program, the risk management controls were operating as intended. We concluded FTC's risk management program controls in place were effective.

Observation 1: Four FTC documents were not noted as approved by an authorizing official, and two additional documents were in draft status. Without approved plans or assessments, FTC officials cannot determine and validate whether the documents express management conclusions, objectives, strategies, or goals. *The Government Accountability Office (GAO), Standards for*

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

Internal Control in the Federal Government: Section 1 - Fundamental Concepts of Internal Control, Definition of Internal Control states,

> "Internal control comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity. Internal control serves as the first line of defense in safeguarding assets. In short, internal control helps managers achieve desired results through effective stewardship of public resources."

FTC does not have a consistent approval process for its procedures, plans, strategies, assessments, profiles, and reports. The lack of consistent approval from authority officials concerning procedures may result in an increased risk of unclear, misunderstood, fragmented, inconsistent, and improperly implemented security practices. Also, plans, strategies, assessments, profiles, and reports without designated management approval embedded in these documents may not accurately express management's views or conclusions.

Recommendation 1: We recommend FTC develop a consistent approval process that includes the designation of management's approval embedded in its policies, procedures, plans, strategies, assessments, profiles, and reports.

Observation 2: FTC consistently manages its POA&Ms to identify and track weaknesses at the enterprise-level, as well as track system-specific weaknesses at the system-level. However, some POA&Ms are significantly beyond the completion date and other POA&Ms that were past due were not updated to include a revised completion date, nor was a sufficient justification provided as to why they were not closed. The *OMB Circular No. A-50 Revised Audit Follow-up September 29, 1982*, requires Federal Entities to perform corrective actions promptly on audit recommendations. The FTC POA&M process did not include the evaluation of FTC's explanations of delay to complete the corrective action by the estimated completion date. Most importantly, the longer the corrective action is outstanding, there is an increased risk controls will not detect or prevent unauthorized activities.

Recommendation 2: We recommend FTC implement fully effective policies and procedures related to POA&Ms to ensure all identified security weaknesses are tracked, prioritized, and remediated in a timely manner, including a process to evaluate the adequacy of justifications to ensure the estimated completion date is met and determine the dependencies and completion of milestones that affect the estimated due date.

Observation 3: FTC did not use qualitative and quantitative performance metrics to measure, report, and monitor information security performance of its contractor-operated systems and services, change control activities, data exfiltration, enhanced network defenses, and data breach response plan. *NIST SP 800-55 Revision 1 Performance Measurement Guide for Information Security* states,

> "The information security measurement program described in this document can be helpful in fulfilling regulatory requirements. The program provides an underlying data collection,

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

analysis, and reporting infrastructure that can be tailored to support Federal Enterprise Architecture's (FEA) Performance Reference Model (PRM) requirements, and any other enterprise-specific requirements for reporting quantifiable information about information security performance."

The information security measurement program ensures measures are developed, causes are identified for poor performance, and appropriate corrective actions are taken. Although FTC has employed a sustained process of performing risk assessments to determine the respective risk posture of its systems, it did not enhance the process to leverage and report in a broader array of quantitative and qualitative performance metrics. FTC has prioritized the analysis and reporting of Enterprise Risk Management (ERM) performance metrics as a means of assessing effectiveness.

Recommendation 3: We recommend FTC enhance its process of performing ERM assessments to determine the respective risk posture of its systems to include the entity-wide performance metrics for measuring the effectiveness of its:

- Contractor-operated systems and contractor-provided IT services;
- Change control activities to ensure data supporting the metrics is obtained accurately, consistently, and in a reproducible format;
- Data exfiltration and enhanced network defenses; and
- Data Breach Response Plan to ensure data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

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

FTC applied standard baselines to control hardware and software configurations and centrally managed its flaw remediation process and applied software patches. In addition, the agency's Continuous Assurance Branch (CAB) performs vulnerability scans at least monthly for all FTC owned and operated systems that do not have internal scanning capabilities. Moreover, FTC employed Security Content Automation Protocol (SCAP) 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.

Furthermore, FTC adopted the Trusted Internet Connections (TIC) program to assist in protecting its network. The agency routed external network traffic to non-FTC systems through a Managed Trusted Internet Protocol Service (MTIPS)[2] connection, which is a DHS and General Services Administration (GSA) approved TIC provider.

Although we found areas where FTC can improve its program, we concluded the agency's configuration management security controls in place were effective.

Observation 4: Although FTC's configuration settings prevent users from downloading software on their systems, [redacted] *NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations Revision 4* states,

- "An organization should employ automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system;" and
- "Takes the following actions when unauthorized components are detected: [*Selection (one or more): disables network access by such components; isolates the components; notifies* [*Assignment: organization-defined personnel or roles*]]."

Although FTC has procured sufficient tools, it has yet to implement all the tools. The agency plans to implement the security tools upon the completion of higher priority information security initiatives, including the implementation of the Center of Information Security (CIS) level-one benchmarks. However, [redacted]

Recommendation 4: We recommend FTC develop and implement a defined process to [redacted] on its network and employ automated mechanisms such as application whitelisting and network management tools to [redacted]

Identity and Access Management

Identity and Access Management (IAM) 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

[2] MTIPS was developed by the US General Services Administration (GSA) to allow US Federal agencies to physically and logically connect to the public Internet and other external connections in compliance with the Office of Management and Budget's (OMB) Trusted Internet Connection (TIC) Initiative.

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

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 refers to granting 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 then be granted access related to the user's permissions settings.

We determined FTC's overall maturity level for the identity and access management program is Managed and Measurable. FTC established an identification and authentication policy[3] that defines processes of managing, monitoring, and securing access to protected resources. In addition, FTC's access control policy[4] required the Information System Security Officer (ISSO) to ensure a review of system and user accounts are performed monthly for privileged access and every six months for non-privileged access.

Moreover, FTC conducted background investigations on all new employees before allowing access to its network, as well as centrally tracked and shared risk designations and screening information with necessary parties. The agency also granted access only on a need-to-know basis and employees, including contractors to use Personal Identity Verification (PIV) for identification, authentication, and access to IT services and physical locations.

Although we found areas where FTC can improve its program, our testing found the controls were operating as intended. We concluded FTC's identity and access management security controls in place were effective.

Observation 5: FTC did not implement [redacted] *NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations Revision 4* states,

- "The organization should employ automated mechanisms to support the management of information system accounts. The FTC relied on manual approaches to disabling accounts."
- "The organization separates [Assignment: organization-defined duties of individuals], documents separation of duties of individuals, and defines information system access authorizations to support the separation of duties."

[3] [redacted]
[4]

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

[redacted] Without automated segregation of duties, there is an increased risk for unauthorized modification, deletion, or retrieval of information and system files without detection. Lastly, the absence of least privilege reviews puts the organization at risk as it is uncertain if personnel have appropriate account configurations.

Recommendation 5: We recommend FTC implement automated mechanisms to [redacted] inventory and manage accounts, and perform segregation of duties and least privilege reviews.

Data Protection and Privacy

Data protection and privacy refers to a collection of activities focused on the security objective of confidentiality, restrictions on information access, and protection of personal privacy and proprietary information. 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 determined FTC's overall maturity level for the data protection and privacy program is Managed and Measurable. FTC protects PII through a combination of measures, including operational safeguards, privacy-specific safeguards, and security controls. FTC uses a risk-based approach for protecting the confidentiality of PII. FTC's Privacy Program Plan[5] 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 FTC. Its mission is to help implement an effective agency-wide privacy program and ensure sound practices and controls are integrated into 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 duties include overseeing the agency's privacy compliance efforts, reviewing all agency privacy policies, performing assessments and monitoring, directing privacy training for all FTC employees and contractors, and promoting privacy awareness amongst FTC staff.

Moreover, 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 record notices for all applicable systems. FTC also removed unnecessary PII and had an independent third-party review of its privacy program.

[5] *Privacy Program Plan* updated November 2016.

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

Additionally, 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 table-top exercises and uses lessons learned to make improvements to the plan.

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

Security Awareness Training

A successful IT security program consists of 1) developing 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.

We determined FTC's overall maturity level for the security training program is Managed and Measurable. The FTC developed, documented, and disseminated comprehensive policies and procedures[6] for security awareness and specialized security training. FTC defined the roles and responsibilities of individuals executing duties serving the security awareness and training program.

In addition, 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 FTC information systems. The second part is the auditing of that training for all employees, through fake phishing emails delivered into their accounts in order to test their application of training concepts during the course of 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.) in order to enhance their understanding of the particular challenges faced during the course of their roles/duties.

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

Information Security Continuous Monitoring

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

[6] [redacted]

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

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 in support of the organization's core missions and business processes. Subsequently, determinations are made from an organizational perspective on whether to conduct mitigation activities or to reject, transfer, or accept risk.

We determined the FTC's overall maturity level for the ISCM program is Managed and Measurable. FTC's ISCM strategy[7] established a general approach to maintain awareness of FTC's cybersecurity posture to support risk management decisions and establish guidelines for granting ongoing authorizations. The strategy focused on actions at enterprise and system-levels that support the shift from a static snapshot of the organization system's security posture, to a near real-time, dynamic security status. The strategy initiated the CAB referenced earlier, which supports and prioritizes the implementation of the DHS Continuous Diagnostics and Mitigation (CDM) program and aligns the ISCM activities.

Additionally, FTC continuously maintained the status of known security weaknesses by its POA&M process. The POA&M process documented and tracked weaknesses of security controls and other program deficiencies in the [redacted] Furthermore, FTC maintains a list of control activities that are continuously monitored and analyzed that act as qualitative and quantitative performance measures on the effectiveness of its ISCM strategy.

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

Incident Response

Computer security incident response has become an essential component of IT programs. Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

We determined FTC's overall maturity level for the incident response program is Managed and Measurable. FTC has published Incident Response policies and procedures[8] 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, FTC centralized its incident response function by establishing the Computer Security Incident Response Team (CSIRT), which is comprised of incident handlers within the CAB and other agency security officials.

[7] *Information Systems Continuous Monitoring Strategy*, July 2018.
[8] [redacted]

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

We found FTC personnel reported potential incidents to the CSIRT, which handled reported incidents in accordance with the plan. In addition, FTC used several software tools to detect suspected incidences and uses 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).
Furthermore, FTC participated in the Eagle Horizon 2019 exercise. The exercise simulated a major cyber-attack, disrupting not only the Nation Capital Region (NCR), but also included the FTC regional offices. The exercise scenarios facilitated tabletop discussions concerning emergency communications, staff communications, preparing and securing facilities, actions to preserve IT systems functionality and data, emergency activities conducted by FTC Regional Offices (specifically Cleveland), and reconstitution and devolution efforts. The exercise was internally evaluated and received an overall score of 95 percent.

Moreover, FTC uses DHS's EINSTEIN program for intrusion detection/prevention capabilities for traffic entering and leaving FTC's networks. The agency uses the incident detection and prevention services provided by AT&T in partnership with DHS as part of the EINSTEIN program. Through this capability, FTC was able to detect and prevent potential compromises.

Our testing of the incident response program found no exceptions and concluded FTC's incident response program controls in place 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;
- Performing some or all of 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 FTC's overall maturity level for the contingency planning program is Consistently Implemented. FTC developed, maintained, and integrated system contingency planning[9] through policies, procedures, and strategies. The policies and procedures defined roles and responsibilities which the agency posted to an intranet site to notify all stakeholders. Additionally, FTC allocated people, processes, and technology in a risk-based manner to effectively implement system

[9] [redacted]

contingency planning activities. FTC prepared a Business Impact Assessment (BIA) and used the results to guide contingency planning efforts. Moreover, the agency performed a tabletop exercise of its information system contingency planning processes and used the lesson learned to improve the plan.

Although we found areas where FTC can improve its program, our testing found the security controls were operating as intended. We concluded FTC's contingency planning security controls in place were effective.

Observation 6: The FTC BIA was last updated on September 8, 2015, and did not accurately reflect the agency's current systems affecting its business efforts. The assessment included several system-level BIAs integrated with the FTC organization BIA. *NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organization***s** *Revision* states,

> "The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation."

FTC management stated, "simulating recovery exercises and revising the Information System Contingency Plan (ISCP) have been contingency planning priorities." This may decrease the risk of having an outdated BIA, but it is not as effective as a current and accurate BIA. An outdated BIA could result in FTC not being able to effectively identify contingency planning requirements and priorities, including mission essential functions.

Recommendation 6: We recommend FTC consistently review and update its BIA based on its defined frequency to ensure operational impact is appropriately measured and contingency planning can be developed appropriately.

We concluded, consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, FTC's information security program and practices were established and have been maintained for the five Cybersecurity Functions and eight FISMA Metric Domains. Additionally, we found FTC's information security program and practices were effective for the period October 1, 2018, to September 30, 2019, and the overall maturity level of the FTC's information security program was Managed and Measurable.

Scope and Methodology

Scope

The scope of the FISMA audit evaluated the overall information security program and practices of FTC's unclassified systems to determine the effectiveness of such programs and practices for FY 2019. RMA answered the 67 FY 2019 IG FISMA Reporting Metrics' questions. 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.

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

Additionally, this audit reviewed corrective actions taken by the Office of the Chief Information Officer (OCIO) to implement prior OIG audit recommendations.

Methodology

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

We also conducted this audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) (also known as the Yellow Book) issued by the Comptroller General of the United States. Those 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. We obtained evidence that provided a reasonable basis for our findings and conclusions based on our audit objectives.

The overall strategy of our audit considered NIST SP 800-53A, "Guide for Assessing Security Controls in Federal Information Systems and Organizations," NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," and the FISMA guidance from Council of the Inspectors General on Integrity and Efficiency (CIGIE), OMB, and DHS. Our testing procedures were developed from NIST SP 800-53A. We determined the overall maturity level of each of the eight domains by a simple majority of the competent scores of the maturity level of each question within the domain, in accordance with the FY 2019 IG FISMA Reporting Metrics V1.3.

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.

Criteria

We focused our FISMA audit approach on Federal information security guidelines developed by NIST, OMB, DHS, and FTC. The following is a listing of the criteria used in the performance of the FY 2019 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 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*

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

- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- 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 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*
- NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*
- NIST SP 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-83, Revision 1, *Guide to Malware 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, *Supply Chain Risk Management Practices for Federal Information Systems, and Organizations*
- NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*

OMB Policy Directives

- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High-Value Asset Program*
- OMB Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections (TIC)*
- OMB Circular A-130, *Managing Information as a Strategic Resource*

Department of Homeland Security

- *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.3 April 9, 201*

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

Federal Trade Commission

[redacted]

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

Appendix A: Acronyms

BIA.....Business Impact Assessment
CIA.....Confidentiality, Integrity, and Availability
CAB .....Continuous Assurance Branch
CDM .....Continuous Diagnostics and Mitigation
CIGIE.....Council of the Inspectors General on Integrity and Efficiency
CIO.....Chief Information Officer
CPO.....Chief Privacy Officer
CIS .....Center for Internet Security
CSIRT .....Computer Security Incident Response Team
DHS.....Department of Homeland Security
ECAB.....Enterprise Change Advisory Board
ERM.....Enterprise Risk Management
FEA .....Federal Enterprise Architecture
FIPS.....Federal Information Processing Standards
FISMA .....Federal Information Security Modernization Act of 2014
FTC .....Federal Trade Commission
FY .....Fiscal Year
GSA.....General Services Administration
GAGAS.....Generally Accepted Government Auditing Standards
GAO.....Government Accountability Office
HVA .....High-Value Asset
IAM.....Identity and Access Management
IG .....Inspector General
ISCM.....Information Security Continuous Monitoring
ISSO.....Information System Security Officer
IT.....Information Technology
MTIPS.....Managed Trusted Internet Protocol Service
NIST.....National Institute of Standards and Technology
OCIO.....Office of the Chief Information Officer
OIG .....Office of Inspector General
OMB .....Office of Management and Budget
PRM .....Performance Reference Model
PII.....Personally Identifiable Information
PIV .....Personal Identity Verification
POA&M.....Plan of Action and Milestones
RMA .....RMA Associates LLC
SCAP.....Security Content Automation Protocol
SP. .....Special Publication
TIC .....Trusted Internet Connections
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 B: Management's Response

Management's response begins on the next page.

UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION

WASHINGTON, D.C. 20580

MEMORANDUM

DATE: January 23, 2020

FROM: **Raghav Vajjhala, Chief Information Officer and Chief Data Officer**

TO: **Andrew Katsaros**, Inspector General

SUBJECT: Management's Response to the RMA's FY2019 Audit Report for Fiscal Year 2019 (Report)

Management has reviewed the RMA Report. The Report assessed the FTC's information security program as "effective" based on:

- Reduction in open Office of the Inspector General (OIG) recommendations proposed by OIG auditors from 5 to 2[1]
- Improvements in Council of the Inspectors General on Integrity and Efficiency (CIGIE) ratings
    - FY19: 4 categories rated "Managed and Measurable" and 1 category rated "Consistently Implemented"
    - FY18: 4 categories rated "Consistently Implemented" and 1 category rated "Defined"

The Report also made six new recommendations for improving the FTC's information security program and practices. Management concurs with these recommendations, which reinforce agency priorities to improve the capture of quantitative and qualitative metrics, manage Plan of Actions and Milestones (POA&Ms), and protect information technology systems using a list of approved applications (whitelisting).

In addition, the Report's results align with other measurements of the FTC's information security program:

- Rating of "Managing Risk" per the FY19 CIO Federal Information Security Management Act (FISMA) metrics from the Office of Management and Budget (OMB)
- 95%+ compliant with Binding Order Directive (BOD) 18-01[2]
- Fully compliant with BOD 19-02[3]

Management appreciates the time and attention OIG devotes to supporting all agency efforts to pursue and maintain "Managed and Measurable" ratings[4] for the FTC's information security program.

---

[1] Baseline of 5 recommendations as reported in FTC OIG Semiannual Report to Congress, September 30, 2019.
[2] DHS BOD 18-01, "*Enhance Email and Web Security.*"
[3] DHS BOD 19-02, "**Vulnerability Remediation Requirements for Internet-Accessible Systems.**"
[4] The FY2019 IG FISMA Reporting Metrics characterize "Managed and Measurable" as "effective."

Recommendation 1

Develop a consistent approval process that includes the designation of management's approval embedded in its procedures, plans, strategies, assessments, profiles and reports.

Responsible Official: Raghav Vajjhala

Management concurs that the recommendation will address the assessed condition, and will submit its Corrective Action Plan within 60 days of receipt of the final report.

The FTC will develop a process to develop management-approved, unsigned IT services policy and procedural documents based upon distribution and communication processes.

Recommendation 2

Implement fully effective policies and procedures related to POA&Ms to ensure all identified security weaknesses are tracked, prioritized, and remediated in a timely manner, including a process to evaluate the adequacy of justifications to ensure the estimated completion date is met and determine the dependencies and completion of milestones that affect the estimated due date.

Responsible Official: Raghav Vajjhala

Management concurs that the recommendation will address the assessed condition, and will submit its Corrective Action Plan within 60 days of receipt of the final report.

The FTC will implement effective policies and procedures related to POA&Ms to ensure that all identified security weaknesses are tracked, prioritized, and remediated in a timely manner, including a process to evaluate the adequacy of justifications to ensure the estimated completion date is met and determine the dependencies and completion of milestones that affect the estimated due date.

Recommendation 3

FTC should enhance its process of performing risk management assessments to determine the respective risk posture of its systems to include the entity-wide performance metrics for measuring the effectiveness of its: 1. Contractor-operated systems and contractor-provided information technology services; 2. Change control activities and ensure that data supporting the metrics is obtained accurately, consistently, and in a reproducible format; 3. Data exfiltration and enhanced network defenses; and 4. Data Breach Response Plan and ensure that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

Responsible Official: Raghav Vajjhala

Management concurs that the recommendation will address the assessed condition, and will submit its Corrective Action Plan within 60 days of receipt of the final report.

The FTC will develop and implement a plan to identify and capture qualitative and quantitative metrics to help assess the performance of IT systems and services. The plan will provide the

opportunity for periodic review, and it will be used as the basis for continuous improvement as well as the provision of artifacts to support the "Managed and Measurable" cybersecurity maturity level across the enterprise.

Recommendation 4

Develop and implement a defined process to [redacted] and employ automated mechanisms such as application whitelisting and network management tools to [redacted]

Responsible Official: Raghav Vajjhala

Management concurs that the recommendation will address the assessed condition, and will submit its Corrective Action Plan within 60 days of receipt of the final report.

The FTC will implement an application whitelisting solution and implement a Network Access Control (NAC) solution.

Recommendation 5

Implement automated mechanisms to [redacted] and perform segregation of duties and least privilege reviews.

Responsible Official: Raghav Vajjhala

Management concurs that the recommendation will address the assessed condition, and will submit its Corrective Action Plan within 60 days of receipt of the final report.

The FTC will implement automated [redacted]

Recommendation 6

Consistently review and update Business Impact Assessment (BIA) based on its defined frequency to ensure operational impact is appropriately measured and contingency planning can be developed appropriately.

Responsible Official: Raghav Vajjhala

Management concurs that the recommendation will address the assessed condition, and will submit its Corrective Action Plan within 60 days of receipt of the final report.

The FTC will conduct a new BIA based on a defined frequency in accordance with FTC policy.

Appendix C: FY 2019 IG FISMA Reporting Metrics

The FY 2019 FISMA Reporting Metrics begin on the next page.