Federal Trade Commission
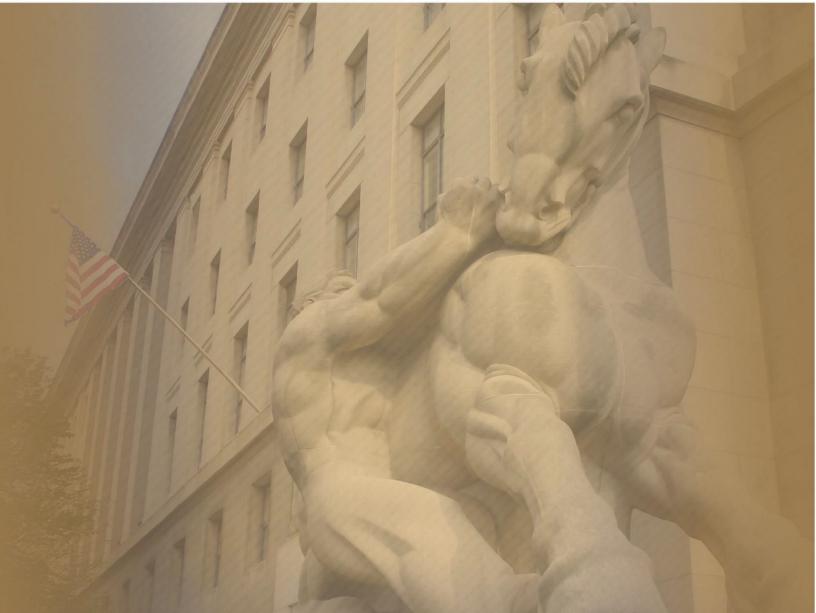# Office of Inspector General

Independent Evaluation of Information Security Program and Practices For Fiscal Year 2018

OIG Report No. OIG 19-02   February 28, 2019

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

Office of Inspector General

February 28, 2019

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 2018 Independent Evaluation 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 FTC's Information Security Program and Practices for Fiscal Year (FY) 2018. The Office of Inspector General (OIG) contracted with TACG, LLC to conduct this independent evaluation.

The objective of the evaluation was to assess the effectiveness of the Federal Trade Commission's (FTC) information security and privacy programs at September 30, 2018. Through analyses of FTC policies, procedures, supporting systems, and other products, the contractor assessed the level of maturity of the FTC's information security and privacy programs and its compliance with the FISMA statute, using guidance from the Office of Management and Budget (OMB), Department of Homeland Security (DHS), and the National Institute of Standards and Technology.

TACG, LLC is responsible for the evaluation and the conclusions expressed in this report. In connection with the contract, the OIG monitored the contractor's work and progress and reviewed the report and relevant supporting documentation.

Using the maturity model developed by the Council of the Inspectors General on Integrity and Efficiency, TACG, LLC assessed four of the model's five functional areas at Level 3 (Consistently Implemented) and one at Level 2 (Defined). DHS has established Level 4 (Managed and

FINAL REPORT – REDACTED FOR PUBLIC RELEASE

Measurable) as the effective level for federal program maturity. As a result, TACG, LLC identified five recommendations to assist the FTC in achieving a future Level 4 rating in the five functional areas.

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 five recommendations.

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 Oversight and Government 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 will provide a copy of its reports to the Comptroller General of the United States.

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

If you have any questions or concerns regarding this report, please contact me at (202) 326-3527, or by email at akatsaros@ftc.gov.

FISCAL YEAR 2018
FEDERAL TRADE COMMISSION
INDEPENDENT EVALUATION
OF THE
FTC'S INFORMATION SECURITY PROGRAM AND
PRACTICES

CONDUCTED UNDER THE
FEDERAL INFORMATION
SECURITY MODERNIZATION ACT OF 2014

Submitted to:
THE FEDERAL TRADE COMMISSION
OFFICE OF INSPECTOR GENERAL
600 Pennsylvania Avenue, N.W.
Washington, DC 20580
ATTN:
Inspector General

February 28, 2019
Submitted by:

TACG, LLC
Contract Number: 29FTC116C0050

EXECUTIVE SUMMARY

The Federal Information Modernization Act of 2014 (FISMA), Public Law 113–283, requires an annual independent evaluation of the effectiveness of agency information security programs. TACG, LLC, under contract with the Office of Inspector General, conducted the FY 2018 evaluation of the Federal Trade Commission's information security and privacy programs and identified the following deficiencies:

- The FTC methodology for identifying and managing risk is not supported by an enterprise architecture with an embedded security architecture. The FTC should develop and maintain these architectures to facilitate development of the systems it needs to support its mission with appropriate, cost-effective security controls.

- The FTC has systems and system components that are not categorized and that do not have associated security control baselines. FTC should develop security baselines for its information systems and components, conduct system-level risk assessments, and maintain appropriate security artifacts, including authorizations to operate or use.

- The FTC has not fully defined or completed the implementation of its ███████████ ████████████████████ tool to support its governance and security programs. The FTC should complete its implementation per prior year action plans to provide a centralized, enterprise-wide view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.

- The FTC has not yet fully applied its configuration baselines. It should complete these baselines for all FTC information systems and components.

- Although the FTC has a documented information security continuous monitoring strategy, it has not been fully implemented. The FTC should implement a fully functional program in accordance with security control monitoring practices identified in related policies and procedures.

LIST OF ACRONYMS	
Acronym	**Definition**
ATO	Authorization to Operate / Approval to Operate
ATU	Authorization to Use
CFO	Chief Financial Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
███████	████████████████████████
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
ERM	Enterprise Risk Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014 (Previously Federal Information Security Management Act of 2002)
FTC	Federal Trade Commission
GAO	Government Accountability Office
GSS	General Support System
IG	Inspector General
IRM	Information Resources Management
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones (also POAM)
RMA	Risk Management Assessment
SAOP	Senior Agency Official for Privacy
SSP	System Security Plan

TABLE OF CONTENTS

List of Embedded Exhibits

1. INTRODUCTION/BACKGROUND

The Federal Trade Commission (FTC) is a federal agency with a unique dual mission to protect consumers and promote competition. The FTC –

- protects consumers by stopping unfair, deceptive or fraudulent practices in the marketplace, and
- promotes competition by enforcing antitrust laws and helping to keep our marketplace open and free.

FTC consumer protection and competition promotion activities result in the collection, retention, and use of large volumes of sensitive information such as Personally Identifiable Information (PII); competition-sensitive information; intra-agency and interagency reports; and internal memoranda, correspondence, workpapers, and records compiled for law enforcement purposes. The FTC information technology (IT) environment consists of a networked central computing facility that provides information resources for primary mission support to all FTC offices. The FTC augments its central facility with information system support provided through other federal agencies (e.g., Department of Interior, General Services Administration) and commercial contractors. The FTC also promotes a telework environment for FTC staff and contractors.

In 2014, the Congress passed and the President signed the Federal Information Modernization Act (FISMA), Public Law 113–283. FISMA requires an annual independent evaluation of the effectiveness of agency information security programs. These evaluations are conducted by Inspectors General (IG) appointed under the Inspector General Act of 1978, as amended, or by an independent external auditor, as determined by the Inspector General of the agency. The annual evaluations cover work performed during the fiscal year and program status at September 30. The independent assessment includes testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems, and an assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

Fiscal Year 2018 Independent Evaluation

TACG, LLC, under contract with the OIG, conducted the FY 2018 evaluation of FTC information security and privacy programs using a maturity model adopted by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). Data collection was conducted from May 15, 2018 through August 31, 2018. We worked with the FTC to clarify data inconsistencies and information gaps as necessary in developing our FISMA report.

The objective of the FISMA evaluation was to assess the effectiveness and status of the FTC Information Security and Privacy Programs as of September 30, 2018, as required under FISMA. Accordingly, the FY 2018 IG FISMA metrics defined requirements to be addressed in this

evaluation.[1] The FY 2018 IG FISMA Reporting Metrics were developed as a collaborative effort amongst the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and CIGIE, in consultation with the Federal Chief Information Officer (CIO) Council.

CyberScope Metrics within the FISMA Independent Evaluation

DHS issues reporting guidance, maintains the CyberScope reporting system, and supports OMB's analysis of CyberScope reporting. The DHS FISMA evaluation process also integrates metrics and questions directed at agency CIOs and Senior Agency Officials for Privacy (SAOP). The annual independent FISMA evaluation assesses the maturity of agency information security and privacy programs using a CIGIE maturity model (CyberScope Metrics) and a written report (FISMA Report) with content and format determined by the agency Inspector General.

The DHS OIG CyberScope Metrics allow assessment of agency information security and privacy program maturity on a 5-level scale: Level 1 – Ad Hoc; Level 2 – Defined; Level 3 – Consistently Implemented; Level 4 – Managed and Measurable; and Level 5 – Optimized. The CyberScope metrics (questions) plus the maturity level definitions constitute the criteria to assess the agency information system and privacy program maturity. The use of standardized metrics allows measurement of program maturity changes across fiscal years.

The model collects metrics that demonstrate whether agency security and privacy programs are evolving toward an environment where program practices and controls are defined, repeatable, measured, and continuously monitored and improved.[2] DHS established Level 4 (Managed and Measurable) as the effective level for federal program maturity.

---

[1] *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (Version 1.0.1, May 24, 2018).
[2] "Defined" means that a program is formally documented to ensure consistent application.

Exhibit 1: CyberScope Metric Scoring, FYs 2018 - 2017

Cybersecurity Framework	FY 2018 Assessment		FY 2017 Assessment	
	CIO Rating	OIG Rating	CIO Rating	OIG Rating
Overall	At Risk	Not Effective	At Risk	Effective
Identify	Managing Risk	Consistently Implemented	At Risk	Defined
Protect	At Risk	Consistently Implemented	At Risk	Consistently Implemented
Detect	At Risk	Defined	Managing Risk	Defined
Respond	Managing Risk	Consistently Implemented	At Risk	Defined
Recover	Managing Risk	Consistently Implemented	At Risk	Defined

The FTC has increased the level of resources that it devotes to information security over the last three fiscal years. The CyberScope metrics and the evaluation, however, show that information security program progress will be dependent on staff retention, the development of formal practices, and improved planning and governance.

2. METHODOLOGY

TACG, LLC conducted this evaluation using the CIGIE maturity model as required by the DHS. Our data collection extended from May 15, 2018 through August 31, 2018. We worked with the FTC to clarify data inconsistencies and information gaps as necessary in developing our FISMA report.

We conducted our FTC FISMA evaluation as two separate but interrelated and complementary assessments that are contained in a single, consolidated report:

- First, we assessed the maturity of the FTC information security and privacy programs. This entailed an evaluation of the capability of the FTC programs to address the 67 CIGIE metrics distributed across the five functions/domains defined in the NIST Cybersecurity Framework (see Exhibit 2). Our maturity assessment examined whether information and privacy control processes were appropriately defined, formalized and consistently implemented, measured, and monitored across the agency; and

- Second, we assessed whether in place (current state) program-level security controls effectively protect FTC information assets (data and systems) from intentional or unintentional threats to information asset confidentiality, integrity, and availability. This part of the evaluation used reporting generated by in place program controls for ongoing assessment and continuous monitoring.

The maturity assessment is provided to DHS and OMB through CyberScope, and the consolidated report, the FTC FISMA 2018 Annual Report, is provided in written form to the Congress and the Government Accountability Office (GAO).

Exhibit 2: CIGIE Metrics by NIST Cybersecurity Framework Function

IG Metrics by NIST Cybersecurity Framework Function	
Functions (Domains)	**Number of IG Metrics[3]**
1. Identify (Risk Management)	12
2. Protect	
Protect (Configuration Management)	8
Protect (Identity and Access Management)	9
Protect (Data Protection and Privacy)	5
Protect (Security Training)	6
3. Detect (Information Security Continuous Monitoring)	5
4. Respond (Incident Response)	7
5. Recover (Contingency Planning)	7
General questions	8
Total Metrics	**67**

3. FINDINGS AND RECOMMENDATIONS

3.1 Assessment of the Risk Management Domain

The Risk Management domain is a foundational element of the CIGIE process maturity assessment model and is contained within the Cybersecurity Identify Function. The Risk Management domain contains twelve of the maturity model metrics, nine of which were assessed as Consistently Implemented (Level 3) and three of which were assessed as Defined (Level 2).

The remainder of this section provides the findings and recommendations for the Risk Management domain.

3.1.1 Finding 1 – Disciplined and Structured Methodology for Managing Risk (CyberScope Question 6)

FISMA Metric and Criteria: To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (NIST SP 800-39; FEA Framework; NIST SP 800-53: PL-8, SA-3, SA-8, SA-9, SA12, and PM-9; NIST SP 800- 161; DHS Binding Operational Directive 17-01)?

Condition: The FTC has not completed an enterprise architecture with embedded information security architecture.

---

[3] The CIGIE metrics include a general question for each of the domains.

The absence of an embedded information security architecture limits the FTC's capability to plan information security control environments that cover all applicable risks. The security architecture helps ensure control measures support FTC business processes and are mutually supportive. For example, security architectures show system and system components and interconnections and interfaces with consideration for security issues. Architectures also show how system and system component controls are layered/overlapped to eliminate single points of failure and ensure a security incident requires failure of multiple controls. The information security architecture should provide a structure for the FTC risk management program.

Recommendation 1

Develop and maintain an information security architecture with embedded information security plans.

3.1.2 Finding 2 – System-Level Risk Assessments (CyberScope Question 9)

FISMA Metric and Criteria: To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing (i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework, (ii) internal and external asset vulnerabilities, including through vulnerability scanning, (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and (iv) security controls to mitigate system level risks (NIST SP 800-37; NIST SP 800-39; NIST SP 800-53: PL-2 and RA-1; NIST SP 800-30; CSF:ID.RA-1 – 6)?

Condition: The FTC has not fully implemented its policies and procedures for conducting system level risk assessments. FTC system risk assessment policies and procedures do not provide for use of a common vulnerability scoring system (or equivalent) framework.

The FTC has systems and system components that are not categorized as either low, moderate, or high, in accordance with requirements contained in Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*. Some of these systems and components also do not have associated security control baselines. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. These information systems and system components include non-digital systems, systems embedded within the General Support System (GSS), social media sites and other applications. FTC systems without baselines also do not have the associated security artifacts that document security implementations and tests to baseline requirements.

Recommendation 2

Implement policies and procedures for conducting system-level risk assessments and maintain appropriate security artifacts, including authorizations to operate or use.

3.1.3 Finding 3 – Centralized, Enterprise-Wide (Portfolio) View of Risks (CyberScope Question 12)

FISMA Metric and Criteria: To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?

Condition: The FTC selected the ██ product as its governance, risk management and compliance tool.[4] The FTC has not fully defined or completed its implementation of ████████.

Not all FTC information systems or components have formal security baselines that can be used to ensure systems have appropriate controls that can be monitored and tested. The FTC has not consistently implemented a manual or automated solution that provides a centralized, enterprise wide view of risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. Not all potential risks are integrated into the risk management solution. The FTC is continuing to implement ████████ as its tool to manage its information systems inventory and security accreditation process as recommended in prior IG evaluations. The plan of action included: reviewing and updating System Security Plans (SSP) to comply with NIST; entering SSP information into ████████; documenting a risk management framework strategy (incorporating governance, risk and compliance tool); and validating that completed SSPs, security control assessments/risk assessments, Plan(s) of Action and Milestones (POA&M)s, and Approval(s) to Operate (ATO) are documented.

The FTC is also implementing ████████ as its tool to support its governance and security programs.

Recommendation 3

> Complete implementation of ████████ per prior year action plans and provide a centralized, enterprise-wide view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.

3.1.4 Finding 4 – Security Control Baselines (CyberScope Question 17)

FISMA Metric and Criteria: To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53: CM-2 and CM-8; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; CSF: ID.DE.CM-7)?

Condition: The FTC has not yet fully applied its configuration baselines.

---

[4] ████████ is a product offered by the Department of Justice.

The primary FTC computing facility is its Headquarters Data Center (Data Center). The Data Center supports a number of FTC mission-focused applications and provides general support for FTC's information processing infrastructure. The FTC augments its central facility with information system support provided through other federal agencies (e.g., Department of Interior, General Services Administration). We identified a number of applications installed on the General Support System at the Data Center that did not have security control baselines.

The FTC is implementing ▮▮▮▮▮ as its tool to support its governance and security programs. The tool is still in the implementation phase and supporting policies and procedures continue in development. As mentioned in Finding 2, the FTC has systems and system components that are not categorized in accordance with FIPS 199 and do not have associated security control baselines. FTC systems without baselines also do not have the associated risk assessments that document security implementations and tests to the baseline requirements.

Recommendation 4

Complete the defined security configuration baselines for all information systems and components.

3.2   Finding 5 – Assessment of the CIGIE Detect Function Area (ISCM) Domain (CyberScope Questions 46, 47, 49, and 50)

NIST defines Information Security Continuous Monitoring (ISCM) as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."[5] The remainder of this section provides the assessment of the FTC ISCM. Questions 46, 47, 49, and 50 deal with performance of the ISCM. The FTC does not have a fully functional ISCM. The metrics are consolidated for presentation.

FISMA Metric and Criteria (Question 46): To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM (NIST SP 800-137: Sections 3.1 and 3.6)?

FISMA Metric and Criteria (Question 47): To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collection of security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53: CA-7) (Note: The overall maturity level should take into consideration the maturity of question 49)?

FISMA Metric and Criteria (Question 49): How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security

---

[5] NIST briefing to the Federal Computer Security Program Manager's Forum, Department of Commerce, August 8, 2013 (https://csrc nist.gov/Presentations/2013/The-Fundamentals-of-Continuous-Monitoring).

controls (NIST SP 800- 137: Section 2.2; NIST SP 800- 53: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)

FISMA Metric and Criteria (Question 50): How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?

Condition: Although the FTC has documented an ISCM strategy, it has not been fully implemented.

In FY 2014, OMB required that agencies develop and maintain an ISCM. Although the FTC developed an ISCM strategy in FY 2014 and revised that strategy in FY 2018, the FTC has not fully implemented an ISCM. Fiscal years 2018 and 2019 are the baseline years in which the FTC will conduct ISCM discovery and analysis activities.

The ISCM is a critical component of information security as defined in OMB, NIST, and DHS requirements. A fully functioning ISCM requires the development of monitoring techniques embedded into agency information security programs. The use of a functioning ISCM is also a prime determinant of the maturity of an agency's information security program. The FTC is presently reengineering and re-hosting its information systems in its transition to a cloud-based architecture. This is the optimum point within the System Development Lifecycle to institute an ISCM.

The FTC has not fully placed diagnostic and monitoring tools for ongoing security assessments into service as defined by the ISCM strategy for analyzing data and reporting issues. The FTC has also not consistently implemented processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls. ISCM policies and procedures have not been consistently implemented for the following areas:

- ongoing assessments and continuous monitoring of security controls;
- collection of security related information required for metrics, assessments, and reporting;
- analyzing ISCM data and reporting findings; and
- reviewing and updating the ISCM strategy.

Recommendation 5

Implement an Information Security Continuous Monitoring (ISCM) program in accordance with security control monitoring practices identified in related policies and procedures.

4. SUMMARY OF OPEN PRIOR YEAR AND FY 2018 RECOMMENDATIONS

At the commencement of the FY 2018 evaluation, the FTC had fourteen recommendations with mitigations in process. At the conclusion of the FY 2018 evaluation, eight recommendations had been closed. Closing these recommendations demonstrates the ongoing commitment that the FTC has made to address conditions in its information security program. The data also show that

the decline in the maturity of its information security program is being addressed, as are more timely corrective actions for recommendations.

The FTC nonetheless faces continuing challenges. Our recommendations for corrective actions focused on improvements that advance the maturity of the FTC's information security programs. In subsequent years, evaluations will change focus to examine the effectiveness of the control processes that the FTC is now implementing. Demonstrating that the program can achieve the Managed and Measurable level will be a significant challenge as the FTC continues to advance into cloud-based computing. Monitoring this program maturity advancement will require the FTC to include security in its information system architectures and embed self-checking controls into its modernized architecture. This will facilitate operation of ISCM controls as part of normal operations, thereby increasing the reliability of measurement metrics, reducing the cost of security monitoring, and ensuring that FTC management has near real-time status of information system security.

Exhibit 3 provides a list of the of prior year recommendations that were open as of September 30, 2018.

Exhibit 3: Prior Year Open Recommendations

Reference	Target Date of Completion[6]	Status at September 30, 2018
FY 2015 – 07 Contractor Systems	FY 2017 Q1	Open – Status In Progress[7]
FY 2016 – 06 Information Systems Continuous Monitoring	FY 2017 Q4	Open – Status In Progress[8]
FY 2017 – 02 ███ Implementation/ ATO Process	FY 2019 Q2	Open – Status In Progress[9]
FY 2017 – 07 IRM Strategy	FY 2019 Q1	Open – Status In Progress[10]
FY 2017 – 08 Configuration Management	FY 2018 Q4	Open – Status In Progress
FY 2017 – 09 Contingency Planning	FY 2019 Q1	Open – Status In Progress

Exhibit 4 provides a summary of the FY 2018 recommendations. Our recommendations address specific deficiencies we identified in the FTC information security program. Three current year recommendations were either repeated or largely resembled and overlapped with prior year recommendations.

---

[6] Target Date of Completion shown is that provided by the FTC.
[7] This recommendation was open at September 30; now consolidated into FY 2018 Recommendation 5.
[8] This recommendation was open at September 30; now consolidated into FY 2018 Recommendation 5.
[9] This recommendation was open at September 30; now consolidated into FY 2018 Recommendation 3.
[10] This recommendation was open at September 30; now consolidated into FY 2018 Recommendation 1.

Exhibit 4: Summary of FY 2018 Recommendations

Reference	Recommendation	Status
Recommendation 1	Develop and maintain an information security architecture with embedded information security plans.	Repeat recommendation (consolidated prior recommendation 2017-07)
Recommendation 2	Implement policies and procedures for conducting system-level risk assessments and maintain appropriate security artifacts, including authorizations to operate or use.	New recommendation
Recommendation 3	Complete implementation of ▮▮▮▮ per prior year action plans and provide a centralized, enterprise-wide view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.	Repeat recommendation (consolidated prior recommendation 2017-02)
Recommendation 4	Complete the defined security configuration baselines for all information systems and components.	New recommendation
Recommendation 5	Implement an Information Security Continuous Monitoring (ISCM) program in accordance with security control monitoring practices identified in related policies and procedures.	Repeat recommendation (consolidated prior recommendations 2015-07 and 2016-06)

APPENDIX A – FY 2018 FISMA INSPECTOR GENERAL CYBERSCOPE SECTION REPORT

APPENDIX A – CONTAINS INFORMATION DESCRIBING FTC INTERNAL
OPERATIONS AND IS REDACTED IN ITS ENTIRETY (formerly pages 11-42)

UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION

WASHINGTON, D.C. 20580

MEMORANDUM

DATE: February 25, 2019

FROM: David Robbins, Executive Director ~~DAVID ROBBINS~~

Digitally signed by DAVID ROBBINS
Date: 2019.02.25 16:57:37 -05'00'

TO: Andrew Katsaros, Inspector General

SUBJECT: Management's Response to TACG's FY2018 Evaluation of the FTC's Information Security Program and Practices ("Report")

Management has reviewed the TACG Report. The Report reflects progress towards a mature information security program at the FTC as indicated by:

- Reduction in open OIG recommendations proposed by TACG from 30 to 7[1]
- Increase in the number of Cybersecurity Framework domains rated as "Consistently Implemented" to 4 out of 5 in FY2018 from 1 out of 5 in FY2017

Management concurs with the Report's five recommendations; they reinforce agency priorities and already-in-place action plans towards improving ███████████ ███████████████ Information Security Architecture (ISA), and Information Security Continuous Monitoring (ISCM).

In addition, the recommendations align with ongoing technology enhancements established successfully in response to DHS Binding Operational Directives (BOD) as reflected in the DHS Cyber Exposure Scorecard:

- BOD 15-01 ("Critical Vulnerability Mitigation")
- BOD 18-01 ("Enhance Email and Web Security")
- BOD 19-01 ("Mitigate DNS Infrastructure Tampering")
- 100% enforcement of encryption on scanned domains
- 100% enforcement of DMARC for email on all scanned domains

Management appreciates OIG's professionalism and dedication in producing this report, as well as OIG's support of the agency's ongoing efforts to achieve a "Managed and Measurable"[2] information security program.

---

[1] Baseline of 30 recommendations as reported in FTC OIG Semiannual Report to Congress, September 30, 2018.

[2] The FY2018 IG FISMA Reporting Metrics characterize "Managed and Measurable" as "effective."

Recommendation 1

Develop and maintain an information security architecture with embedded information security plans.

Responsible Official: Raghav Vajjhala

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

Management will embed, as practical, system level information into the enterprise level information security architecture. In addition, Management shall review and update information system architecture content in system security plans.[3]

Recommendation 2

Implement policies and procedures for conducting system-level risk assessments and maintain appropriate security artifacts, including authorizations to operate or use.

Responsible Official: Raghav Vajjhala

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

Management recognizes that this finding reflects its decision to update its policy portfolio to better align with the agency's increasing adoption of commercial cloud services and government shared services. As part of that update, the agency's Risk Assessment Policy now requires explicit authorizations to operate or use IT systems identified in the system inventory, even if those systems are wholly operated and secured by another agency as a shared service, or social media services that had previously been assessed through a Privacy Impact Assessment. Security control assessments are in process for FY19, which will support the associated risk assessments.[4]

Recommendation 3

Complete implementation of ▮▮▮▮ per prior year action plans and provide a centralized, enterprise-wide view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.

Responsible Official: Raghav Vajjhala

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

---

[3] Management will apply NIST 800-53 revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, PL-8, Information Security Architecture, and PM-7, Enterprise Architecture. In distinguishing the two controls, NIST states that, "[t]he information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture."

[4] As the agency continues to migrate system components to systems operated by cloud providers, Management will continue using FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems.*

The FTC is in the process of implementing ▮▮▮▮ as a centralized, enterprise-wide view of risks associated with each information system.[5]

Recommendation 4

Complete the defined security configuration baselines for all information systems and components.

Responsible Official: Raghav Vajjhala

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

The FTC is in the process of applying configurations documented by the Center for Internet Security (CIS)[6] as standard across all systems, replacing its legacy configurations and documentation. Management determined that based on its intended use of commercial cloud services, CIS would provide more effective updates to configurations relevant to the agency's modernization plans.

Recommendation 5

Implement an Information Security Continuous Monitoring (ISCM) program in accordance with security control monitoring practices identified in related policies and procedures.

Responsible Official: Raghav Vajjhala

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

The FTC recently updated its ISCM strategy (dated July 2018) and Assessment, Authorization and Monitoring Policy (effective December 10, 2018) to reflect NIST requirements related to ISCM.

---

[5] While the current CIGIE methodology encourages use of advanced technology or automation in order for agencies to pursue the rating of "Optimized," it does not cite a specific NIST 800-53 control that requires it at this time.
[6] CIS Benchmarks list configurations for achieving the appropriate level of security hardening across over 140 different hardware, software, and cloud technologies.