OIG Independent Evaluation

of the Federal Trade Commission's Information Security Program and Practices For Fiscal Year 2016

Report No. AR 17-02// March 2017

FINAL REPORT
REDACTED FOR PUBLIC RELEASE

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

Office of Inspector General

March 1, 2017

MEMORANDUM

TO: Maureen K. Ohlhausen, Acting Chairman
Commissioner Terrell McSweeny

FROM: Roslyn A. Mazer
Inspector General

SUBJECT: Transmittal of the Final Report Assessing the Federal Trade Commission's Compliance with the Federal Information Security Management Act for Fiscal Year 2016

As required by the Federal Information Security Modernization Act (FISMA), attached is our annual independent evaluation of the FTC's Information Security Program and Practices for Fiscal Year (FY) 2016.

The FY 2016 evaluation showed that FTC security and privacy programs are robust, demonstrating their ability to protect FTC commission assets while undergoing significant organizational and technological change. The report continues to use the maturity model developed by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). This year, the CIGIE maturity model addressed the Information Security Continuous Monitoring and Incident Response areas. In future years, CIGIE maturity models will be provided for the remaining three of the five functional areas of the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

In previous OIG FISMA and other reporting, we recommended improvements in IT governance, asset management, risk management, training, and contractor management. The FTC expended significant efforts to address our recommendations and improve its governance practices. We assessed that in FY 2016, FTC information security and privacy programs provided adequate and reasonable controls to protect FTC information assets.

We also assessed that the FTC Information Technology and modernization planning and acquisition documents as of September 30, 2016, did not demonstrate the disciplined planning necessary for compliance with Federal Acquisition Regulation (FAR) principles, or with Office of Management and Budget (OMB) and FTC requirements and guidance for such a complex activity; nor did the documents demonstrate a risk-based approach where information security, privacy, and performance risks were identified, considered, and appropriate mitigations planned. These deficiencies did not adversely impact the FTC's current ability to protect FTC information assets, but are indicative of a security environment with decreasing effectiveness.

The key areas for improvement we identified in this review are:

- Information security planning
- Planning and documenting the design and operating procedures for the new FTC information systems inventory
- Conducting and documenting a risk-based approach to support planned technological changes and acquisition methods for the IT Strategy and Transition Plan approved on September 30, 2016
- Completion of the FTC Information Security Continuous Monitoring System in accordance with the Plan originally developed in FY 2014, or a revised plan that accommodates the IT modernization strategy

The report identifies opportunities for improvement and makes eight recommendations. While the recommendations are designed to address multiple issues, four recommendations focus on security monitoring and management; two on risk-based planning; one on acquisition planning; and one on contingency planning. The recommendations are also intended to ensure, through risk-based analyses, that the technological solutions proposed in the IT Strategy and Transition Plan provide security at least equivalent to the security provided by the FTC's in-house systems.

There are 10 open FISMA recommendations from prior years, and 15 from related OIG reporting in the past four years, for a total of 25 open recommendations. In accordance with customary protocols, the OIG will consider consolidating any of the open recommendations based on the Corrective Action Plans management proposes.

Management concurred in the eight recommendations in this year's report and committed to provide action plans to address them, with scheduled completion dates through the fourth Quarter of FY 2018. Excerpts of management's official response are included in Exhibit ES-1, and in their entirety in Appendix B. The OIG's concerns with management's response are included in Appendix C.

The OIG is deferring its assessment of the effectiveness of management's proposed mitigating actions until we have had an opportunity to review the scope, content, milestones, and schedules we anticipate

will be included in the Corrective Action Plans that management agreed to provide the OIG within 60 days. We will also examine the effectiveness of the improvements that address OIG open recommendations as part of the FY 2017 FISMA evaluation.

We appreciate the cooperation from management and staff and acknowledge the commitment of the Office of the Chief Information Officer, Chief Privacy Officer, Office of the Executive Director, and Administrative Services Office, and to ensuring information security and privacy protections at the FTC.

Please do not hesitate to contact me or Mary Harmison if you have any questions or comments.

Cc: Svetlana Gans, Chief of Staff to the Acting Chairman
David Robbins, Executive Director
David Rebich, Chief Financial Officer
David Shonka, Acting General Counsel
Raghav Vajjhala, Chief Information Officer
Katherine Race Brin, Chief Privacy Officer
Patricia Bak, Deputy Executive Director
Monique Fortenberry, Deputy Executive Director
Jeffrey Smith, Assistant Director for Continuous Assurance
Jeanne Bumpus, Director, Office of Congressional Relations

FISCAL YEAR 2016
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 THE INSPECTOR GENERAL
600 Pennsylvania Avenue, N.W.
Washington, DC 20580
ATTN: Roslyn A. Mazer
Inspector General

March 1, 2017

Submitted by:

TACG, LLC
Contract Number: 29FTC116C0050

EXECUTIVE SUMMARY

The Federal Trade Commission (FTC) is an independent agency with a unique dual mission to protect consumers and promote competition. The FTC is dedicated to advancing consumer interests while encouraging innovation and competition. The FTC develops policy and research tools through hearings, workshops, and conferences; collaborates with law enforcement partners across the country and around the world to advance consumer protection and competition missions; and cooperates with international agencies and organizations to protect consumers in the global marketplace.

Under the FTC Act, the FTC guards against unfairness and deception by enforcing companies' privacy promises about how they collect, use, and secure consumers' personal information. Under the Gramm-Leach-Bliley Act, the FTC implements rules concerning financial privacy notices and the administrative, technical and physical safeguarding of personal information, and, in FY 2015, supported the United States-European Union Safe Harbor Framework that provides a process for businesses to transfer personal data from the European Union to the United States in a manner consistent with European Union law. The FTC also protects consumer privacy under the Fair Credit Reporting Act and the Children's Online Privacy Protection Act.

To accomplish its missions, the FTC accumulates significant quantities of data, much of which contain sensitive personal, commercial, or financial information. For example, the FTC collects consumer information in addressing complaints about issues from data security and deceptive advertising to identity theft; by operating the DO NOT CALL registry; and by reviewing proposed mergers and acquisitions pursuant to the Hart-Scott-Rodino Act.

Evaluation Objective

The Federal Information Security Modernization Act of 2014 (FISMA) requires that agency Inspectors General (IG) conduct annual independent evaluations of their agency's information security and privacy environments. The FTC IG contracted with TACG, LLC for the independent evaluation of the Commission's information security and privacy programs for FY 2016.

The primary objective of this year's FISMA evaluation is to assess the status of the FTC information and privacy programs at September 30, 2016, as required under FISMA and the *FY 2016 Inspector General Federal Information Security Modernization Act Reporting Metrics V1*, prepared by the Department of Homeland Security (DHS), Office of Cybersecurity and Communications, Federal Network Resilience and Office of Management and Budget (OMB) Memorandum M-16-03, Fiscal Year 2015-2016 Guidance on Information Security and Privacy Management Requirements. OIG uploaded DHS reporting metrics into CyberScope, the designated FISMA reporting tool by the November 10, 2016, OMB reporting deadline. The FTC FISMA evaluation report is provided to OMB and the appropriate Congressional Oversight Committees by March 1, 2017.

CyberScope Metrics vs OIG FISMA Independent Evaluation

The metrics uploaded into CyberScope (CyberScope metrics) are intended to measure FTC progress in establishing and continuously improving its information security and Privacy programs as defined in a maturity model defined by the DHS and the Council of the Inspectors General on Integrity and Efficiency (CIGIE). While the FY 2016 CyberScope metrics provide useful information, it has limited utility in comparing progress between years until it is fully implemented in FY 2017.

Where CyberScope reporting is intended to measure implementation progress of a particular maturity model, the OIG FISMA report evaluates the status of FTC information security and Privacy programs at September 30, 2016 and the work completed in FY 2016. The FISMA report may include any area covered by the Act to any depth, depending on the discretion of the Inspector General. The FTC FY 2016 FISMA report focused on issues that affect the FTC's capability to protect its information assets and the processes and procedures to continuously monitor and improve its information security and privacy controls.

Both the FISMA and CyberScope reports use the five functional areas (Identify, Protect, Detect, Respond, and Recover) of the National Institute of Standards and Technology (NIST) Cybersecurity Framework as a reporting structure. This approach facilitates analysis of FTC information security and privacy controls. However, since the CyberScope and FISMA reporting use different methodologies with a different frame of reference, and CyberScope reporting is still in transition, direct comparison of CyberScope results with the FISMA results or comparison of CyberScope results between years should include consideration of the differences in methodologies.

Overview of FTC IT Environment

FTC staff are dependent on the use of information technology (IT) to collect, store, and analyze information to conduct their law enforcement efforts; distribute settlements to consumers injured by unfair or deceptive acts or practices; prepare and pursue legal actions against individuals and organizations engaged in unfair or deceptive acts or practices; and examine proposed company merger data for potential antitrust or competition concerns. The FTC also uses its IT systems to perform a variety of administrative functions such as maintaining finance and accounting records, supporting acquisitions, time reporting and payroll, and human capital.

The FTC IT architecture evolved as the primary data center was expanded with local and wide area networking and individual functional applications, as opposed to following a defined enterprise architecture. The data center supports FTC critical, and most sensitive, mission support activities (e.g., discovery and other litigation support activities). The FTC contracts with other federal agencies (e.g., General Services Administration (GSA) and the Department of Interior (DOI)) for functions such as finance and accounting and with commercial sources for functions such as distribution of money recovered for consumers, public access Internet, and wireless communications.

In accordance with NIST guidance, FTC information security and privacy programs are integrated such that policy responsibility is separated between the CIO and the FTC Chief Privacy Officer (CPO), and implementation of security controls is coordinated to ensure privacy controls are appropriately included in all FTC information systems.

On September 30, 2016, the FTC adopted a Strategy and Transition Plan, an aggressive, multi-year strategy to design, acquire, and implement an enterprise architecture that emphasizes use of cloud technologies to expand the services available to its workforce while improving information security and resilience; ensuring compliance with FISMA, the Privacy Act, and other applicable law, policy, standards, and guidelines; and remaining within budget and staffing constraints.

The Strategy and Transition Plan provides reasonable objectives for modernization of FTC IT capabilities. However, to support the modernization effort, the FTC will need to establish enterprise-level security and privacy control baselines, risk management procedures, acquisition plans, and project management practices that ensure delivered modernization components meet FTC needs, can be effectively managed, and are delivered on schedule and within budget.

OIG FY 2016 Independent Evaluation

Supported by TACG, LLC, the OIG conducted the FY 2016 evaluation of FTC information security and privacy programs as required under the FY 2016 Inspector General Federal Information Security Management Act of 2014 Reporting Metrics, Department of Homeland Security, Office of Cybersecurity and Communications, Federal Network Resilience, June 20, 2016.[1] The primary source documents for baseline information security and privacy requirements are OMB Circular A-130, Managing Information as a Strategic Resource, 7/28/2016; and NIST Special Publication (SP) 800-53, Revision 4, 1/22/2015, Security and Privacy Controls for Federal Information Systems and Organizations.

Under DHS guidance, the FISMA evaluation has two reporting components: a metric-based maturity model (CyberScope report) and a written report. The maturity model is used to summarize the maturity and status of agency information security and privacy programs in a consistent manner that is intended to allow comparison across agencies and over time, i.e., objectively showing whether agency security and privacy programs are improving from year to year. While current CyberScope reports support comparison between agencies within each year, comparison between years is not yet available.

The written reports produced as part of the annual FISMA evaluation are specific to an individual agency, i.e., this report provides an evaluation of the FTC information security and privacy environments. The structure and content of the written report is at the discretion of the agency Inspector General. Through this report, the OIG provides recommendations for

[1] DHS may issue changed guidance through the CyberScope website. In such cases, guidance on the website supersedes the published guidance.

advancing the maturity and capability of the FTC information security and privacy programs to cost effectively protect its information assets while concurrently advancing the programs' maturity as reflected in FTC's CyberScope score.

Results of the Evaluation

The OIG determined that the FTC security environment continues to be strong and robust relative to its ability to protect its information assets. OIG did not identify any weaknesses in its FY 2016 evaluation that were specific to the FTC Privacy controls.

CyberScope metrics show that FTC has substantially met the Cross-Agency Priority (CAP) goals established by OMB and DHS for agency information systems. In those areas where FTC has not met CAP goals, there are compensating countermeasures that minimize the risk of information compromise. Our independent assessment of the FTC information security and privacy environments is consistent with the information provided through the CyberScope reporting. However, as also stated in the OIG's FY 2014 and FY 2015 FISMA reports, the FTC's information security privacy programs continue to be stressed, requiring significant manual activity, and with the modernization effort, the stress will be increased, especially during the transition period.

From FY 2013 through FY 2016, the FTC maintained information security and privacy programs to protect its information assets. In its reporting, the OIG recommended improvements in FTC IT governance, asset management, risk management, and contractor management. While the FTC made significant efforts to improve its governance practices, modernization planning and acquisition documents provided as of September 30, 2016, did not demonstrate the disciplined planning necessary for compliance with Federal Acquisition Regulation (FAR) principles, Office of Management and Budget (OMB), and FTC requirements and guidance for such a complex activity; nor did the documents demonstrate a risk-based approach where information security, privacy, and performance risks were considered and appropriate mitigations were evaluated and planned. FTC progress has been hampered by frequent turnover in the position of the Chief Information Officer and the associated disruptions due to reorganizations and changes in management focus. Further, these efforts are hampered by inconsistent adherence to FTC policies and procedures and lack of documentation. For example, the FTC established information security policies and procedures consistent with federal guidance and best practices, but does not consistently follow those policies and procedures. While the FTC has the management discretion to revise or tailor its policies and procedures to meet mission needs and resource constraints, these decisions should be documented and include supporting risk-based rationales.

Assessment of the FTC Information Security and Privacy Programs within the Cybersecurity Framework

The lack of effective documentation of FTC processes and decisions is an underlying problem for weaknesses identified in four of the five Functions of the NIST Cybersecurity Framework

(Identify, Protect, Detect, and Recover). The root cause of the long-term documentation deficiency appears to be reliance on the small size of the agency and the low turnover rate of key staff. At the FTC, there is significant verbal exchange of information that would be communicated in written form in larger organizations. While this may be a reason for deficient documentation, it is a problem that increases costs and risks and must be resolved. Clear documentation of decisions and the rationale for those decisions is critical as the FTC advances its modernization efforts and strives to meet its maturation objectives for its information security and privacy programs.

In this report the OIG assesses the following vulnerabilities, grouped by the five functions listed in the Cybersecurity Framework.

1. **IDENTIFY**

   The Identify Function covers the capability of an organization to identify its information assets; understand the need for and impact of information security and privacy on its business environment; maintain a governance program that ensures that systems are properly planned, acquired, documented, and monitored; and maintain a risk management program where decisions are risk-based and documented. The following are summaries of Identify vulnerabilities addressed in this report:

   - **FTC replaced its comprehensive system inventory, but did so without the planning and validation controls necessary to demonstrate that the new system has the same data elements as the retired system and that existing data was appropriately transferred.** In addition, FTC needs to ensure that system definitions include all components, those for which FTC is directly responsible and those that are acquired under contract.

   - **FTC has not embedded repeatable processes within its risk management program to ensure risks are consistently evaluated and are analyzed for individual projects and for the overall enterprise.** The risk management process should be applied to FTC modernization initiatives.

2. **PROTECT**

   Activities in the Protect Function support the ability to prevent, limit, and contain the impact of a potential cybersecurity event.

   The FTC information security program relies on legacy systems and manual controls to protect its information assets. The Strategy and Transition Plan issued on September 30, 2016, provides reasonable objectives for the modernization effort. However, the plan does not provide sufficient definitive information or risk analyses to demonstrate that the modernization can be successfully completed within the planned timeframe.

   - **The modernization effort is a substantial effort that will be difficult to manage and monitor.** FTC should plan the modernization as interrelated segments, under an Enterprise Architecture, that can be individually planned, monitored, and implemented. As recommended by both the Office of

Management and Budget and the Government Accountability Office, logical segmentation of complex acquisitions with specific performance criteria increases the potential for successful program performance.

3. **DETECT**

The Detect Function enables timely discovery of cybersecurity events. The cornerstone of the Detect Function is an effective Information Security Continuous Monitoring (ISCM) system.

- **FTC developed an ISCM strategy and plan, but it was not implemented.** FTC acquired tools that can be used to establish an ISCM, but there is no plan for combining these tools into an integrated system. The FTC also has not identified how continuous monitoring requirements are applied to individual system controls to monitor control effectiveness.

- **FTC modified its Plan of Action and Milestones (POA&M) process so that it is no longer the consolidated listing of vulnerabilities and mitigating actions intended by OMB.** FTC needs to revise its POA&M process so that it includes all the data elements required by OMB and aligns with associated Corrective Action Plans and budgets.

4. **RECOVER**

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event.

From FY 2013 through FY2015 the OIG included recommendations in its FISMA reporting to establish and test a viable disaster recovery plan. Disaster planning is an integral part. In each instance, the FTC provided an action plan to establish a disaster recovery capability, but the plans were never implemented.

- **FTC does not have a contingency plan that includes a disaster recovery plan for its HQ data center.** The lack of contingency planning resulted in a three-day data center outage in October 2016 affecting the entire FTC work force that should have been a minor disruption.

Key areas for FTC improvement

This section identifies the areas where improvement of FTC practices will have the greatest impact on reducing FTC security risk. While this section identifies the areas for improvement, FTC management will need to prioritize these areas for improvement based on its planning and resource allocation priorities. The OIG lists eight recommendations for improvement in Exhibit ES-1 that address the following key areas for improvement:

- **FTC security planning continues to be weak.**
  Effective, security planning is institutionalized within the organization. Deferring security planning until the functionality of a system or system component is on order or out-for-bid typically results in increased security risks or systems that require

substantial modification to meet specified security control requirements. Effective security planning, described by NIST, operates at multiple levels and continues throughout the life of a system, from initial conception to disposition when retired.

A number of laws, federal regulations, policies, and guidance (e.g., FISMA, Federal Acquisition Regulation, OMB Circular A-130, and NIST guidelines) identify planning as a requirement for establishing secure information environments. While these requirements cover all aspects of virtually any information system, they also place on management the responsibility to tailor those requirements. Security requirements and their implementation must be appropriately sized to the mission/business need, and the size, complexity, and dollar value of the systems.

While the FTC made significant efforts to improve its governance practices, modernization planning and acquisition documents provided as of September 30, 2016 do not demonstrate the disciplined planning necessary for compliance with Federal Acquisition Regulation (FAR), OMB, and FTC requirements and guidance for such a complex activity; nor do the documents demonstrate a risk-based approach where information security, privacy, and performance risks were considered and appropriate mitigations evaluated. While the FTC has the management discretion to tailor its policies and procedures to meet mission needs and resource constraints, such tailoring needs to be documented with supporting risk-based rationales. Governance oversight will then need to include monitoring activities to ensure that decisions are documented and supported by risk-based criteria.

- **Documentation of and planning for the CSAM-based inventory is deficient.** The FTC initiated a project to replace its legacy system inventory system with a new system that would use CSAM and SharePoint components. Documentation provided to the OIG describing the system replacement was deficient: there is no description of the complete system that shows the system coverage (i.e., what systems will be included), data elements that will be maintained, how data contained in disparate databases are consolidated to provide enterprise level inventory reporting, and assignment of responsibility for ensuring inventory data is current. Also, no plan was provided that showed how data from the legacy system was controlled and validated when migrated to the CSAM-based system.
- **While the IT Strategy and Transition Plan approved on September 30, 2016. discussed risks as something that will need to be addressed, there was no risk analysis that supported the technological approach or acquisition method.** As with any significant change, implementation of the Strategy and Transition Plan has associated risks: risk that change will introduce new vulnerabilities without associated mitigating factors, solutions proposed will not provide anticipated benefits, or information assets are compromised during the transition. Effective planning and FTC senior management and governance oversight will be critical to ensure that the FTC is able to complete its modernization efforts while maintaining its ability to protect its information assets.

- **While the FTC has had an Information Security Continuous Monitoring Strategy and Plan in place for several years, it has not implemented that plan and has not provided a revised plan.**
  OMB requires that all agencies implement an Information Security Continuous Monitoring (ISCM) Plan. FTC developed and approved an ISCM Strategy and an ISCM Plan. While the FTC has obtained a number of components that could support an ISCM system, it has not executed its ISCM plan nor provided an alternative plan.
- **The FTC Plan of Action and Milestones (POA&M) does not adhere to Office of Management and Budget (OMB) requirements and NIST Guidance.**
  OMB requirements and NIST guidance requires that agencies maintain a POA&M for its information security programs and individual systems. OMB identifies the POA&M as a primary management tool for tracking the progress of corrective actions to mitigate identified vulnerabilities. The POA&M content is specified by OMB to ensure they contain the information necessary to support agency risk mitigation, resource allocation, budgeting, and capital planning. The current FTC POA&M does not collect the information necessary to serve as the consolidated planning tool required by OMB or NIST guidance.
- **Documents presenting the FTC's disaster recovery plan do not provide the basic supporting information required under National Institute of Standards and Technology (NIST) contingency planning guidance.**
  The OIG has repeated its recommendation that the FTC should implement a viable disaster recovery plan for its headquarters data center. The FTC has provided several plans over the past three years, but none was implemented or presented viable solutions. The current FY 2016 disaster plan also does not provide a viable plan. Further, the plan is based on incorrect planning assumptions and does not include a risk analysis supporting the cloud-based approach presented as a future alternative.

Recommendations for Improvement

Exhibit ES-1 lists eight recommendations to improve the FTC's information security program. The recommendations focus on improving the FTC's capability to identify the information assets that need to be protected and cost-effectively implement a control environment where successful performance may be defined, measured, monitored, and continuously improved.

Column 5 of Exhibit ES-1 presents an extract of management's official response to each OIG recommendation. Management's official response is included in this report as Appendix B.

The OIG cannot at this time provide detailed assessments of management's proposed actions to address the OIG's FY 2016 recommendations. The OIG will provide specific comments after we receive Management's Action Plans and have an opportunity to evaluate the milestones, performance measures, and plan alignment and timing of the Action Plans with the FTC's IT Strategy and Transition Plan.

The OIG's observations about management's official response are included in this report as Appendix C.

Exhibit ES-1: Listing of Recommendations for Improving FTC Information Security and Privacy Programs

Reference	Paragraph	Recommendation	Potential Impact	Management Action Plan[2]
FY 2016 – 01 - ID.AM	6.1.3.1	*To ensure FTC has an inventory that contains the information required to describe its information systems and data holdings, FTC should document its inventory practices and validate associated databases.* The FTC should document its system inventory management system and validate the system, database, and management procedures, at least on an annual basis, as a trusted FTC ISCM component under configuration control.	Moderate	Management will develop an action plan within 60 days, with overall completion expected no later than FY18 Q4.
FY 2016 – 02 - ID.AM	6.1.3.2	*To ensure controls are properly documented and responsibility for control maintenance and testing is identified, FTC should review its information system boundaries and control inheritance practices.* The FTC should complete its evaluation of its system boundaries as it completes its CSAM implementation. FTC should eliminate use of the Minor Application designation and document leveraged/common controls in accordance with NIST RMF guidance and ensure that all FTC systems are covered by an FTC ATO, either specific to the system or under a related system.	Moderate	Management will develop an action plan within 60 days, with overall completion expected no later than FY18 Q4.

[2] Management comments are extracted from the Management's Response included as Appendix B.

Exhibit ES-1: Listing of Recommendations for Improving FTC Information Security and Privacy Programs

Reference	Paragraph	Recommendation	Potential Impact	Management Action Plan[2]
FY 2016 – 03 - ID.GV, ID.RA	6.1.3.3	*To ensure the rationale for decisions are transparent and auditable, the FTC should document decisions made and the associated risk-based supporting rationale.* The FTC should implement a formal procedure for documenting risk-based decisions as part of the FTC risk management program.	Moderate	Management will develop an action plan within 60 days, with overall completion expected no later than FY 18 Q2.
FY 2016 – 04 - ID.RA	6.1.3.4	*To ensure that the FTC understands the risks associated with its modernization initiative, FTC should conduct risk analyses from both the individual information system and organization levels (Tier1 and Tier 3).* The FTC should implement a formal risk management program that addresses the requirements of OMB Circulars A-123 and A-130 and the guidance contained in NIST Special Publications 800-30, 800-37, and 800-39. The FTC should conduct risk analyses for its IT Modernization Initiative.	Moderate	Management shall address this recommendation through an overall action plan to address A-123and A-130 requirements within the next 60 days as set forth under recommendation 3 above and expects that this plan shall also address and ideally consolidate or close action plans in response to the two recommendations (ER 16 – 03, 2 and 5) found in the OIG IT Governance evaluation. Management will develop an action plan within 60 days, with overall completion expected no later than FY 18 Q2.
FY 2016 – 05 – PR.IP, PR.MA	6.2.3.1	*To ensure IT investments are appropriately planned, funded, executed, and monitored, the FTC should divide its modernization initiatives into segments that provide useful products in relatively short timeframes within a defined Enterprise Architecture.*	Moderate	Management shall address this recommendation through an overall action plan to address A-130 requirements for Planning and Budgeting and IT Investment Management within the next 60 days. This plan shall include determination of enterprise architecture requirements sufficient to cost effectively meet the mission

Exhibit ES-1: Listing of Recommendations for Improving FTC Information Security and Privacy Programs

Reference	Paragraph	Recommendation	Potential Impact	Management Action Plan[2]
		The FTC should structure modernization activities for acquiring major IT investments as useful segments that can be independently planned, acquired, and monitored.		requirements of the FTC. The plan shall likely generate recurring reviews and updates every year to the IT Strategy and Transition Plan in accordance with A-130. Management will develop an action plan within 60 days, with a first iteration of updates expected no later than FY18 Q1.
FY 2016 – 06 – DE.CM	6.3.3.1	*To ensure it has the capability to monitor the health of its security and privacy programs, the FTC should implement a fully compliant ISCM.* The FTC should implement a fully compliant ISCM as described in its ISCM Plan in FY 2013 and its ISCM Strategy, dated November 2014.	Moderate	Management will develop an action plan within 60 days, with overall completion expected no later than FY18 Q1.
FY 2016 – 07 – DE.CM	6.3.3.2	*To ensure that the POA&M is the consolidated tracking tool required by OMB, FTC should revise and update its POA&M procedures.* The FTC should revise its POA&M process and content to ensure it meets OMB information requirements (e.g., all security weaknesses found, and in need of remediation, during any assessment done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments) and can be an effective, authoritative,	Moderate	Management will develop an action plan within 60 days, with overall completion expected no later than FY 18 Q2.

Exhibit ES-1: Listing of Recommendations for Improving FTC Information Security and Privacy Programs

Reference	Paragraph	Recommendation	Potential Impact	Management Action Plan[2]
		agency-wide management tool.		
FY 2016 – 08 – RC.RP	6.5.3.1	*To minimize the potential for and disruption from both short and long-term outages, the FTC should institute a continuing contingency planning capability.* The FTC should develop viable contingency plans for the HQ data center and hosted applications. Plans should be tested to ensure viability and ensure staff are trained to execute them. Contingency plans should clearly define actions to be performed and individuals responsible for plan activation and other critical decisions should be identified.	Moderate	Management shall address this recommendation through an overall action plan within the next 60 days. This action plan shall also address and ideally consolidate or close action plans in response to prior OIG recommendations. Management will develop an action plan within 60 days, with overall completion expected no later than FY 18 Q4.

Table of Contents

Executive Summary ii

List of Acronyms xvii

1. Background 1

1.1. Criticality of IT Security for the FTC Mission 1

1.2. FTC's Legacy IT Architecture and New IT Strategic Plan 2

1.3. Organization of the Office of the Chief Information Officer 3

2. Scope 8

3. Objectives 11

4. Methodology 12

4.1 Relation of CyberScope Maturity Model to OIG FISMA Evaluation 13

4.2 Analysis Domains 14

4.3 CyberScope Report Considerations 16

4.4 Assessment of Privacy Controls 16

5. General Overview 18

6. Recommendations and Impact Assessments 23

6.1. Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities 24

6.1.1 CyberScope Metrics 24

6.1.2 OIG Assessment of the Identify Function 25

6.1.3 Recommendations 26

6.1.3.1 Complete the System Inventory 26

6.1.3.2 Review application classification to ensure conformity with NIST guidance 29

6.1.3.3 Document Risk-Based Decisions 31

6.1.3.4 Develop Risk Analyses for its IT Modernization Initiative 34

6.2 Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services 36

6.2.1 CyberScope Metrics 36

6.2.2 OIG Assessment of the Protect Function 37

6.2.3 Recommendations 40

6.2.3.1 Segment Modernization Activities Into Useful Segments 41
6.3 Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event 43
6.3.1 CyberScope Metrics 43
6.3.2 OIG Assessment of the Detect Function 43
6.3.3 Recommendations 44
6.3.3.1 Implement an ISCM 44
6.3.3.2 Revise the Plan of Action and Milestones Process 45
6.4 Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event 46
6.4.1 CyberScope Metrics 46
6.4.2 Respond Function Assessment 47
6.4.3 Recommendations 47
6.5 Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services impaired due to a cybersecurity event ... 47
6.5.1 CyberScope Metrics 47
6.5.2 OIG Assessment of Recover Function 47
6.5.3 Recommendations 50
6.5.3.1 Develop Contingency Plans for the FTC HQ data center 50
7. Status of Prior Year Recommendations 52
8. Summary of Findings and Recommendations 62
APPENDIX A – FTC OIG FY 2016 FISMA CYBERSCOPE RESPONSE A-1
APPENDIX B – MANAGEMENT'S RESPONSE B-1
APPENDIX C - OIG OBSERVATIONS ABOUT MANAGEMENT'S RESPONSE C-1

List of Exhibits

Exhibit ES-1: Listing of Recommendations for Improving FTC Information Security and Privacy Programs x
Exhibit 1: OCIO Organization at September 30, 2016 3
Exhibit 2: OCIO Organization Responsibilities at September 30, 2016 4
Exhibit 3: FTC Ten IT Strategic Initiatives 7
Exhibit 4: NIST Security Identifiers and Family Names 8
Exhibit 5: Policy Guidance Significantly Affecting Security and Privacy Programs 9
Exhibit 6: Cybersecurity Framework Functional Taxonomy 14
Exhibit 7: Metric Analysis Domains 15
Exhibit 8: Status of Cross-Agency Priority (CAP) Goal 18
Exhibit 9: FTC Reported Incidents FY 2016 19
Exhibit 10: OIG CyberScope Summary 20
Exhibit 11: FTC CyberScope Scoring for Identify Function 25
Exhibit 12: ITGB Strategy Concerns on 60% Version (4/26/2016) 32
Exhibit 13: FTC CyberScope Scoring for Protect Function 37
Exhibit 14: Detect CyberScope Score 43
Exhibit 15: Respond CyberScope Score 46
Exhibit 16: Recover CyberScope Score 47
Exhibit 17: Previous OIG FISMA Recommendations That Remain Open 52
Exhibit 18: Status of FY 2013 OIG Recommendations 53
Exhibit 19: Status of FY 2013 OIG Recommendations 54
Exhibit 20: Status of FY 2015 OIG Recommendations 57
Exhibit 21: Summary of FY 2016 Recommendations 63

List of Acronyms

Acronym	Definition
ATO	Authorization to Operate
BCA	Business Case Analysis (analogous to BIA)
BIA	Business Impact Analysis (analogous to BCA)
C&A	Certification and Accreditation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information Security Officer (analogous to IAM)
COR	Contracting Officer Representative
COTS	Commercial-off-the-shelf
CPO	Chief Privacy Officer
CUI	Controlled, Unclassified Information
DRP	Disaster Recovery Plan
DHS	Department of Homeland Security
FedRAMP	Federal Risk and Authorization Management Program
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
IAB	Information Assurance Branch
IAM	Information Assurance Manager (analogous to CISO)
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ITBC	IT Business Council
ITC	IT Council
ITGB	IT Governance Board
ITMO	Information Technology Management Office (now OCIO)
NARA	National Archives and Records Administration
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
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones (also POAM)
PSC	Privacy Steering Committee
SAOP	Senior Agency Official for Privacy
SIEM	Security Information and Event Management
SORN	System of Records Notice
TSD	Task Solution Document

1. BACKGROUND

The Federal Trade Commission (FTC) is an independent agency with a unique dual mission to protect consumers and promote competition. The FTC is dedicated to advancing consumer interests while encouraging innovation and competition. The FTC develops policy, rules, and research tools through hearings, workshops, and conferences; collaborates with law enforcement partners across the country and around the world to advance its consumer protection and competition missions; and cooperates with international agencies and organizations to protect consumers in the global marketplace.

The FTC protects consumers by stopping unfair, deceptive, or fraudulent practices in the marketplace; conducts investigations and brings enforcement actions against companies and people that violate the law; develops rules to ensure a vibrant marketplace; and educates consumers and businesses about their rights and responsibilities.

The FTC promotes competition by enforcing antitrust laws in a range of sectors of critical importance to American consumers, including health care, technology, energy, consumer goods and services, and manufacturing. The FTC challenges anticompetitive mergers and business practices that could harm consumers with higher prices, lower quality, fewer choices, or reduced rates of innovation. Also, the FTC returns money recovered through FTC legal actions to consumers that were harmed by unfair or illegal actions. For example, in FY 2016, FTC returned more than $830,000 to Spanish-speaking individuals who lost money in a targeted, bogus telemarketing scheme, and $3.7 million to consumers who lost money in a pyramid scheme.

To accomplish its missions, the FTC accumulates significant quantities of data, much of which contain sensitive personal, commercial, or financial information. For example, the FTC collects substantial volumes of consumer information in addressing consumer complaints about issues from data security and deceptive advertising to identity theft; operating the DO NOT CALL registry; and reviewing proposed mergers and acquisitions pursuant to the Hart-Scott-Rodino Act.

1.1. CRITICALITY OF IT SECURITY FOR THE FTC MISSION

FTC staff are dependent upon the use of information technology (IT) to collect, store, and analyze information to conduct their law enforcement efforts; distribute settlements to consumers injured by unfair or deceptive acts or practices; prepare and pursue legal actions against individuals and organizations engaged in unfair or deceptive acts or practices; and examine proposed merger data for potential antitrust or competition concerns. The FTC also uses its IT systems to perform a variety of administrative functions such as maintaining financial and accounting records, supporting acquisitions, time reporting and payroll, and human capital

operations. In FY 2016, the FTC spent approximately $48.7 million for IT expenditures, representing 15.9% of the FTC's FY 2016 $ 306.9 million appropriation.[3]

1.2. FTC'S LEGACY IT ARCHITECTURE AND NEW IT STRATEGIC PLAN

Over the past three years, the FTC IT architecture has continued to evolve with the addition of individual functional applications as opposed to following a defined enterprise architecture. Under this structure, the FTC established a data center to support the FTC infrastructure (e.g., local and wide area networking and general office automation activities) and its critical, and most sensitive, mission support activities (e.g., discovery and other litigation support activities). The FTC contracts with other federal agencies, including the General Services Administration (GSA) and the Department of Interior (DOI), for functions such as finance, accounting, and acquisition support, and with commercial sources for functions such as distribution of redress recovered for consumers, public access Internet, and wireless communications. Support applications operate in independent IT environments with minimal connectivity to the FTC IT architecture. For administrative functions, the FTC connects with and shares information with agencies such as the DOI and the Office of Personnel Management (OPM). The FTC also works with other agencies such as the Department of Justice (DOJ) and the Department of Commerce (DOC) in jointly pursuing litigation and law enforcement actions. In some cases, this necessitates sharing of mission-related data and may require interconnection to the FTC network. All interconnections and information sharing arrangements require specific FTC authorization enforced through administrative and technical controls.

The FTC's IT environment is critically dependent on the support provided by its contractor workforce for operation of its IT infrastructure and for technical expertise and support for contracted applications. The FTC protects its information assets through control environments subject to the Federal Information Security Modernization Act (FISMA), the Privacy Act, the FTC Act, and related policies, guidelines, standards, and guidelines issued by the Office of Management and Budget (OMB), Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST), General Services Administration (GSA), and National Archives and Records Administration (NARA).[4] The FTC may shift responsibility for preparing work products to its contractors, but it retains responsibility under FISMA and other laws for ensuring its information assets are appropriately protected, regardless of contract arrangement. FTC information assets may also be subject to additional access and usage restrictions under specific legislation, such as information provided to the FTC under the Hart-Scott-Rodino Act.

On September 30, 2016 – the end date for the period of review covered by the OIG's FY 2016 FISMA evaluation – the FTC adopted a Strategy and Transition Plan, an aggressive, multi-year strategy to design and implement an enterprise architecture that emphasizes use of cloud

[3] OCIO staff provided the figure for IT expenditures.

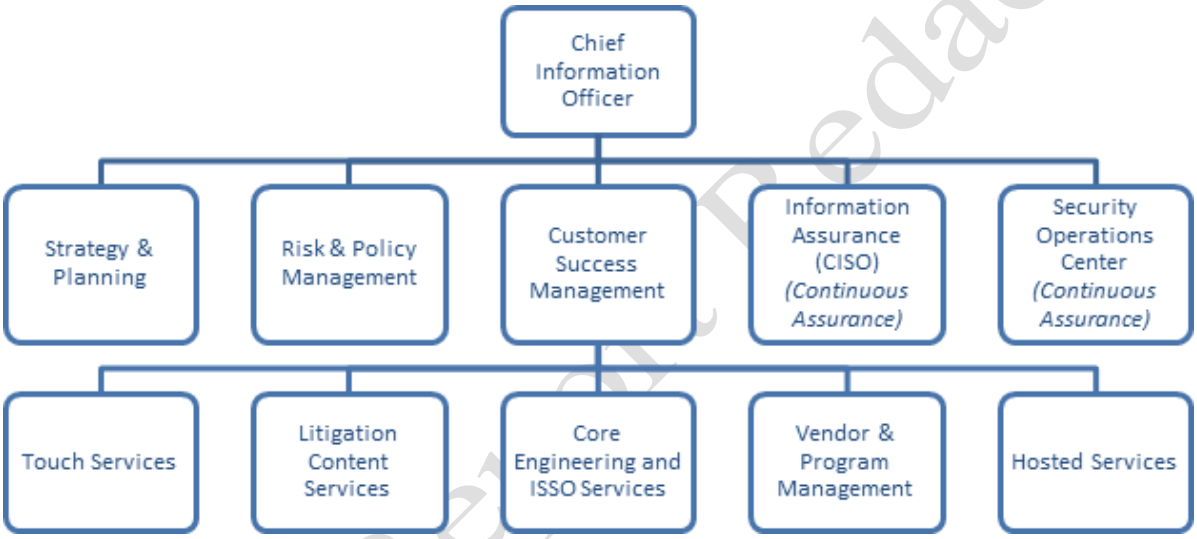
[4] The Federal Information Security Modernization Act of 2014 (FISMA), 5 U.S.C. Section 552a (the Privacy Act), and FTC Act, 15 U.S.C. §§ 41-58, as amended, replaced the Federal Information Security Management Act of 2002 (FISMA)).

technologies to expand the services available to its workforce while improving information security and resilience and ensuring compliance with FISMA, the Privacy Act, and other applicable law, policy, standards, and guidelines while remaining within budget and staffing constraints.[5]

1.3. ORGANIZATION OF THE OFFICE OF THE CHIEF INFORMATION OFFICER

Exhibit 1 provides the organizational structure for the Office of the Chief Information Officer (OCIO) at September 30, 2016. The responsibilities associated with the new structure are shown in Exhibit 2. Reorganization of the OCIO with a customer focus is a key component of the FTC's Strategy and Transition Plan.

Exhibit 1: OCIO Organization at September 30, 2016



While the OCIO has had multiple reorganizations in the past decade, this was the first strategy that seeks to align OCIO staffing and organizational responsibilities with customer business needs and IT support capabilities. Exhibit 2 displays the duties of the current OCIO organization shown in Exhibit 1.

[5] See Federal Trade Commission, *Strategy and Transition Plan, Security and Technology Services (FY 2016 – FY 2019).*

Exhibit 2: OCIO Organization Responsibilities at September 30, 2016

Organization	Team Duties	Desired Results
Chief Information Security Officer Continuous Assurance	• FISMA categorizations, control implementation, authorizations and assessments • POA&M management • Government-wide security reporting • Annual security training • Change management process	• Risk properly documented and reported to the commission • Commission risk tolerance defined • Continuous authorization of FISMA systems • ISSO design controls based on risk tolerance • SOC monitors ongoing threat status and suggests mitigations • Monitor progress on CAP security goals
Security Operations Center Continuous Assurance	• CIRT incidents • Internal investigations • Threat management • Security policies • US CERT Reporting	• Compliance with technical and security standards • Alert management on deviations from optimal technical and security operations • Continuous monitoring • Continuous authorization
Risk & Policy Management Conducts continuous review and analysis of business practices, with the goal of improving decision making	• Governance processes and procedures • Governance meeting management • Ensure IT decisions are made in partnership with business stakeholders	• Increased transparency agency-wide of performance gains, challenges, and actions underway to correct deficiencies • Policies and procedures are assessed for effectiveness and impact on the budget, performance, and operations services
Strategy & Planning Ensures information technology investments make meaningful and measurable impacts on the FTC mission	• Budget and financial management • Strategic planning • Data and performance analysis • Discover new technologies and monitor IT trends • Overall enterprise architecture accountability and central artifact repository	• IT strategy and transition plan aligns with FTC mission and strategic plan, and drive creation and management of IT budgets • Acquisition strategy and HR recruitment aligned with skills required to execute IT strategy and transition plan • Representation of FTC services and performance reflects industry best practices to inform evaluation of FTC capabilities • Customers welcome changes prescribed in the IT Strategy

Exhibit 2: OCIO Organization Responsibilities at September 30, 2016

Organization	Team Duties	Desired Results
Core Engineering & ISSO Services Provides the foundation required to deliver robust, scalable, and integrated IT services	• Maintenance and management of data centers • Server environment management • Network management • Configuration management • Manage test lab environment • Desktop engineering • Patch management • Storage management • Remote access management • PIV implementation • DR procedures • Technical architecture development	• Proactively provision systems and services which align with agency needs and client expectations • Balance availability, security, functionality and ease of use to provide cost effective services • Creation of an architecture library to contain baseline configurations, as well as justifications for deviations
Litigation Content Services Focuses on customer needs related to Litigation processing	• Maintenance and management of enterprise litigation applications • Technical consultant and system owner for Litigation Support System environment	• Become a valued litigation solution provider for the customer • Prioritize and resolve issues • Understand the work being performed and customer needs • Find litigation support products that meet customer needs (in-house or in the cloud)
Touch Services Focuses on putting the "human touch" at the core of IT service delivery, shifting the way we communicate, deliver and support IT services	• Helpdesk management • Asset management • Intranet web page development and maintenance • Remote litigation team support • Enterprise content management • Event planning • Audio, video, and photo support • Graphic support • Print services • Web applications • SES support • Calling card program	• Improved communication with customers • Improved level of customer service and personalized support • Tailor services to better meet the needs of the customer • Increased customer satisfaction

Exhibit 2: OCIO Organization Responsibilities at September 30, 2016

Organization	Team Duties	Desired Results
Hosted Services Determines appropriate service offering to meet current and future customer needs	• Application management • Secure environment support • Technical POC for externally hosted agency systems • COTS application support • Database support • Ticket escalation/Desktop support • Enterprise software management	• Delivers modern, scalable, and secure environments to the FTC • Services that do not need to be hosted inside the FTC can be moved to an external provider for recognized cost savings, added reliability, enhanced security, or with greater methods of access to the data
Vendor & Program Management Enables the organization to improve performance through increased value from vendors	• Contract management • Contract renewals • Invoicing • Project management office • 508 compliance	• IT resources and work efforts are transparent, integrated, and traceable to clear business outcomes and user benefits • Establish clear and effective service levels for all contracted services • Vendors actively contribute ideas to improve efficiency and accelerate innovation • All IT service contracts are migrated to the BPA(s)

As shown in Exhibit 3, the OCIO Strategy and Transition Plan, at the conceptual level, identifies ten IT strategic initiatives to address the three FTC strategic goals.

Exhibit 3: FTC Ten IT Strategic Initiatives

Summary of Strategic Initiatives	Goal 1: Protect Consumers	Goal 2: Maintain Competition	Goal 3: Advance Performance
BE Application Modernization (Business Specific)	Powerful data analysis tools and a scalable infrastructure to enable FTC economists and investigators in researching the impact of fraud and deceptive business practices on the economy and consumers	Powerful data analysis tools and a scalable infrastructure to enable FTC economists and investigators to determine and predict consumer harm from anticompetitive business practices, despite increasingly complex data sets	Pay as go model for scalable infrastructure service being more responsive to immediate needs, and built-in Disaster Recovery (DR)
Legal Review Tool Replacement (Business Specific)	Reliable, easy-to-use, and integrated tools and systems to support the entire spectrum of the electronic discovery reference model and improve FTC's ability to investigate and take action against deceptive and unfair business practices		
Custom Application Reengineering (Business Specific)	Agile cloud-based application development platform to reengineer FTC's portfolio of custom applications, increasing the ability of FTC staff to quickly develop new applications, respond to changing business requirements and processes, and new regulatory procedures		
NextGen Devices and Remote Access (General Purpose)	Robust end-user technology devices, such as laptops and smartphones, and high-quality remote access services for a more mobile workforce, providing access to FTC resources anywhere and anytime		
Enterprise Content Management (ECM) (General Purpose)	Consolidated and standardized ECM solution, leveraging cloud services to enhance availability and access that supports compliant eDiscovery, legal hold, data loss prevention, version control, records management, and built-in DR		
FTC.gov Rehosting (PaaS) (General Purpose)	FTC resources redirected to maintain content not technology, disseminating information to consumers and maintain competition		Platform as a Service (PaaS) increases security, content delivery and access while reducing costs of patching, infrastructure maintenance and duplicative services; built-in DR
Office Productivity Tools and Unified Communications (UC) (General Purpose)	Cloud based office productivity tools and UC increase user access and number of tools available for use for work and collaborate. Workforce empowered to create new innovative work processes to meet changing needs.		Cloud services reduce operational costs associated with patching and maintaining infrastructure while providing latest applications and DR
Enabling Strategic Initiatives			
Modernize Network (Infrastructure)	Modernized network increase connectivity, uses latest technology, streamlines security controls while improving efficiency, access and availability allowing FTC staff to better perform the mission		
Improve IT Resources (IT & Customer Success)	Hiring FTEs based on Clinger-Cohen competencies and obtaining contract resources via flexible vehicles will allow FTC to accomplish the strategic initiatives		
User Training & Change Mgmt. (IT & Customer Success)	Provides all FTC staff the ability to fully understand and utilize the available technologies		

2. SCOPE

The Office of Inspector General (OIG) conducted an independent assessment of the FTC information security and privacy programs as required under the Federal Information Security Modernization Act of 2014 (FISMA). Our assessment focused on the status of FTC information security and privacy programs at September 30, 2016, and work performed in maintaining these programs from October 1, 2015, through September 30, 2016. The structure of the assessment was provided by the DHS in the *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*. The primary source for applicable technical controls was NIST Special Publication (SP) 800-53, *Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations* (January 22, 2015). SP 800-53 also includes consideration for all laws, policy, regulation, and guidance originating from a variety of sources including Congress (e.g., FISMA, Privacy Act, Cybersecurity Act); OMB (e.g., Circular A-130, Circular A-123, and OMB Memorandum 14-04); NIST (e.g., Special Publications, Federal Information Processing Standards); General Services Administration (e.g., Federal Acquisition Regulation); National Archives and Records Administration; Office of Personnel Management; and General Accountability Office.

NIST SP 800-53 provides for the establishment of a security environment with security controls in eighteen groups or "families" and eight families of privacy controls as shown in Exhibit 4 below.

Exhibit 4: NIST Security Identifiers and Family Names

INFORMATION SECURITY AND PRIVACY CONTROLS			
ID	**FAMILY**	**ID**	**FAMILY**
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management
ID	**PRIVACY CONTROL FAMILIES**		
AP	Authority and Purpose		
AR	Accountability, Audit, and Risk Management		
DI	Data Quality and Integrity		
DM	Data Minimization and Retention		
IP	Individual Participation and Redress		

Exhibit 4: NIST Security Identifiers and Family Names

INFORMATION SECURITY AND PRIVACY CONTROLS			
ID	**FAMILY**	**ID**	**FAMILY**
SE	Security		
TR	Transparency		
UL	Use Limitation		

NIST SP 800-53 guidance is continuously reviewed and vetted to ensure that information control measures are clearly described and presented so that agencies can select the controls that best fit their needs. It also is periodically upgraded (a multi-year effort) and revised to accommodate changes in law and guidance, and changes in vulnerabilities and threats. We reviewed current activity of responsible agencies to identify changes that impact FISMA evaluation criteria, depending on their scope and implementation date, and relevant best practices that will enhance the FTC's security efforts.

OMB and NIST are continuously issuing new guidance that revises existing guidance. The guidance listed in Exhibit 5 will significantly affect FTC security and privacy programs and were considered in this evaluation.

Exhibit 5: Policy Guidance Significantly Affecting Security and Privacy Programs

Item	Date[6]	Source	Impact
Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control	7/15/2016	OMB	• Agencies should implement an Enterprise Risk Management (ERM) framework. • Agencies should follow a risk-based approach to integrate and coordinate internal controls across their organization. • Agencies should maintain an annual documented risk profile, a prioritized inventory of its most significant risks identified through the annual risk assessment process. • Agencies should work cooperatively with Offices of Inspectors General and GAO to resolve audit findings.
Circular A-130, Managing Information as a Strategic Resource	7/28/2016	OMB	Revised OMB basic policy document for information security, privacy, and IT acquisition. Placed into policy best practices (e.g., governance and ISCM) that were instituted as federal requirements under OMB, NIST, and other

[6] The date shown is the issue date for the guidance. The effective date for agency requirements depends on the implementation guidance they contain.

Exhibit 5: Policy Guidance Significantly Affecting Security and Privacy Programs

Item	Date[6]	Source	Impact
			governmentwide guidance since the last revision to the Circular.
NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations	June 2015	NIST	Provides guidelines that apply to organizations supporting the FTC. FTC is to use these guidelines in assessing the adequacy of contractor information controls.
NIST Special Publication 800-181, DRAFT NICE Cybersecurity Workforce Framework (NCWF): National Initiative for Cybersecurity Education	11/02/2016	NIST	Provides a common language to categorize and describe cybersecurity work. Provides guidance for use in developing competency requirements for information resources staff, including program managers, information security, privacy, and IT leadership positions, and develop and maintain a current workforce planning process (see Circular A-130).
32 CFR Part 2002, Controlled Unclassified Information	9/4/2016	NARA	Provides the final rule for labeling and handling of controlled unclassified information.
Federal Cybersecurity Workforce Assessment Act (contained in FY 2016 Budget Act, Public Law No. 114-113)	12/18/2015	2016 Budget Act	Requires agencies use the NCWF to identify and manage their cybersecurity workforce. Baseline assessment required by December 2016.

3. OBJECTIVES

The Federal Information Security Modernization Act of 2014 (FISMA) requires that agency Inspectors General conduct annual independent assessments of their agency's information security and privacy environments. The FTC OIG contracted with TACG, LLC for the independent evaluation of the Commission's information security and privacy programs for FY 2016.

The primary objective of the evaluation is to assess the status of the FTC information and privacy programs at September 30, 2016, as required under FISMA and associated guidance (*FY 2016 Inspector General Federal Information Security Modernization Act Reporting Metrics V1*) prepared by the DHS, Office of Cybersecurity and Communications, Federal Network Resilience and OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Information Security and Privacy Management Requirements*).[7] The FTC FISMA agency report is due to OMB and the appropriate Congressional oversight committees by March 1, 2017.

The OIG evaluation has four interrelated secondary objectives:

- Assess the capability of the FTC's in place controls to provide adequate security and privacy protection for agency information assets (hardware, software, and data); [8]

- Assess capability of in place inventory, change management, documentation, and governance procedures to provide FTC managers with the status of the FTC security and privacy environment;

- Assess the capability of in place monitoring tools and procedures to continuously improve the effectiveness of security and privacy controls as protection requirements change and new threats are addressed; and

- Identify areas for improvement.

  In accordance with DHS and OMB direction, the OIG reported weaknesses or areas for improvement to the OCIO when identified to facilitate timely mitigation. Items reported during the conduct of the evaluation may or may not be separately identified in the FISMA reporting metrics or this report, depending upon their impact on the overall FTC security environment.

[7] DHS annual reporting guidance may be modified through online CyberScope documentation. The online guidance takes precedence over published guidance. The OIG submitted its FY 2016 FISMA reporting metrics into CyberScope, the designated FISMA reporting tool, on November 10, 2016, meeting the OMB reporting deadline.

[8] "Adequate security" means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls. (OMB Circular A-130, *Managing Information as a Strategic Resource (*July 28, 2016)).

4. Methodology

Maintaining effective information security is an ongoing process. Threats and vulnerabilities are continually changing as are the control measures agencies use to protect their information assets and the government seeks to establish public/private partnerships to ensure that effective security is consistent and embedded in all critical infrastructures. Government-wide policy and guidance evolve to address changing requirements and risks and ensure that the best, reasonable security practices are applied across all federal agencies and federal interest systems. Accordingly, the standards for evaluating information security also evolve to match requirements, address new threats and technologies, and implement new techniques for monitoring information security and privacy effectiveness.

The OIG's FY 2016 evaluation is a continuation of an improvement process initiated with the OIG's FY 2015 FISMA evaluation. The DHS guidance for FY 2016 is contained in the *FY 2016 Inspector General Federal Information Security Management Act of 2014 Reporting Metrics*, Department of Homeland Security, Office of Cybersecurity and Communications, Federal Network Resilience (June 20, 2016). The primary source documents for baseline information security and privacy requirements are OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016); and NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (January 22, 2015).

The FISMA evaluation has two reporting components: a metric-based, maturity model (CyberScope report) and a written evaluation report. The maturity model is used to provide a tool through which agency information security and privacy programs may be summarized and compared across the federal government. FISMA evaluation reports are specific to an individual agency, i.e., this report provides an evaluation of the FTC information security and privacy environments. The structure and content of the FISMA evaluation report is at the discretion of the Inspector General.

With the FY 2015 FISMA evaluation, OMB and DHS, working through the Joint Continuous Monitoring Working Group (JCMWG) and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed a maturity model for the first of the 10 "domains" assessed in FY 2015: an *Information Security Continuous Monitoring (ISCM) Maturity Model*. The CIGIE maturity model provides a consistent approach for evaluating the control maturity and effectiveness of agency continuous monitoring programs that can be applied and compared across federal agencies. For FY 2016, FISMA evaluation procedures applied the maturity model approach to two domains: the ISCM and Incident Response domains.

The purpose of the CIGIE Maturity Models is to (1) summarize the status of agencies' information security programs and their maturity on a 5-level scale, (2) provide transparency to agency CIOs, top management officials, and other interested readers of FISMA evaluation

reports about agency progress and additional improvements for the information security program, and (3) help ensure consistency across agencies in the Inspectors General annual FISMA reviews. "Within the maturity model context, all things being equal, DHS determined that Level 4, Managed and Measurable, represents an effective information security program."[9]

DHS guidance continues to emphasize that the OIG's independent security evaluation is a cooperative effort to strengthen agency information security and privacy programs. Guidance for OIG independent evaluations is intended to "empower" OIGs to analyze "how Agencies are evaluating risk and prioritizing security issues."[10] This focus allows OIGs to evaluate whether agencies have in place the framework and supporting processes necessary to establish and maintain risk-based, cost effective information security and privacy programs that are sufficiently flexible to make real-time adjustments to address new threats and vulnerabilities. Importantly, with a risk-based approach, the OIG analysis changes from a strict compliance audit to a performance-based approach, wherein the OIG evaluates *an agency's capability to effectively make and document reasonable, risk-based decisions*. Accordingly, our evaluation focused on the tools and techniques the FTC uses to develop, maintain, and safeguard its information assets. The scope of analysis included governance, workforce management, and management and planning of the information environment as well as day-to-day operations. Further, the OIG evaluated policy, procedures, and operations metrics against the CIGIE maturity model. The objective of this approach is to determine whether the FTC has fully implemented risk-based security and privacy approaches that protect information assets and evaluate the maturity of that approach (i.e., whether FTC has controls and monitoring tools in place that provide FTC with the information necessary to determine whether those controls are effective).

4.1 Relation of CyberScope Maturity Model to OIG FISMA Evaluation

It is important to note that the DHS CyberScope Maturity Model and associated metrics and the FISMA evaluation have different purposes and use different criteria. Where the FISMA evaluation seeks to determine program status *at a point-in-time*, the Maturity Model is intended to determine whether agency information security and privacy programs, as defined by the Maturity Model, *are maturing* (i.e., are program requirements defined; are policies and procedures in place; are policies and procedures consistently implemented; is there a metric-based approach to monitor and measure program performance; and is there an ongoing program to analyze changing threats and requirements and continuously improve the program). For example, the Maturity Model scores the maturity of agency Contingency Planning with one primary question ("Has the organization established an enterprise-wide business continuity/disaster recovery program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines"), with 10 subordinate questions.

[9] FY 2016 Inspector General Federal Information Security Modernization Act Reporting Metrics, V1.0 (June 20, 2016), page 5.
[10] FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.2 (June 19, 2015), page 4.

The 10 subordinate questions identify specific components of Contingency Planning to be addressed under the Maturity Model. For FY 2016, 0 questions address level 1 concerns; 2 questions address level 2; 6 questions address level 3; 3 questions address level 4, and 0 questions address level 5. When completed, the questions asked for each level will show whether an agency's process has successfully met the metrics established for that level of maturity. Comparison of scores over time will show whether the agency's programs are maturing.

Concurrent analysis of the FISMA and CyberScope reporting thus shows the status of the information security and privacy programs (FISMA reporting) and if the programs are maturing (CyberScope reporting).

4.2 ANALYSIS DOMAINS

In prior years, the OIG FISMA evaluation focused on 10 "security domains." For FY 2016, OMB and DHS elected to incorporate the five-function security structure contained in the NIST *Framework for Improving Critical Infrastructure Cybersecurity: Identify, Protect, Detect, Respond, and Recover* (Cybersecurity Framework) shown in Exhibit 6.[11]

Exhibit 6: Cybersecurity Framework Functional Taxonomy

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

The 10 security domains used in prior years are "metric domains" in the five-function structure Cybersecurity Framework, as shown in Exhibit 7.

[11] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

Exhibit 7: Metric Analysis Domains

Cybersecurity Framework Security Functions	FY 2016 IG FISMA Metric Domains
Identify	Risk Management and Contractor Systems
Protect	Configuration Management, Identity and Access Management, and Security and Privacy Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

The Cybersecurity Framework also uses Framework Implementation Tiers ("Tiers") to provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices.

The DHS aligned the four Cybersecurity Framework Tiers to the five maturity model Levels (Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized) by combining the Ad Hoc and Defined Levels into the Cybersecurity Framework Tier 1. The evaluation report presents the five Cybersecurity Framework functions: Identify, Protect, Detect, Respond, and Recover. We discuss each of the five functions showing the applicable CyberScope score, followed by an analysis of the Cybersecurity Framework function and how it is affected by findings related to the Metric Domains. We label recommendations for improvement using the Cybersecurity Framework/Category designations. This affords insight into how effective implementation of these recommendations will increase the FTC's CyberScope scores and, importantly, strengthen the effectiveness of the FTC's information security and privacy programs.

OIG FISMA evaluations are conducted on an annual basis. It is not uncommon for similar weaknesses to be identified within the same Cybersecurity Function in different years. The performance data on which our analyses are based differ from year-to-year, as do security requirements, threats, and the status of agency information security and privacy programs. For example, recommendations in this report are labeled using the Cybersecurity Framework. Recommendations from prior years are labeled using the analysis structure appropriate for the year in which they were provided.

Recommendations from FISMA reports or other OIG reports may be consolidated when the FTC management action plan shows that a single mitigation addresses multiple recommendations.

4.3 CyberScope Report Considerations

The metric-based, maturity model CyberScope report is intended to support cross-agency and longitudinal (over time) analyses. Cross-agency analyses are possible for FY 2016 because all agencies are using the same metrics and scoring processes. However, longitudinal analyses were not and should not be performed because the data elements collected and the collection approach do not provide the year-to-year consistency to support such analysis. The OIG favors the use of an analytical approach that allows cross-agency, cross-domain, and longitudinal data comparisons. The Maturity Model is moving in that direction. However, until the Maturity Model is implemented for all Cybersecurity Framework functions and scoring methodologies are consistent between years, analysis should include consideration for differences in CyberScope methodologies.

The OIG assessed that the FTC security and privacy program effectiveness is substantially the same from FY 2013 through FY 2016. FTC provides effective security for its information and privacy assets. However, planning deficiencies and staff turnover have inhibited information security improvement and program maturation.

4.4 Assessment of Privacy Controls

The requirements for safeguarding information subject to the Privacy Act are addressed in the eighteen control families contained in the body of NIST SP 800-53 r4 and eight control families specific to Privacy Requirements. Recommendations that affect the primary eighteen control families are presented as information security issues. Recommendations, if any, regarding the eight Privacy control families (Appendix J of SP 800-53 r4) are reported as Privacy issues to align with the NIST SP 800-53 family structure. Our evaluation procedures include a number of activities that are specific to assessment of the controls contained in Appendix J, including:

- Review of the FISMA Senior Agency Official for Privacy (SAOP) FISMA response submitted through CyberScope.

- Review of FTC Privacy Impact Assessments (PIAs) (see SP 800-53 r4 (AR-2)) policies to identify any policy changes. Reviewed all PIAs to evaluate content and coverage. As PIAs are published documents, this information is obtained from the FTC website. This also allows matching of PIAs with the system inventory to ensure that all system PIAs are published as required.

- Review the FTC System of Records Notices (SORNs) to determine if there were any changes that needed to be addressed. Ensured that FTC systems were covered by SORNs as required.

- Discussion with the FTC Office of the Chief Privacy Officer (CPO), OCIO, and Office of General Counsel (OGC) activities related to the new NARA requirements for identifying and managing Controlled Unclassified Information (CUI) as well as Personally

Identifiable Information (PII). This included review and discussion of comments FTC provided to NARA regarding CUI requirements.

The legal issues associated with CUI requirements are outside the scope of a FISMA assessment, except to the extent that they impose a new information security requirement. Our concerns in this area related to the capability of the new inventory system to appropriately identify and monitor the location and size of FTC CUI and PII holdings.

- Reviewed policies and procedures to incorporate appropriate security and privacy protection in contractor systems. For this assessment, we also requested information describing procedures for monitoring contractor performance including sanctions for poor performance and incentives for high performance -- emphasis on information security and privacy controls.

- Reviewed Authorizations to Operate (ATOs) to ensure that the CPO is afforded an opportunity to review ATOs for potential privacy issues.

- Reviewed FTC privacy activities such as information security and privacy awareness training, efforts to reduce PII holdings, and activities to increase the level of awareness of PII issues among FTC and FTC contractor staff.

5. General Overview

As we have concluded in the last three FISMA evaluations, the FTC security environment continues to be strong and robust relative to its ability to protect its information. In our FY 2016 evaluation we did not identify any weaknesses in controls specific to FTC Privacy controls.

Exhibit 8 shows that FTC has "substantially met" the Cross-Agency Priority (CAP) goals established by OMB and DHS for agency information systems. In those areas where the FTC has not met CAP goals, there are compensating countermeasures:

- Hardware and Asset Management – the FTC is a small agency where its primary hardware and software assets are contained within its Headquarters facility. Access to the facility is limited to the FTC workforce and authorized visitors. While its ability to maintain its hardware and software inventories does not meet CAP goals, the capability to compromise FTC's hardware and software suite is reduced by physical access controls and restrictions on the adding or removing of hardware and software assets;

Exhibit 8: Status of Cross-Agency Priority (CAP) Goal

CAP Goal Metrics	2015 % Goal	2015 FTC Met (M)	2016 % Goal	2016 FTC Met (M)
Hardware Asset Management	0		32	
Software Asset Management	0		26	
Vulnerability Management	100	M	100	M
Secure Configuration Management	100	M	100	M
Unprivileged User PIV Implementation	0		7	
Privileged User PIV Implementation	0		100	M
Anti-Phishing Defense	4		4	
Malware Defense	2		3	M
Other Defenses	4	M	3	M

- Personal Identity Verification (PIV) Implementation for unprivileged users – As we have reported since 2013, the FTC's implementation of the PIV requirement is deficient. However, access from within the facility requires authorization enforced by PIV access

control. Access from outside an FTC facility is remote and requires two-factor identification access control. Public facing applications are generally hosted at off-site contractor facilities. These compensating controls limit the potential for unauthorized access to the FTC and inward facing applications; and

- Anti-Phishing – In addition to inclusion in annual awareness training, and newly instituted phishing testing, the FTC has ongoing awareness activities that address the phishing threat. In place spam controls also reduce the potential for a successful phishing attack. Our review of FTC trouble and incident reports during the period of our review showed a low number of incidents affecting the FTC infrastructure (see Exhibit 9).

Exhibit 9: FTC Reported Incidents FY 2016

US-CERT Incidents by Threat Vectors* Total Number of Incidents: 73	
Attrition	0
Email	25
External/ Removable Media	0
Impersonation	2
Improper Usage	9
Loss or Theft of Equipment	1
Web	1
Other	31
Multiple Threat Vectors	3

*US-CERT data may exhibit some differences from other incident data sources due to changes in reporting guidance in FY 2016.

Our assessment of the effectiveness of the FTC information security and privacy environments is consistent with the information the OIG provided through the CyberScope reporting in November 2016. FTC information security and privacy controls focus on protecting information assets and using isolation of its most sensitive information assets as a primary control technique. The FTC also is an early adopter of cybersecurity services offered through the DHS and GSA,

leveraging government-wide cybersecurity support capabilities to improve its information security and privacy programs at reduced costs.

Within the CIGIE maturity model, the OIG determined that the FTC information security and privacy programs are between Levels 2 and 3. As shown in Exhibit 10, three of the five have matured to Level 3, but not beyond. This is indicative of a process where application of security controls is inconsistent and often dependent on an individual's action, i.e., control usage varies within the FTC and there is no effective process for monitoring quality performance. This assessment aligns with prior OIG FISMA assessments for FY 2013 through FY 2015. DHS established Level 4 under the CyberScope maturity model structure as an effective program, "all things being equal." Enhancing FTC information security from its current Level 3 to Level 4 under the CIGIE maturity model will require significant effort, primarily in planning and performance monitoring and evaluation**.**

Exhibit 10: OIG CyberScope Summary

Function	Scored Assessment
Identify	Level 3: Continuously Implemented
Protect	Level 3: Continuously Implemented
Detect	Level 2: Defined
Respond	Level 3: Continuously Implemented
Recover	Level 2: Defined

The OIG criteria for an effective information security and privacy program focus both on process maturity and in place controls to protect FTC data from loss or compromise. Specifically, OIG assessment criteria (in accordance with NIST guidelines) require that data protection controls should be in place to protect FTC information assets, regardless of their placement within or omission from the Maturity Model. For example, our criteria assesses all the controls in place to protect FTC assets, including compensating countermeasures that may use manual procedures where automated procedures are not in place. Under our criteria, if the compensating controls provided adequate protection, the information security program would be rated as effective, even though it would be scored lower under the maturity model because the maturity model emphasizes automated control. Similarly, although reputation risk is not specifically identified in the CyberScope metrics, our criteria for effective loss prevention include loss of reputation as a factor because the FTC has a very low risk tolerance for loss of reputation.

For more than three years, the OIG has identified weaknesses in FTC information security planning. In addition to recommending improvements in governance, the need for development of an enterprise architecture, acquisition planning, and documentation of decisions and supporting rationale, we emphasized that reliance on the FTC workforce as a countermeasure for inadequate planning and mature business processes is not a long-term solution. Staff turnover

and introduction of new technologies are critical changes that introduce greater risk and consequently require more mature business processes, planning, and monitoring if the FTC is to maintain its capability to protect its information assets.

The FTC adopted a two-year IT Strategy and Transition Plan to design, acquire, and implement commercial cloud technology solutions for its FTC IT needs. The complexity of the modernization plan and the aggressive implementation time frame necessitate careful planning and documentation of requirements along with monitoring of contractor performance and product quality – areas of FTC weakness identified in prior OIG FISMA and other reports.

The FTC has been working to improve its governance practices through its governance boards. As evidenced by meeting minutes and other governance board artifacts, governance board members have taken a more active role in reviewing project plans, risk evaluations, and other artifacts. The importance of governance boards' monitoring roles has significantly increased as the FTC proceeds with its efforts to modernize and expand its IT capabilities. The disruption that is a normal part of any major change increases risk. The governance boards will serve a critical role in identifying, accepting, and mitigating risks during the modernization.

While the establishment and use of the governance boards are significant FTC information security and privacy planning enhancements, there remain substantial opportunities for improvement. To support the modernization effort, the FTC will need to establish enterprise-level security and privacy control baselines, risk management procedures, acquisition plans, and project management practices that ensure modernization components meet FTC needs and are delivered on schedule and within budget.

The FTC has not developed an enterprise architecture that addresses both IT and information assets, as required under FISMA and OMB Circular A-130. Even the latest Strategy and Transition Plan issued on September 30, 2016, while a substantial improvement over prior planning efforts, has a Headquarters (HQ) data center focus and does not address the full scope of FTC information activities. For example, the document describes the broad scope and range of the FTC mission to protect consumers and maintain competition, but focuses planning on services provided to staff and contractors (e.g., the strategy identifies 10 mission-critical IT systems, such as email, telecommunications, Internet access, and mobile devices). The Strategy and Transition plan recognizes the presence of systems hosted outside the FTC HQ data center, but does not address their information content or how they are part of the FTC IT enterprise architecture.

While planning for information assets that directly support the FTC workforce is critical, FTC information system planning should be more comprehensive, establishing security monitoring requirements and monitoring approaches that can demonstrate that FTC systems, wherever they are located, protect information assets and have the control mechanisms to demonstrate that the controls are effective. Until the FTC effectively addresses enterprise architecture planning, it will

continue to show deficiencies under the CIGIE maturity model and fall short of FISMA and OMB requirements.

6. RECOMMENDATIONS AND IMPACT ASSESSMENTS

The remainder of this report provides the OIG assessment of the FTC information security and privacy programs for each of the Cybersecurity Framework functional areas. For each recommendation for improvement, we also identify the potential adverse impact from failing to address the finding, using the Low, Moderate, High scale contained in NIST Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, defined as follows:

- Low: The vulnerability may have a limited adverse effect on organizational operations, assets, or individuals;
- Moderate: The vulnerability could be expected to have a serious adverse effect on organizational operations, assets, or individuals; or
- High: The vulnerability could be expected to have a severe or catastrophic adverse effect on organizational operations, assets, or individuals.

The impact assessments are provided to assist FTC planning of mitigating actions and to address OMB required deficiency reporting. In this report, a NIST severe or catastrophic adverse effect is classified as an OMB "significant deficiency," a NIST serious impact is classified as an OMB "reportable condition," and a NIST limited adverse impact is classified as an OMB "other" weakness. A weakness that presents an imminent threat to FTC assets or mission is identified as a "significant deficiency" or a "reportable condition" and is immediately reported to FTC management.[12]

In our FY 2016 evaluation, we did not identify any situations that we rated as High under the NIST definition. As stated in our report, and as we have done in prior years, a High would have been immediately reported to FTC management. This would provide FTC management the opportunity to implement mitigating actions such that vulnerabilities initially assessed as High are reduced to Moderate (and FTC assets are protected) prior to completion of our FISMA data collection period.

[12] FISMA defines a significant deficiency as: 1) a material weakness under the Federal Managers Financial Integrity Act (FMFIA) and 2) an instance of a lack of substantial compliance under Federal Financial Management Improvement Act (FFMIA), if related to financial management systems. For example, A significant deficiency is defined as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken. A reportable condition is a control deficiency or combination of control deficiencies that in management's judgment represent significant deficiencies in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives. A reportable condition that the agency head determines to be significant enough to be reported outside the agency shall be considered a material weakness under the FMFIA. (See OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Managem*ent, and OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*).

Our FY 2016 report does not include any items with a Low rating on the NIST scale. The FTC has generally resolved items with a Low impact during the course of our evaluation and are not included in our reporting. Thus, as shown in our report, the recommendations remaining in our FY 2016 report are Moderate impact.

Recommendations in this report should be included in the appropriate FTC Plan of Action and Milestones (POA&M) for resolution by management. The OIG independently monitors mitigation of all open FISMA recommendations based on the FTC corrective action plan, as part of its ongoing FISMA assessment process.

6.1. IDENTIFY – DEVELOP THE ORGANIZATIONAL UNDERSTANDING TO MANAGE CYBERSECURITY RISK TO SYSTEMS, ASSETS, DATA, AND CAPABILITIES

The activities in the Identify Function are foundational for effective use of the Cybersecurity Framework because they measure the organization's understanding of information security and privacy requirements and risks within the business context (i.e., FTC mission), the resources that support critical functions, and the related cybersecurity risks. The Metric Domains within the Identify function are Risk Management and Contractor Systems.

6.1.1 CyberScope Metrics

The CIGIE Maturity Model 5-level scoring criteria is intended to be automatically applied to all cybersecurity framework functions (Identify, Protect, Detect, Respond, and Recover). However, CIGIE and DHS have not revised the questions for the Identify function for the Maturity Model approach. Failure to revise the question set resulted in providing no questions for Levels 1 (Ad Hoc) and 5 (Optimized), but awarding FTC 3-points for Level 1, and no points for Level 5. DHS anticipates resolving scoring inconsistencies when it completes revisions for FY 2017 CyberScope reporting.

REDACTED

Under the Maturity Model concept, this response pattern means the FTC understands the risks and vulnerabilities and has defined adequate policies and procedures, but does not consistently implement those policies and procedures. This scoring conclusion is supported by OIG test results. We reviewed a number of artifacts (e.g., FTC policies and procedures, Authorization to Operate (ATO) packages, performance work statements, status reports, and Privacy Impact Assessments) that are normal products of the FTC information security and privacy programs. The artifacts were inconsistent: some documents showed an understanding of IT security and information technology, while other documents evidenced a lack of understanding of the technology, how it is used by the FTC, and associated FTC security requirements. Similarly, some documents showed lack of attention to detail by referencing obsolete laws and guidance and describing solutions that are inconsistent with the identified technology.

Exhibit 11: FTC CyberScope Scoring for Identify Function

REDACTED

6.1.2 OIG Assessment of the Identify Function

The Identify Function contains the foundational elements for an information security and privacy program. As shown in the Cybersecurity Framework Functional Taxonomy, the Identify Function includes the capability of an organization to identify its information assets; understand the need for and impact of information security and privacy on its business environment; maintain a governance program that ensures that systems needed to support its missions are properly planned, acquired, documented, and monitored; and maintain a risk management program where decisions are risk-based and documented.

As the OIG reported in prior FISMA evaluations, the FTC has an in-depth understanding of its mission, and its workforce understands its information assets and the need for an emphasis on protecting them from unintentional as well as intentional acts by insiders and outsiders. By embedding concern for protecting information assets in its daily activities, the FTC's workforce has long served as a compensating countermeasure. FTC staff have made extra efforts to identify and correct deficiencies resulting from poor contractor performance and the lack of systems and procedures that monitor performance and automatically identify and report anomalies.

The FTC recognizes that its technological infrastructure requires modernization. Over the past several years, the agency has started efforts to modernize its information technology capabilities. In concert with OIG recommendations for improvement, the FTC instituted an IT Governance Program, improved capital investment procedures, improved its system inventory practices, and leveraged DHS and GSA services to improve security while constraining costs. The FTC is continuing its modernization efforts with its September 30, 2016, Strategy and Transition Plan.

As with any significant change, implementation of the Strategy and Transition Plan has associated risks: risk that change will introduce new vulnerabilities without associated mitigating factors, solutions proposed will not provide anticipated benefits, or information assets are compromised during the transition. Controls inherent in the Identify Function of the Cybersecurity Framework – Governance, Risk Management, and Asset Management – will be critical to ensure that the FTC is able to complete its modernization efforts with minimal risk.

In prior FISMA evaluations, the OIG made recommendations to improve IT governance, asset management, risk management, and other areas within the Identify Function. While the FTC made significant efforts to improve its governance practices, other changes have weakened FTC

controls. For example, in prior years, the FTC had a comprehensive system inventory. While the technological implementation was inefficient, poorly documented, and relied on individual action to maintain integrity, the replacement system is poorly documented, and requires use of multiple, technologically different databases.

6.1.3 Recommendations

Our FY 2016 evaluation identified the following four recommendations to improve the Identify Function.

6.1.3.1 Complete the System Inventory

As part of our FY 2016 evaluation, we sought to determine the status of the replacement of the FTC legacy system inventory (i.e., is the replacement complete, does it have the appropriate security artifacts, and does the replacement system meet FTC needs). The FTC proposed to address weaknesses OIG identified in its Certification and Accreditation (C&A) process (FY 2014 – 04: Certification and Accreditation) with a new process based on the Department of Justice (DOJ) *Cyber Security Assessment and Management* (CSAM) product. The CSAM implementation would also replace the FTC legacy system inventory process, resolving OIG concerns about insufficient control identification and documentation for systems classified as Minor Applications.[13] The CSAM C&A and system inventory processes were scheduled for completion by the second quarter FY 2016.

The FTC legacy system inventory was originally created using the Microsoft Access database language. The legacy system evolved so that it included both technology-based and paper systems and all the data elements needed to support FTC security information such as Authority to Operate (ATO) expiration dates, hosting location, FISMA categorization, System Owner, Information System Security Officer (ISSO), and privacy requirements. The system was augmented with an Excel spreadsheet that tracked similar information for FTC websites and social network presence. The legacy system, however, was difficult to maintain, poorly documented, had limited reporting flexibility, was not fully integrated with FTC ATO procedures, and required extensive manual support.

During our FY 2014 FISMA evaluation, the OCIO stated that the replacement inventory system would support its ISCM implementation. The new inventory system would provide an integrated view of all systems used by the FTC regardless of system ownership and hosting arrangements. OCIO advised the OIG that the revised inventory would also include information showing that associated requirements (e.g., ATO, Privacy Impact Assessment (PIA), System of Records Notice (SORN), and System Security Plan (SSP)) are in place and current, and that security artifacts are continuously reviewed, as required under the FTC's continuous monitoring plan.

[13] An assumption of the Minor Application classification is that the majority of controls needed are inherited from the system with which it is consolidated (NIST SP 800-16). The Minor Application classification is no longer used in current NIST and OMB guidance.

In our FY 2016 system inventory evaluation, we sought to determine whether available documentation showed the data elements the system contains, where they are located (i.e., within CSAM or other database), and procedures that are or will be used to maintain the system inventory. We also attempted to review procedures used to validate the system data transferred.

OCIO advised that the new system is based on use of the CSAM and that it is in the process of moving the FISMA inventory data elements contained in the legacy system to CSAM. Data elements that were not moved to CSAM were to be ported to SharePoint. Management did not provide a requested mapping that showed the name of the data elements moved from the legacy system to either CSAM or SharePoint and their designation in the new system.

The OIG is concerned that the CSAM-based inventory system may not have the data elements necessary to support FTC security and privacy activities, especially as the FTC continues its extensive modernization efforts. We asked for a transition plan and a list of data elements that the new inventory system would contain. OCIO advised that there was no transition plan, and the data elements had not been finalized.

The FTC's legacy system inventory contained both electronic and paper-based systems that collect and maintain federal information and included information such as: System Name, System Owner, System Category, Privacy Impact Assessment (PIA) and System of Records Notice (SORN) requirements.[14] The FTC's legacy systems inventory was used to support both FISMA and privacy OMB quarterly and annual reporting requirements, and is provided to the OIG annually. In prior evaluations, the OIG assessed the FTC's legacy inventory system as maintaining the information necessary to support its needs.

OMB Circular A-130 requires that agencies maintain an inventory of the agency's major information systems, information holdings, and dissemination products, at the level of detail that OMB and the agency determine is most appropriate for overseeing and managing the information resources. We expected that the FTC would add new data elements to its new system inventory to address new requirements (e.g., NARA Controlled, Unclassified Information requirements) and that all data elements from the legacy system would not be carried forward as FTC designed its systems inventory to meet current needs and architecture. When we asked if the all data elements in the legacy system would be carried forward, OCIO advised that the legacy system still existed and all data elements in the legacy system would be carried forward into the new system in either the CSAM component or the SharePoint component. However, no complete data element list was provided. Without a complete list of the data elements the new system would contain, it is not possible to determine whether FTC has aligned the inventory contents with its business needs as required under OMB Circular A-130. Without a system replacement

[14] The Federal Trade Commission Information Security Program Handbook, Volume 3: All Employee Information Security Policy and Procedure (June 2012).

and transition plan, the risk is increased that the system inventory system will not meet FTC needs, and the FTC has no assurance that associated processes include appropriate controls.

With regard to database validation during transition, the OCIO provided the standard FTC policy for adding systems to the inventory. In its POA&M, the OCIO also stated that it had "reached out to system points of contact to determine if the systems are still in use, and whether or not the system can be discarded from future systems inventory reports." This comment, our identification of a system that remained in the inventory after we were informed that it was not in use and should have been removed more than three months earlier, plus the OCIO identification of three expired ATOs during FY 2016 increased our concerns regarding the risk associated with propagating the new database with erroneous data when transferring legacy data without validation.[15] When converting to a new system, the best practice is to test the data transferred using the same controls as new data input. This ensures that all data meets the same level of accuracy and consistency.

The FTC determined that the CSAM portion of the system inventory is a Moderate Impact system. To ensure that the FTC has a complete inventory of its information systems assets, as required under OMB Circular A-130, the FTC should identify all components used to maintain its inventory of information systems and data assets (e.g., CSAM, SharePoint-based, and manual components) as a system under the provisions of SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* (RMF). The system may be comprised of one or more subsystems, as determined by the FTC. The complete inventory system should be categorized as a Moderate Impact system under the same criteria as its CSAM component. This will ensure that security of the FTC inventory meets a consistent baseline regardless of the implementation approach (e.g., automated or manual). The total system should be supported by the security artifacts appropriate for a Moderate Impact system under NIST guidance, e.g., a System Security Plan that includes a description of current state and target state architectures, a security controls baseline, a description of the data element content and structure, and a description of the user community (privileged and unprivileged). The documentation should identify the data elements in the new system, their location in the CSAM-based inventory, and any special characteristics such as Privacy Act restrictions, subject to NARA requirements, or subject to a litigation or law enforcement hold.

OCIO should also validate the accuracy and completeness of the CSAM-based inventory and place it under strict configuration management procedures so that it can operate as a trusted component of the FTC ISCM system. The ISCM should identify validation of the systems inventory as a critical control that is performed at least on an annual basis.

[15] OCIO identified three systems with expired ATOs after the data were migrated to the new CSAM-based system. These types of errors should be caught when migrating data to ensure that data errors are eliminated from the new database.

Recommendation: FY 2016 – 01 - ID.AM

To ensure FTC has an inventory that contains the information required to describe its information systems and data holdings, FTC should document its inventory practices and validate associated databases.
The FTC should document its system inventory management system and validate the system, database, and management procedures, at least on an annual basis, as a trusted FTC ISCM component under configuration control.
Potential Impact: Moderate Reference: OMB Circular A-130 (Jul 2016) section 5. a.1) a) Inventories

6.1.3.2 Review application classification to ensure conformity with NIST guidance

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems* (February 2006), identified three types of information systems: Major Applications, General Support Systems, and Minor Applications. Major Applications and General Support Systems were required to have individual ATOs. Minor applications were not required to have fully documented security controls because it was assumed that their security controls are typically provided by the General Support System or the Major Application with which they operate.

NIST has been removing the concepts of General Support System (GSS), Major Application, and Minor Application from its security guidance for a number of years. This change was reinforced with the July 2016 release of a rewritten OMB Circular A-130, which no longer uses this terminology. Instead, NIST describes a process for combining components of a system into a single system boundary in SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*. The Risk Management Framework (RMF) discusses the process for establishing the boundaries for a system using concepts such as system of systems, subsystem, and application. The RMF approach has the advantage of allowing individual system components (e.g., systems, subsystems, or applications) to be independently categorized and can include the concepts of external systems and dynamic systems. While the RMF provides agencies with increased flexibility for establishing system boundaries, it also requires increased attention to ensure that 1) control requirements for all systems are identified, 2) controls are evaluated to identify those that are shareable (by subordinate systems, subsystems, applications, or across the enterprise), 3) ownership and responsibilities of shareable controls is defined, and 4) all controls are tested in accordance with established procedures.

The FTC system inventory contains a number of systems classified as Minor Applications under the HQ data center using prior NIST guidance. These Minor Applications include systems that are isolated from the data center (e.g., the SIL), systems that are externally hosted with little

interaction with the data center (e.g., Maas360), and systems that provide critical mission support and are a significant cost investment (e.g., litigation support). Under the prior NIST classification approach, the controls for the Minor Applications were not effectively documented because the approach assumed that controls were provided by the HQ data center.

In response to an FY 2014 OIG recommendation to improve security artifacts, the FTC began to improve its documentation for Minor Applications.[16] In the action plan FTC proposed for our FY 2014-04 recommendation, FTC stated that –

> CSAM will be used to document the security controls in our General Support systems (GSS), and Major and Minor applications. CSAM will also provide a framework to support the security assessments of our GSS, and Major and Minor applications.

The CSAM system implementation was scheduled for completion by the second quarter of FY 2016, and completion of the population of the database by the first quarter of FY 2017. However, by the end of the FY 2016 data collection period, the FTC had not provided criteria for classifying its systems so that they better align with NIST guidance. Further, the FTC classified a system as a Minor Application and placed it under the HQ data center ATO even though the system's primary control component is the cloud-based Maas360 which has its own Provisional-ATO issued by the GSA under its FedRAMP cloud services program. This structure was not appropriate using Minor Application assumptions because it resulted in omission of documentation of those security controls for which the FTC retained operational responsibility (e.g., documentation of the certificate-based security for FTC supplied mobile devices).

Under RMF procedures, there is no assumption that needed controls are present. Needed controls must be identified and their implementation or inheritance documented. Controls may be system-specific (control responsibility remains with the system), common (the control is inherited from another system which retains responsibility for operation and testing), or hybrid where the control is partly the responsibility of the system and partly the responsibility of another system (inherited control).

As part of its inventory system revision and upgrade, the FTC should review its system boundaries and categorizations, especially for systems identified as a Minor Application. The review should ensure that system boundaries are aligned with current NIST RMF guidance and controls for all systems are properly documented, in accordance with the RMF, and their implementation and/or control inheritance described. The capabilities of the FTC CSAM

[16] FY 2014 – 04: Certification and Accreditation - FTC should revise its process for determining Minor Applications and documenting security controls. Minor Applications should be differentiated from system services/functions and should be documented in a format that supports the ability to assess the security impact of a Minor Application as well as its impact on the associated GSS. SSPs should adequately document control environments so that they can serve as an implementation guideline, a security baseline for testing, and a reference for individuals assessing the level of control compliance.

implementation should be configured to support the RMF system boundary and control inheritance approach.

Recommendation: FY 2016 – 02 - ID.AM

To ensure controls are properly documented and responsibility for control maintenance and testing is identified, FTC should review its information system boundaries and control inheritance practices.

The FTC should complete its evaluation of its system boundaries as it completes its CSAM implementation. FTC should eliminate use of the Minor Application designation and document leveraged/common controls in accordance with NIST RMF guidance and ensure that all FTC systems are covered by an FTC ATO, either specific to the system or under a related system.

Potential Impact: Moderate Reference: NIST 800-37 rev 1 (June 2014), NIST 800-53r4 (April 2013)

6.1.3.3 Document Risk-Based Decisions

In SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST describes a risk management framework (RMF) for government use to establish, maintain, and monitor information security and privacy environments in federal interest systems and programs. NIST SP 800-53 provides a catalog of controls that agencies are to use to identify baseline controls for control environments established in accordance with the RMF. While the use of RMF structure and SP 800-53 controls is mandatory, NIST recognizes that building effective security control environments requires that controls and their implementation be tailored to agency missions, information sensitivity, threat environment, technology, resource constraints, and risk tolerance (i.e., level of risk or harm an agency is willing to accept).

The FTC makes numerous decisions in deciding what technologies to implement and how they should be configured as they design, develop, and maintain their information systems. In its current governance posture, FTC information and privacy decisions are typically made after discussions among individuals from various organizations that may be affected. While there is evidence that risk topics are discussed from review of governance board Meeting Minutes and by the nature of decisions made, there is no repeatable process for ensuring that risks are identified and mitigation strategies developed, and that board decisions are clearly documented, especially the nature of the decision; the risks, costs, and benefits of alternatives considered; and the potential impact on the FTC's risk threshold. These deficiencies illustrate ongoing challenges in maturing the FTC's IT governance.

For example, FTC has embarked on a major initiative to move applications to cloud technologies. The ITGB approved the 60% Strategy and Transition Plan in its April 26, 2016 meeting, subject to a number of expressed concerns, including those shown in Exhibit 12.

Exhibit 12: ITGB Strategy Concerns on 60% Version (4/26/2016)

A concern was raised regarding Records Management and E-Discovery being included in the 60% Strategy and Transition Plan.
Cybersecurity is also a concern. Need to ensure that going to the Cloud is secure.
Everyone wants to be comfortable with moving to the Cloud. This option needs to address our Privacy and Security controls, and then we can choose a Cloud solution.
Today's vote is on the concept, not necessarily the solutions at this time.
Whatever solution we pick will have to be accredited and go through the ATO process (FedRAMP).
Unanimous approval of the 60% plan, noting the concerns and risks mentioned in today's meeting.

Subsequently, the ITGB approved a final version of the Strategy and Transition Plan dated September 30, 2016. However, the FTC did not document how or if the ITGB concerns raised when approving the 60% Strategy and Transition Plan were resolved or document risk-based support for the decision to transfer hosting services from the HQ data center to cloud technology. Instead, the OCIO stated that –

> The concerns raised by the ITGB were high-level statements on the direction or were about specific solutions that the plan did not and would not be addressing. For example, concerns related to ensuring that a cloud solution is secure, accredited, and go through the ATO process, was included in the 60% plan when discussing the Target Architecture. The ITGB meeting minutes reflect the comments made, and the discussion that the vote was on the concept of moving to the cloud and not on specific solutions. Any specific comments or concerns on the plan by governance board members or their staff were captured by the comment spreadsheet.

In reviewing the comment spreadsheet provided by the OCIO, the OIG could not identify that the ITGB comments regarding cloud security concerns were captured or addressed.

While the final *Strategy and Transition Plan* (September 30, 2016) acknowledged OMB direction to "evaluate safe, secure cloud computing options before making any new investments" and that GSA established a "standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services," the document did not discuss the risks associated with cloud technology that could affect its use by the FTC. For example, NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, and SP 800-53 remind decision-makers that using multi-tenant service model cloud services has a "serious underlying complication - subscribing organizations typically share components and resources with other subscribers that are unknown to them."

While the final Strategy and Transition Plan contains statements that security issues would need to be addressed, it contained no discussion as to how the cloud-based approach would affect the FTC's security risks; The Strategy and Transition Plan also identified properly documented risks reported to the Commission, a definition for FTC risk tolerance, and a requirement for the Information System Security Officer (ISSO) to design controls based on risk tolerance, as desired outcomes from the CIO Team, but did not discuss when these items would be available or procedures to be used to evaluate risk associated with the Strategy and Transition Plan activities. For example, reputation risk is a significant risk to the FTC, yet the potential impact of transitioning to a cloud-based structure on reputation risk was not discussed.

Conducting government business has inherent risks. Government law, regulation, and guidelines recognize that agencies can manage risk to acceptable levels, but risk cannot be eliminated. Key to effective risk management is documentation of decisions made, evaluation of associated risks, and documentation of the decisions and the rationale for those decisions. Decision documentation helps ensure that management objectives regarding risk thresholds and risk acceptance are met, managers are held accountable, and information assets are accorded the security and privacy protection required as the FTC introduces new technologies and procedures in response to changes in mission and the FTC risk/vulnerability profile.

The FTC has embarked on an accelerated effort to modernize its IT capabilities. Success in achieving the modernization objectives will require a risk management process that is integrated with the FTC IT governance process to ensure that requirements are defined and associated with business needs and that decisions are made using repeatable, documented risk-based decisions. Properly documented risk-based decisions will ensure risk rationales are communicated between related components, between contractors, and will facilitate analysis of the level of residual risk and future risk reduction activities as the FTC systems mature and evolve.

Recommendation: FY 2016 – 03 - ID.GV, ID.RA

To ensure the rationale for decisions are transparent and auditable, the FTC should document decisions made and the associated risk-based supporting rationale.

The FTC should implement a formal procedure for documenting risk-based decisions as part of the FTC risk management program.

Potential Impact: Moderate Reference: OMB Circular A-130 (Jul 2016) 5. a. 1) c) NIST SP 800-37, SP 800-53r4 (April 2013) Chapter 2.1

6.1.3.4 Develop Risk Analyses for its IT Modernization Initiative

The modernization initiative described in the Strategy and Transition Plan identifies a number of activities that must be completed. Each of these activities and associated information assets have performance, schedule, resource, security, and other risks that should be considered before acquisitions or other resource commitments are approved. At the FTC, under NIST guidance, the objective of risk analysis should be to identify and mitigate relevant risks before committing to a strategy, that also commits FTC to –

- an information or data architecture;
- a funded investment;
- an acquisition to obtain goods and services to support investment completion; and
- production installation where a failed activity could adversely impact FTC mission performance or compromise information assets (e.g., unauthorized access to controlled unclassified information or omission of a control results in project delay).

In accordance with NIST SP 800-30, (*Guide for Conducting Risk Assessments*), NIST SP 800-39 and the Federal Acquisition Regulation (FAR Parts 7 and 39), risk analyses should be conducted from the information system (Tier 3), mission/business process (Tier 2), and organization (Tier 1) perspectives. The tiered analyses help to ensure all relevant risks are identified and mitigated. For example, at Tiers 1 and 2, organizations may use risk assessments to evaluate, systemic information security-related risks associated with organizational governance and management activities, mission/business processes, enterprise architecture, or the funding of information security programs; and at Tier 3, organizations may use risk assessments to more effectively support the implementation of the Risk Management Framework (i.e., security categorization; security control selection, implementation, and assessment; information system and common control authorization; and security control monitoring).

A risk analysis might be accomplished for each separately monitored modernization activity or as a consolidated analysis applicable to the total modernization effort (see NIST SP 800-30 and

800-37). The objective is to ensure appropriate risks are identified and addressed. As explained in the NIST risk analysis guidance, "organizations employ risk assessments on an ongoing basis throughout the system development life cycle and across all of the tiers in the risk management hierarchy—with the frequency of the risk assessments and the resources applied during the assessments, commensurate with the expressly defined purpose and scope of the assessments."

As described in NIST SP 800-30 and SP 800-39 guidance and OMB Circular A-130, the range of risks that should be considered may overlap among the three NIST risk analysis tiers. For example, potential risks that could apply to an activity in any tier at some level may include, but are not limited to: the threat space; vulnerabilities; missions/business functions; mission/business processes; enterprise and information security architectures; information technologies; personnel; facilities; supply chain relationships; organizational governance/culture; procurement/acquisition processes; organizational policies/procedures; organizational assumptions, constraints, risk tolerance, and priorities/trade-offs. The FTC will need to develop guidance and standard operating procedures to ensure adequate risk analyses are consistently performed to support FTC decision-makers in making specific decisions and allowing comparisons across the organization.

In its Risk Management Framework (SP 800-37), NIST identified risk-based decisions as the basis for effectively managing risk. Risk-based decision-making ensures that management understands the nature and magnitude of risks affecting mission performance and has the opportunity to mitigate or accept those risks. Formally documenting risk decisions facilitates ongoing analysis so that the decisions may be revisited as vulnerabilities or technology changes, or management's risk tolerance changes and funding is increased to mitigate previously accepted risks.

The FTC needs to formalize its risk-decision process to support ongoing planning and acquisition activities. The FTC Modernization Initiative introduces a critical need to quickly implement a formal risk management process. FTC's modernization initiative is scheduled for substantial completion within the next two years. Decisions made about these initiatives will impact FTC operations and, given the projected systems life spans, its capability to effectively protect its information assets for at least the next 10 years. The FTC needs to ensure that decisions are clearly documented and the rationale for selecting an alternative are consistently performed. Documenting decisions and the supporting rationale will help ensure that management has the information necessary to evaluate the level of residual risk and facilitate integration of separately acquired or developed components into a cohesive system with known and acceptable risks.

Recommendation: FY 2016 – 04 - ID.RA

To ensure that the FTC understands the risks associated with its modernization initiative, FTC should conduct risk analyses from both the individual information system and organization levels (Tier1 and Tier 3).

The FTC should implement a formal risk management program that addresses the requirements of OMB Circulars A-123 and A-130 and the guidance contained in NIST Special Publications 800-30, 800-37, and 800-39. The FTC should conduct risk analyses for its IT Modernization Initiative.

Potential Impact: Moderate	References: OMB Circular A-123 (Jul 2016), OMB Circular A-130 (Jul 2016), NIST SP 800-30 rev. 1 (Sept 2012), NIST 800-37 rev 1 (June 2014), NIST 800-39 (March 2011)

6.2 PROTECT – DEVELOP AND IMPLEMENT THE APPROPRIATE SAFEGUARDS TO ENSURE DELIVERY OF CRITICAL INFRASTRUCTURE SERVICES

The activities in the Protect Function support the ability to prevent, limit, and contain the impact of a potential cybersecurity event. The Metric Domains within the Protect Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

6.2.1 CyberScope Metrics

In FY 2016 the Protect function used the same metrics as in FY 2015 without use of the Maturity Model approach. The OIG assessed the protect function as most critical to the FTC as it relates to the agency's capability to protect its information assets. The OIG assessment of the CyberScope metrics showed that the FTC focused on information protection. REDACTED

We assessed that the metrics that were not met under the Consistently Implemented category are effectively addressed through compensating countermeasures that ensure asset protection is not adversely affected. For example, the FTC has not yet fully implemented PIV for logical access control, but implemented two-factor authentication for remote access prior to establishment of the PIV requirement. Further, the FTC met 50% of the Metrics identified as Managed and Measurable even though the scoring approach awarded no points for that achievement.

Exhibit 13: FTC CyberScope Scoring for Protect Function

REDACTED

6.2.2 OIG Assessment of the Protect Function

The FTC focuses on protecting its information assets. As stated in prior FISMA evaluations, the FTC's focus on asset protection has come at a price of systems that may not be as technologically current or efficient as FTC management would like, but the risk averse approach has thus far been successful in protecting FTC information assets.

The FTC recognizes that its information technology needs substantial modernization and upgrade if it is to continue to effectively support mission needs and continue to protect its information assets and address new vulnerabilities. The FTC initiated a two-year modernization plan to modernize and increase the resilience of its information technology. The modernization strategy is set forth in the *Strategy and Transition Plan, Security and Technology Services*, FY 2016 – FY 2019, dated September 30, 2016. The objective of this Strategy and Transition Plan is to provide "a roadmap that will guide significant changes for core operations that will lead to revitalized support for objectives, strategies, and goals identified in the FTC's Strategic Plan."

As described by the Chief Information Officer (CIO), the Strategy and Transition Plan identifies five key areas for improvement:

- Section 1: Highlights the alignment of IT strategic initiatives to FTC's mission. Establishes priorities to refocus workforce efforts from maintenance of legacy services to continuous improvement and business aligned change. Establishes performance metrics in the areas of Customer Satisfaction, Stable and Secure Operating Environment, and Effective IT Resources;

- Section 2: Baselines current IT performance and practices;

- Section 3: Discusses industry best practices and relevant federal guidance;

- Section 4: Establishes IT performance guidance and practices to include focusing on the customer, increasing mobility, effective cybersecurity, highly available architecture, data driven decision culture, and realigns IT resources to better support the FTC mission; and

- Section 5: Provides a high-level schedule and budget for key IT strategic initiatives that will transform FTC's IT environment from on premise custom hosting to secure leased services.

As described, the Strategy and Transition Plan provides reasonable objectives for the modernization effort. However, as described in the previous section of this report, the Strategy and Transition Plan does not provide sufficient information to demonstrate that the modernization can be reasonably completed within the Strategy and Transition Plan's planning horizon; nor does it provide sufficient information to demonstrate that information security and privacy and performance risks have been considered and that appropriate mitigations have been planned (e.g., risk assessments have not been conducted).

The Strategy and Transition Plan acknowledges its deficiencies regarding performance criteria. For example, the plan includes the following statement about Key Performance Indicators (KPI) for monitoring performance of the FTC modernization effort:

> As the FTC works to stabilize and improve the IT operating environment, we will be developing KPIs to monitor our progress. The FTC is looking to establish metrics for both the regional offices and headquarters around the areas of user satisfaction, security, and effective use of IT resources. We will evaluate performance indicators, establish a baseline and create annual performance targets.[17]

Strategic Planning Challenge

FTC strategic security planning has been hampered by high turnover in the CIO position. As reported in the OIG's *Evaluation of the Federal Trade Commission's Office of the Chief Information Officer*, Report No. ER 16-02 (December 2015), since 2000, FTC has had five permanent CIOs with a 34-month average tenure. This turnover level results in inconsistent strategic planning as direction and approaches change with each new CIO. Further, the lack of formal strategic plans weakens the ability of the FTC to move forward on strategic plans that are not adequately defined and supported. The Strategy and Transition Plan provides a foundation for developing an FTC enterprise-level strategic plan but, as described throughout this report, it misses key elements that OMB and NIST require for effective, risk-based IT planning, particularly when undertaking risk-laden commercial cloud services.

[17] The OIG identified similar deficiencies in an acquisition that was to provide litigation support to FTC users, known as eDSS. The OIG found that management failed to identify and incorporate performance criteria and metrics. As a result, the eDSS product selected did not have the functionality needed to support FTC mission requirements and could not be effectively supported by the FTC computing infrastructure. See FTC Office of Inspector General, *Opportunities Exist to Accelerate Maturation of the FTC's Information Technology Governance Practice* (September 30, 2016).

Why IT Investments Fail

The Government Accountability Office (GAO) has performed numerous studies to determine why "federal IT investments too frequently fail or incur cost overruns and schedule slippages while contributing little to mission-related outcomes." [18] While GAO focused on IT investment failures at large agencies, the findings are also applicable to small agencies like the FTC. Specifically, that –

> These and other failed IT projects often suffered from a lack of disciplined and effective management, such as project planning, requirements definition, and program oversight and governance.

In prior FISMA evaluations, the OIG has made a number of recommendations for improving FTC IT governance and acquisition practices. For example, in its FY 2015 FISMA Evaluation Report the OIG recommended that the FTC –

> Continue to evolve FTC Continuous Monitoring Management practices through improvements in governance practices and providing improved documentation and estimating guidance; Review governance policies and procedures to resolve potential organizational conflicts of interest and confusion in roles and responsibilities, and ensure that Boards are appropriately established and resourced and processes are sufficiently guided and documented to complete assigned responsibilities. (Recommendation FY 2015 – 01)

The OIG made similar recommendations for improving FTC IT governance practices in its report, *Opportunities Exist To Accelerate Maturation Of The FTC's Information Technology Governance Practices* (September 30, 2016). The OIG based its recommendations for improving FTC governance practices on guidance included in various OMB Memoranda and NIST guidance such as SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* (March 2011). OMB policy and guidance for IT governance was consolidated into OMB Circular A-130, *Managing Information as a Strategic Resource* (July 27, 2016). OMB considered IT governance to be sufficiently important that Circular A-130 addresses Governance as the second of nine policy topics (Planning and Budgeting, Governance, Leadership and Workforce, IT Investment Management, Information Management and Access, Privacy and Information Security, Electronic Signatures, Records Management, and Leveraging the Evolving Internet). Among the specific governance requirements with which agencies must comply are –

- Define, implement, and maintain processes, standards, and policies applied to all information resources at the agency, in accordance with OMB guidance;

[18] Government Accountability Office, GAO 14-713, *High-Risk Series: An Update, February 2015, Improving the Management of IT Acquisitions and Operations*.

- Require that the CIO, in coordination with appropriate governance boards, defines processes and policies in sufficient detail to address information resources appropriately. At a minimum, these processes and policies shall require that:

    - Appropriate measurements are used to evaluate the cost, schedule, and overall performance variances as IT investment management, enterprise architecture, and other agency IT or performance management processes;

    - There are agency-wide policies and procedures for conducting IT investment reviews, operational analyses, or other applicable performance reviews to evaluate IT resources, including projects in development and ongoing activities; and

    - Data and information needs are met through agency-wide data governance policies that clearly establish the roles, responsibilities, and processes by which agency personnel manage information as an asset and the relationships among technology, data, agency programs, strategies, legal and regulatory requirements, and business objectives.

- Ensure that the CIO is a member of governance boards that inform decisions regarding IT resources to provide for early matching of appropriate information resources with program objectives; and

- Require that information security and privacy be fully integrated into the system development process.

6.2.3 Recommendations

The FTC should continue efforts to modernize its IT environment. The Strategy and Transition Plan provides a reasonable description of FTC's modernization objectives, but the lack of IT investment planning, risk evaluation, and performance criteria creates an unknown level of performance risk. For example, the Strategy and Transition Plan did not address the risk differences between a shared environment of a commercial cloud and the dedicated environment of the HQ data center (e.g., the Contract Lifecycle Management (CLM) system may not be compatible with a shared services environment); and the modernization documents describe an environment where components are acquired from different suppliers without describing how interoperability and consistency will be maintained.

The FTC's existing governance program provides an acceptable planning structure, but, as previously recommended, needs improvement before it can effectively support the significant level of activity anticipated for the modernization effort.

6.2.3.1 Segment Modernization Activities Into Useful Segments

GAO and OMB have determined that agency major IT investments frequently fail because requirements were consolidated into large, complex acquisitions with requirements that are difficult to effectively define and manage, especially in IT where technologies rapidly change.[19] To reduce the risk of investment failure, OMB Circular A-130 requires agencies to structure acquisitions for major IT investments into "useful segments, with a narrow scope and brief duration, in order to reduce risk, promote flexibility and interoperability, increase accountability, and better match mission need with current technology and market conditions." Specifically, OMB directs agencies to divide investments into segments that perform useful functions where performance objectives can be clearly defined and measured and monitored to facilitate assessment of successful performance.

The FTC modernization initiative is a major IT investment. The Strategy and Transition Plan identifies three FTC strategic goals supported by the IT modernization (Protect Consumers, Maintain Competition, and Advance Organizational Performance). The Strategy and Transition Plan then identifies ten Strategic Initiatives to address those goals and identifies them as Business Specific, General Purpose, Infrastructure, and IT Customer & Success Management as shown below:

- Business Specific
  - BE Application Modernization
  - Legal Review Tool Replacement
  - Custom Application Reengineering
- General Purpose
  - NextGen Devices and Remote Access
  - Enterprise Content Management
  - FTC.gov Rehosting
  - Office Productivity Tools and Unified Communications
- Infrastructure
  - Modernize Network
- IT Customer & Success Management
  - Improve IT Resources
  - User Training & Change Management

The Strategy and Transition Plan associates the four groups identified above, with approximately 15 activities identified in a one-page transition schedule that assumes that there will be multiple projects aligned to each strategic initiative; projects that will cover both new features and decommission legacy technology.

[19] See Government Accountability Office, GAO-16-469, *Information Technology Reform: Agencies Need to Increase Their Use of Incremental Development Practices,* August 2016 and Government Accountability Office, GAO-11-672, *Acquisition Planning: Opportunities to Build Strong Foundations for Better Services Contracts*, (August 2011).

The Strategy and Transition Plan describes a complex set of activities, with a focus on technological functionality, but with limited consideration for establishing an acquisition management approach that ensures that products developed through independent projects can be integrated into a cohesive enterprise architecture.

In moving forward, the FTC needs to define an overarching enterprise architecture strategy to serve as guidance to ensure that independently acquired functional components meet equivalent (but not necessarily identical) security requirements and can be interconnected to comprise the single campus environment visualized in the Strategy and Transition Plan.

The Strategy and Transition Plan presents the modernization effort from a functional perspective. The FTC also needs to examine its modernization effort from the acquisition perspective to address OMB guidance regarding acquisition segmentation, i.e., identify the goods and services to be acquired to support the modernization initiative and establish a plan for defining (dividing the acquisitions into manageable segments), acquiring, and managing those acquisitions that minimizes risk. For example, analysis of performance risk might indicate risk could be reduced if planning services to document the current enterprise architecture and target architecture were acquired and the deliverable successfully completed before a solicitation to implement modernization components are awarded. Similarly, acquisition planning addressing schedule and performance risk might indicate that use of benchmarking is appropriate in selecting litigation support products that meet FTC needs for scalability and flexibility.

In implementing its modernization Strategy and Transition Plan, the FTC should divide the modernization activities into cohesive segments that can be independently planned, budgeted, acquired, and monitored. The segments and their overall importance to the completed architecture should be evaluated through techniques such as risk analysis and critical path analysis that identify security, functional, sequencing, and time dependencies that affect successful performance. Segmentation allows security, privacy, and performance criteria to be tailored to the requirements of each segment while maintaining consistency and provides an opportunity to evaluate performance at specific milestones, with an acquisition and program management structure that allows for correction of underperforming segments.

Recommendation: FY 2016 – 05 – PR.IP, PR.MA

To ensure IT investments are appropriately planned, funded, executed, and monitored, the FTC should divide its modernization initiatives into segments that provide useful products in relatively short timeframes within a defined Enterprise Architecture.

The FTC should structure modernization activities for acquiring major IT investments as useful segments that can be independently planned, acquired, and monitored.

Potential Impact: Moderate Reference: OMB Circular 130 (Jul 2016) 5. d. 1) f)

6.3 DETECT – DEVELOP AND IMPLEMENT THE APPROPRIATE ACTIVITIES TO IDENTIFY THE OCCURRENCE OF A CYBERSECURITY EVENT

The Detect Function enables timely discovery of cybersecurity events. Metric Domains within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

6.3.1 CyberScope Metrics

The key element of the Detect function is the Information Security Continuous Monitoring (ISCM) program/system. Continuous monitoring offers a solution for information security gaps resulting from point-in-time monitoring by providing near real-time data on high priority controls and less current information for lower priority controls. While the FTC developed a *Continuous Monitoring Plan* in FY 2013 and a *Continuous Monitoring Strategy* dated November 12, 2014, it did not fully implement an ISCM. REDACTED

Exhibit 14: Detect CyberScope Score

REDACTED

6.3.2 OIG Assessment of the Detect Function

The Detect Function relates to controls an agency uses to identify threats and vulnerabilities. Prior assessment approaches used a variety of point-in-time analyses that sought to determine the health of an information security and privacy environment. OMB and NIST determined that the point-in-time approaches had several significant problems, including an unknown program status between analysis points, coverage gaps in those instances when all controls were not evaluated, and unnecessary costs incurred through testing of less important controls.

On October 3, 2014, OMB and NIST established a requirement for agencies to implement an ISCM program that would allow them to tailor the test cycle for individual controls based on risk. Using this approach, controls that guard against high impact, high occurrence potential could provide near real-time information, and agencies could implement a continuous authorization process to replace the three-year reauthorization cycle for federal information systems. ISCM is also part of the cyber security Cross-Agency Priority (CAP) goal, which is part of a broader plan to (1) simplify the IT environment (with cloud computing and enterprise architecture) to make it more manageable, and (2) invest in the needed security to make the IT systems more resilient.

The FTC developed an ISCM Plan in FY 2013 and an ISCM Strategy, last updated in November 2014. An ISCM is intended to provide a management tool that allows senior management and other stakeholders the ability to effectively manage today's IT environments. Given the scale and complexity of an enterprise-level IT environment, effective management is a data intensive undertaking that must be tailored (in scope and level of detail) to stakeholder needs. For example, FTC executive managers will want information consolidated at very high levels to address questions such as which are all systems operating normally and which are not. Technical staff require detailed information such as which communications ports are open and which sensors are reporting anomalies that might indicate an attack in progress. To achieve these multiple objectives, an ISCM system is not a single tool, but a set of tools operating within a structure that allows inputs from multiple sources to be combined to provide consolidated displays showing system performance tailored to stakeholder needs. The FTC ISCM Strategy and ISCM Plan described how the FTC proposed to implement an ISCM.

The ISCM was not implemented as written. The FTC has not completed a number of significant elements of its ISCM, such as identifying controls to be monitored and frequency and monitoring method; mapping of recipients of ISCM reporting, and the nature of the information reported (e.g., raw metrics for technical support staff and summary displays for management personnel) and frequency of reporting (e.g., as requested, weekly, quarterly). The FTC also has a number of tools in place that can be used in constructing an ISCM (e.g., Nessus, Remedy Trouble Reports, DHS FTC cyber hygiene reports, and Trouble Reports, and FedRAMP continuous monitoring reporting). As described in its ISCM planning documents, the FTC needs to show what information will be extracted from these individual tools and how they will be combined to provide the system status needed for its stakeholders. The completed ISCM should also be able to identify anomalous conditions that warrant direct and potentially immediate review by a security officer (for security issues) or a manager (for performance issues). Shifting data analysis and anomaly identification to the ISCM will substantially improve data consistency and quality while reducing staff workloads.

6.3.3 Recommendations

6.3.3.1 Implement an ISCM

The FTC should implement a fully compliant ISCM that ensures information collected through the ISCM is appropriately consolidated and summarized to address the information needs of FTC technical staff and managers. The ISCM should identify the controls to be monitored and associated with appropriate metrics, collection approaches, and collection frequency. It also should have the capability to extract data elements targeted to FTC management needs at all organizational levels and automatically generate cross-domain analyses to support identification of security events and development and evaluation of FTC risk thresholds and tolerances. The ISCM should be evaluated at least on an annual basis to ensure it continues to meet FTC needs and processes and are subject to continuous improvements.

Recommendation: FY 2016 – 06 – DE.CM

To ensure it has the capability to monitor the health of its security and privacy programs, the FTC should implement a fully compliant ISCM.

The FTC should implement a fully compliant ISCM as described in its ISCM Plan in FY 2013 and its ISCM Strategy, dated November 2014.

Potential Impact: Moderate References: OMB Circular A-130 (Jul 2016) Appendix I, 5. k. NIST SP 800-137 (Sep 2011)

6.3.3.2 Revise the Plan of Action and Milestones Process

NIST requires that each Authorization to Operate (ATO) decision package include a Plan of Action and Milestones (POA&M or POAM). Under OMB policy, a POA&M is a document that identifies tasks to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled milestone completion dates. OMB has specified the content for a POA&M, but agencies may use their own discretion in developing a POA&M format.

As outlined in OMB guidance POA&Ms must:

Be tied to the agency's budget submission through the unique system identifier that links the security costs for a system to the security performance of a system;

- Include all security weaknesses found, and in need of remediation, during any assessment done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments. These plans should be the authoritative agency-wide management tool, inclusive of all evaluations; and
- Be shared with the agency Inspector General to ensure independent verification and validation of identified weaknesses and completed corrective actions.

POA&Ms can be incorporated into the new automated processes that agencies are putting in place as part of their ISCM programs. For example, FTC POA&Ms may be incorporated in its CSAM implementation as long as there is no information loss in scope or coverage.

Historically, FTC POA&Ms served as a basis for tracking the status of OIG recommendations as well as providing the system vulnerability mitigation status as required for FTC programs and systems. However, the FTC's previous POA&M did not contain information sufficient to determine the status of OIG recommendations because the recommendation descriptions and FTC mitigation actions did not track to information previously provided on POA&M or action plans. This demonstrates that the FTC's POA&M process requires review to maintain the

consistency and reliability to be the authoritative, agency-wide management tool as intended in OMB policy.

Recommendation: FY 2016 – 07 – DE.CM

To ensure that the POA&M is the consolidated tracking tool required by OMB, FTC should revise and update its POA&M procedures.

The FTC should revise its POA&M process and content to ensure it meets OMB information requirements (e.g., all security weaknesses found, and in need of remediation, during any assessment done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments) and can be an effective, authoritative, agency-wide management tool.

Potential Impact: Moderate	Reference: OMB Memorandum M-14-04 (Nov 2013) item 44 What is required of agency POA&Ms? OMB Circular A-123 (Jul 2016) V.B. Corrective Action Plan Requirements

6.4 RESPOND – DEVELOP AND IMPLEMENT THE APPROPRIATE ACTIVITIES TO TAKE ACTION REGARDING A DETECTED CYBERSECURITY EVENT

The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

6.4.1 CyberScope Metrics

REDACTED

However, due to the agency's small size and controls in place that inhibit attacker ability to successfully penetrate the FTC infrastructure, the FTC has experienced few incidents.

Exhibit 15: Respond CyberScope Score

REDACTED

6.4.2 Respond Function Assessment

The FTC experienced few IT security incidents in FY 2016, as compared to other federal agencies, reporting a total of 73 incidents. The FTC estimated that it averaged approximately one hour to address an incident for a total level of effort of 73 hours.

6.4.3 Recommendations

No recommendations for Respond.

6.5 RECOVER – DEVELOP AND IMPLEMENT THE APPROPRIATE ACTIVITIES TO MAINTAIN PLANS FOR RESILIENCE AND TO RESTORE ANY CAPABILITIES OR SERVICES IMPAIRED DUE TO A CYBERSECURITY EVENT

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

6.5.1 CyberScope Metrics

REDACTED

The FTC uses a mix of contractor owned and operated systems and systems owned, operated, and hosted on its HQ data center. Contractor-hosted systems have in place offsite backup and tested contingency plans. The HQ data center has offsite data backup, but does not have contingency plans in place.

Exhibit 16: Recover CyberScope Score

REDACTED

6.5.2 OIG Assessment of Recover Function

For a number of years, FTC management elected to defer establishment of a disaster recovery capability. During this period, the FTC proposed a number of different disaster recovery strategies, but they never moved beyond conceptualization. In our FISMA evaluations from FY 2013 through FY 2015, the OIG provided recommendations to establish and test a viable disaster recovery plan. In each instance, management provided an action plan to establish a disaster recovery capability that appeared to be a viable solution, but the plans were never implemented. In FY 2014, the FTC began implementing a disaster strategy including acquiring an Alternate Data Center (ADC) that was intended to provide a locale for an alternate processing capability. This plan, however, was changed, and the ADC was repurposed to serve as a data backup site and to support improved redundancy for selected applications and the FTC Wide Area Network

(WAN). The FTC has not provided documentation supporting its continuing decision to defer implementation of a disaster backup capability.

In FY 2016, in response to OIG recommendations, the FTC began to develop a cloud-based alternate processing capability to support a disaster recovery strategy. As part of this effort, the FTC provided the OIG with the following documents to demonstrate its contingency planning efforts:

- FTC Disaster Recovery Plan (DRP), September 30, 2016, Version 1.0
- Federal Trade Commission, Information Systems Contingency Plan, (FTC-ISCP), September 30, 2016
- Information Technology Security Program, Business Impact Assessment, Version 2, September 8, 2015
- Memorandum discussing an FTC Disaster Recovery Strategy for Core IT Services, dated December 30, 2015
- BIA/DR TechStat Materials for a TechStat provided to the FTC It Governance Board on May 24, 2016

The OIG reviewed this material and determined that it does not provide the basic information necessary to support a contingency plan/disaster plan for the HQ data center. Given that improvement of FTC contingency/disaster planning is a long-term outstanding OIG recommendation, the OIG identified the following list of deficiencies in current contingency planning documents:

- Use of laws, regulations, standards, and guidance that were obsolete and superseded, or not applicable;
- Omission of primary NIST contingency planning guidance (e.g., SP 800-34, *Contingency Planning Guide for Federal Information Systems*, Rev 1, 11/11/2010) and failure to follow that guidance;
- Inclusion of externally hosted contractor owned and hosted systems as core systems hosted on the FTC data center;
- Use of a disaster recovery approach that focuses on reestablishing individual application systems before restoring the supporting data center;
- Reliance on general market research describing possible disaster recovery strategies instead of presenting an approach tailored to FTC needs;
- Unrealistic assumptions such as assuming that someone will be assigned to decide when and how to initiate the plan as opposed to identifying that responsibility;
- Use of incorrect contingency planning terminology; and
- Failure to integrate operations contingency planning with disaster planning.

The lack of disaster planning also adversely affects FTC operations and maintenance activities. Under NIST guidance (SP 800-34) and contingency planning best practices, disaster plans are one component of a set of integrated contingency plans. Contingency planning should identify potential areas of failure or system disruption and decide whether they should be addressed through normal operations procedures or through a disaster plan. Developing contingency plans and the associated processes and procedures for their testing and maintenance identifies weaknesses that may result in operational disruption or potential disaster situations.

For example, in October 2016, the FTC experienced an HVAC failure that caused overheating and shutdown of all computers at the data center. Given the facility's redundant HVAC capabilities and sensors, the outage should have been a minor event and resolved as part of normal operations. However, the FTC operates in a "lights out" mode. In a lights out mode, it is critical that contingency plans are in place to effectively address unexpected events occurring during non-duty hours. In the absence of contingency planning, the HVAC failure resulted in a loss of computing service for all FTC staff and contractors of more than 62 hours (almost three workdays) when computers overheated while waiting for appropriate staff to arrive. When they arrived more than four hours after the HVAC failure occurred, it took less than an hour to correct the HVAC failure.

The OIG's review of the FTC's after action/root cause analysis identified a number of planning weaknesses, some of which were immediately corrected, but others remain unresolved because they require longer term solutions. These include identifying and replacing aged equipment that do not have the reliability or serviceability to meet current FTC needs and maintaining a continuous improvement process for its contingency planning efforts. This should include a contingency plan for its HQ data center that can effectively respond to the full range of potential system disruptions (e.g., failure of a single sever to loss of the total data center). Contingency planning will reduce the risk of a total system failure as the planning activities identify single points of failure and high risk areas that may be mitigated without implementing a disaster recovery capability with immediate failover.

In its root cause analysis, the FTC overlooked the need for comprehensive contingency planning for its HQ data center. In responding to OIG legacy FISMA recommendations, the FTC has focused on developing a strategy for disaster backup for the facility. In doing so, however, it has overlooked the full scope of a disaster planning effort.

As shown in NIST SP 800-34, disaster planning is to be performed within a comprehensive contingency planning environment. For the FTC data center, *disaster planning* should be integrated with the *operational response plans* used to address the transitory outages and processing anomalies that are generally resolved through ongoing, daily activities. As shown by the October 2016 HVAC outage, a relatively simple equipment failure can result in a significant and costly outage. A number of the challenges in restoring data center service could have been

avoided or at least mitigated had best practices for disaster planning been included in normal data center operations. For example:

- the FTC encountered difficulties because needed system documentation was not readily available. A basic disaster planning assumption is that no resources or capabilities of the failed system are available to support the recovery effort. Thus, documentation needed to support recovery should be stored elsewhere where it is readily available; and

- the FTC encountered difficulties communicating with senior staff and customers. Disaster plans include regularly updated communications plans describing how communications are maintained with all stakeholders when data center capabilities are not available.

Further, FTC outage analysis procedures do not provide for estimating the cost of a system outage. Outage information is necessary to support return on investment and other cost and risk analyses. The outage cost analysis should include estimates of the impact on the FTC workforce as well as the costs directly associated with service restoration. These estimates are useful regardless of contract type. The information is used for planning and examining the return on investment and not for billing. Thus, the estimates need to be reasonable and consistently developed, but not necessarily all inclusive. For example, it may be sufficient to use an average staff cost as opposed to actual costs.

To ensure continuity of mission support and prevent loss of FTC information, the FTC needs to maintain a contingency planning program. The program, in accordance with NIST SP 800-34 guidance, should address all disruptions that may impact FTC information systems. The program should include metrics (e.g., results of last test) that monitor contingency planning for applications hosted on external sites for input to the FTC ISCM. FTC applications hosted on an internal FTC data center, should have an Information System Contingency Plan (ISCP), as defined in SP 800-34. The FTC HQ data center should have a disaster recovery plan (DRP). FTC contingency planning should be clear that all systems supporting the FTC have plans in place to minimize mission disruption from the occurrence of short-term and long-term disruptions.

6.5.3 Recommendations

6.5.3.1 Develop Contingency Plans for the FTC HQ data center

The FTC should develop contingency plans for its HQ data center and the systems it hosts. This would include contingency plans for normal operations, disaster recovery plans, and information system contingency plans for applications that are hosted on the HQ data center but are independently maintained. The primary planning guidance is NIST SP 800-34. Plans should be developed so that they provide the level of service needed to support FTC mission requirements. If a suitable contingency strategy cannot be developed that provides the needed support level, a POA&M item should be developed (as allowed under SP 800-34 guidance) and the vulnerability elevated to Executive Management. This will ensure Executive Management recognizes and

accepts the adverse impacts that may occur if FTC does not have contingency capabilities that meet its business needs.

Recommendation: FY 2016 – 08 – RC.RP

To minimize the potential for and disruption from both short and long-term outages, the FTC should institute a continuing contingency planning capability.

The FTC should develop viable contingency plans for the HQ data center and hosted applications. Plans should be tested to ensure viability and ensure staff are trained to execute them. Contingency plans should clearly define actions to be performed and individuals responsible for plan activation and other critical decisions should be identified.

Potential Impact: Moderate	Reference: NIST SP 800-34 rev 1 (11/11/2010) CP-2 Contingency Plan

7. STATUS OF PRIOR YEAR RECOMMENDATIONS

The OIG closes and consolidates recommendations based on action plans and related information provided by FTC management. Recommendations are closed when the action plan for mitigating the identified vulnerability is completed as determined through artifacts provided. As is standard practice, recommendations from FISMA reports or other OIG reporting may be consolidated when management's action plan shows a single mitigation addresses multiple recommendations.

Exhibit 17 shows the status of agreed-upon recommendations made in the OIG's FY 2015 FISMA evaluation and those from prior FISMA reports that remain open. [20] We note that the FTC has not implemented a recommendation from the FY 2013 FISMA calling for the FTC to revise its infrastructure access procedure to restrict access by employees and contractors until background screening is completed, in accordance with FTC policy. In addition, three of the six recommendations in the OIG's FY 2014 FISMA evaluation were scheduled to be implemented by no later than September 30, 2016, but they remain open, and management has moved the implementation dates to FY 2017. Only one of the seven recommendations in our FY 2015 FISMA evaluation, to which management concurred, have been implemented, even though two recommendations were scheduled to be implemented by no later than September 30, 2016.

Exhibit 17: Previous OIG FISMA Recommendations That Remain Open

Reference	POAM Reference	OCIO Status	OIG Status[21]
FY 2013 – 07	Not found on POA&M provided	Open	Open – Scheduled FY 2017 resolution
FY 2014 - 03	156	Open	Open – Scheduled Completion – 9/1/2017 – Status In Progress
FY 2014 - 04	157	Open	Open – Scheduled Completion - 9/5/2016 – Status In Progress
FY 2014 - 06	159	Closed	Open – Scheduled Completion – 7/29/2016 – Status In Progress
FY 2015 - 01	233	Open	Open – Scheduled Completion – 12/1/2016 – Status In Progress
FY 2015 – 02	210	Open	Open – Scheduled Completion – 12/30/2016 – Status In Progress
FY 2015 - 03	212	Open	Open – Scheduled Completion – 9/30/2016 – Status In Progress
FY 2015 - 05	235	Open	Open – Scheduled Completion – 4/21/2017 – Status In Progress
FY 2015 - 06	236	Open	Open – Scheduled Completion – 12/30/2017 – Status In Progress
FY 2015 - 07	237	Open	Open – Scheduled Completion – 12/30/2017 – Status In Progress

[20] An OIG recommendation issued in a Final Report that has a CAP in place is "open" if it has not been validated and officially closed by the OIG.

[21] Completion date shown is that shown in the POA&M or provided by FTC. In those instances, where there are multiple milestones and no item completion date, the completion date shown is the completion date for the last milestone completed. *OCIO Open Recommendations*, August 2016.

Exhibits 18 through 20 provide detail on the status of previous OIG FISMA recommendations.

Exhibit 18: Status of FY 2013 OIG Recommendations

STATUS OF FY 2013 OIG RECOMMENDATIONS					
Reference	**Paragraph**	**Recommendation**	**Potential Impact**	**OCIO Action Plan[22]**	**OIG Assessment**
FY 2013 – 07: Identity and Access Management	6.4	FTC should revise its infrastructure access procedure to restrict access until background screening is completed per FTC policy.	Moderate	FTC has reviewed the current process and will make changes as necessary to ensure infrastructure access procedures are aligned with FTC infrastructure access policy.	**OPEN** Per OCIO, completion is now scheduled for FY2017 Q2 For recommendation FY 2013-07, the FTC has developed a process to adjudicate fingerprints prior to allowing employees and contractors network access. The FTC is currently requiring all contractors to have their fingerprints adjudicated prior to allowing network access. The FTC is currently scheduled to implement fingerprint adjudication prior to network access for all new employees and contractors by the end of second quarter FY 16.

[22] OCIO comments are presented as provided.

Exhibit 19: Status of FY 2013 OIG Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[23]	OIG Assessment
FY 2014 – 03: Infrastructure Documentation	6.3	FTC should take appropriate action to ensure completion of an appropriate CM plan and ensure that is effectively applied to the FTC and across all FTC systems.	Moderate	For recommendation FY 2014-03, the draft Configuration Management (CM) plan is currently being circulated and comments are expected back by the end of September 2015. The FTC has made significant progress in updating its configuration management documentation and is currently on schedule to complete all the configuration documents by the end of first quarter FY 16. We are still on track for a second quarter FY16 implementation of the CM plan. The FTC expects to close this recommendation by the end of the second quarter of FY 16. The Configuration Management (CM) plan will be completed by fourth quarter FY 15. Implementation of the CM plan and the associated automated Remedy process will be completed by second quarter FY 16.	**OPEN** The Draft CM plan has not been provided.

[23] OCIO comments are presented as provided.

Exhibit 19: Status of FY 2013 OIG Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[23]	OIG Assessment
FY 2014 – 04: Certification and Accreditation	6.4	FTC should revise its process for determining Minor Applications and documenting security controls. Minor Applications should be differentiated from system services/functions and should be documented in a format that supports the ability to assess the security impact of a Minor Application as well as its impact on the associated GSS. SSPs should adequately document control environments so that they can serve as an implementation guideline, a security baseline for testing, and a reference for individuals assessing the level of control compliance.	Moderate	For recommendation FY2014-04, the FTC has procured the Cyber Security Assessment and Management (CSAM) system. Access to CSAM has been configured for the FTC. User roles have been established and assigned to system owners and system administrators. All current POAMs have been loaded into CSAM and a process to load all future POAMs into CSAM has been established. The System Security Plan (SSP) for the Data Center General Support System (GSS) has been updated and we are reviewing the first draft. By the end of first quarter FY 16, we will initiate the SSP update for the Litigation Support System and the Mobile Internet Lab. The FTC expects to close this recommendation by second quarter FY 16. The FTC has procured the Cyber Security Assessment and Management (CSAM) system. CSAM will be used to document the security controls in our General Support systems (GSS), and Major and Minor applications. CSAM will also provide a framework to support the security assessments of our GSS, and Major and Minor applications. CSAM will be implemented by second quarter FY 16.	**OPEN** The Milestones shown on the POA&M focus on worksteps associated with acquiring and installing CSAM. The worksteps shown do not address the development of processes to ensure that those inventory items that were not transitioned to CSAM are still retained and the criteria used to differentiate Major and Minor Applications. Further, we have not been provided a mapping showing that the data elements contained in the legacy inventory system have been migrated to the new CSAM/SharePoint system.

Exhibit 19: Status of FY 2013 OIG Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[23]	OIG Assessment
FY 2014 – 06: Contingency Plans	6.6	FTC should develop a disaster recovery strategy and implementation plan.	Moderate	For recommendation FY 2014-06, the FTC activated alternative telecommunication and remote data backup services at its Alternate Data Center (ADC) in the first quarter of FY 15. The OCIO is in the process of reviewing the updated FTC Business Impact Analysis (BIA). The FTC is on track to have an agency-approved disaster recovery strategy and implementation plan by the end of the first quarter of FY 16. The FTC expects to close this recommendation by the end of the first quarter of FY 16. In first quarter FY 15, the FTC activated alternative telecommunication and remote data backup services at its Alternate Data Center (ADC). The OCIO is in the process of updating the FTC Business Impact Analysis (BIA). The BIA update will be completed fourth quarter FY 15. The FTC will have an agency-approved disaster recovery strategy and implementation plan by the first quarter of FY 16.	**OPEN** Several documents were provided describing the contingency planning efforts conducted. These documents focused on developing a BIA and general contingency strategy documents. These documents, however, did not provide a viable strategy or structure for developing a contingency plan for the FTC data center. Among the planning issues evidenced by the contingency planning documents are: the laws, regulations, and guidance cited as the underlying authorities and contingency planning guidance were obsolete and superseded; the objective was to provide a contingency plan for the FTC HQ data center, but a number if systems included in the analysis are not hosted on the data center; planning parameters such as the maximum tolerable downtime and restore time objective were incorrectly defined; and the risks associated with alternatives identified were not effectively evaluated.

Exhibit 20: Status of FY 2015 OIG Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[24]	OIG Assessment
FY 2015 – 01: Security Management and Governance Structure	6.1.1	Continue to evolve FTC Continuous Monitoring Management practices through improvements in governance practices and providing improved documentation and estimating guidance. Review governance policies and procedures to resolve potential organizational conflicts of interest and confusion in roles and responsibilities, and ensure that Boards are appropriately established and resourced and its processes sufficiently guided and documented to complete assigned responsibilities. (Also, see recommendation FY 2015-04 to elevate the CPO to voting membership on the ITGB)	Moderate	Management concurs and will continue to improve governance practices and documentation. Planned actions for FY16 include: • Analyze governance practices since the issuance of the August 2014 Governance Charter, conduct lessons learned discussions with IT Governance Board and IT Business Council members, and develop updated Governance Charter to improve governance effectiveness and efficiency. • Review and update IT Business Council and IT Governance Board roles and responsibilities to ensure clearly defined and differentiated governance oversight and operational management responsibilities. • Develop improved Governance Charter documentation, including supporting processes and procedures, and update the FTC Administrative Manual to provide a governance guidance framework for all FTC staff. Expected Completion Date: FY2017 Q2	OPEN Last Milestone is shown as Not Started and included the following comment: "Develop improved Governance Charter documentation, including supporting processes and procedures, and update the FTC Administrative Manual to provide a governance guidance framework for all FTC staff."
FY 2015 – 02: FTC Security Policy and Procedures/Sys	6.1.2	FTC should continue its review of Accreditation Boundaries for Minor Applications, re-	Moderate	Management concurs and has completed the installation of the Cyber Security Assessment and Management (CSAM) tool to assist	OPEN

[24] OCIO comments are presented as provided.

Exhibit 20: Status of FY 2015 OIG Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[24]	OIG Assessment
tem Accreditation Boundaries		designating those systems that are significant resource investments or have special security considerations as Major Applications.		in documenting our Accreditation Boundaries. Planned actions for FY16 include: • Continue review of Accreditation Boundaries. • Based on the results of the review, designate new Minor and Major FISMA applications. Expected Completion Date: FY2017 Q1	Expected completion date shown as 12/30/2016 with the final task showing as Not Started.
FY 2015 – 03: Certification and Accreditation	6.1.3	To support FTC Approval to Operate/Authorization (ATO) decisions, FTC should provide staff applicable NIST guidance, including risk assessment criteria, for reviewing security artifacts provided by other federal organizations that are using the same software or services.	Moderate	Management concurs. Planned actions for FY16 include: • Develop risk assessment criteria using applicable NIST guidance to assist in review of security artifacts provided by other federal organizations in support of Approval to Operate/Authorization (ATO) decisions. • Review all existing ATOs that leverage security artifacts from other federal agencies using the new criteria. Expected Completion Date: FY2016 Q4	OPEN OIG requested a copy of the *Draft of risk assessment criteria applied to third party audits and ATO from other federal agencies* identified as completed on 6/16/2016 with a final scheduled for completion at 8/31/2016 but still noted as In Progress. The artifact provided in response to the OIG request was a "list of documents that provide NIST guidance for leveraging third party audits and ATO from other federal agencies" reported as completed on 3/28/2016.
FY 2015 – 05: Configuration Management	6.2	FTC should review its CM strategy to ensure that it is addressing CM from the agency perspective and not a single, system level approach.	Moderate	Management concurs. Planned actions for FY16 include: • Revise the change management policies and procedures to incorporate configuration management principles.	OPEN Scheduled completion date shown as 4/21/2017 with last milestone shown as not started. No intermediate artifacts were shown as completed.

Exhibit 20: Status of FY 2015 OIG Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[24]	OIG Assessment
				• Develop procedures for revision of documentation, security baselines and correcting configuration errors. • Develop a reporting methodology to inform stakeholders of the configuration and change management status for systems and services. Expected Completion Date: FY2017 Q1	
FY 2015 – 06: Identity and Access Management / Remote Access Management	6.3	FTC should focus on achieving full compliance with PIV-enabled I&A so that compliance is not subject to continuing delay and PIV compliance is maintained as new technologies and contracting approaches are added as part of FTC's modernization efforts.	Moderate	Management concurs and has enabled logical PIV access for all administrators and select users on a test basis. The technical infrastructure necessary for a Commission-wide role out is in place and tested. Planned actions for FY16 include: • Revise existing policies and procedures to be compatible with PIV Card issuance for logical access and identity management for FTC users. • Update information in the FTC Administrative Manual and provide guidance for all FTC staff regarding new procedures. • Review and update FTC roles and responsibilities for FTC organizations affected by changes to policies and procedures. • Require mandatory PIV-enabled I&A for logical access to the FTC network for all administrative and end-user access.	OPEN Scheduled completion shown as 12/30/2017. Four of five milestones shown as Not Started.

Exhibit 20: Status of FY 2015 OIG Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[24]	OIG Assessment
				• Develop plans for further integration of PIV Card two-factor authentication as the I&A for all FTC Enterprise-wide systems. Expected Completion Date: FY2017 Q2	
FY 2015 – 07: Contractor Systems	6.8	FTC should implement the user-focused metrics for the FTC Data center and determine whether the monitoring approach or similar approach should be expanded to other FTC systems.	Moderate	Management concurs, and the Infrastructure Performance Report has been updated to focus on user-facing services. Infrastructure components have been separated so that the Contractor can report on infrastructure outages as well as service outages. Infrastructure outages have a calculated effect on services and all outages can be leveled based on specific impact and are weighted based on user populations to provide a consistent evaluation of performance. The new format allows for ongoing adjustment as services and communities change over time. Planned actions for FY16 include: • Update configuration of the Cascade performance management systems in order to investigate poor regional office performance and establish continuous monitoring of user service performance from a network perspective. • Assess current custom user performance-measuring tool. Based on the results of the assessment,	OPEN The development of user focused performance metrics is critical for development of an ISCM system. Metrics need to be aligned with the capabilities to monitor that are allowed under the various acquisition approaches. FTC is still seeking to improve its current tool or select an alternate tool or process to develop additional user performance metrics.

Exhibit 20: Status of FY 2015 OIG Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[24]	OIG Assessment
				either take steps to improve the current tool or select an alternate tool or process to develop additional user performance metrics. Expected Completion Date: FY2017 Q1	

8. SUMMARY OF FINDINGS AND RECOMMENDATIONS

In FY 2012, the FTC instituted a process to evolve its information security and privacy programs to change from ad-hoc, reactive processes to a formalized structure. This change was intended to provide a security environment where the status of the environment was known and change would be planned and controlled to avoid the introduction of security weaknesses.

In support of this initiative, the FTC developed policies and procedures and established a governance program to provide consistent planning and oversight of FTC information security investments. As noted in previous FISMA reports, the governance program has been maturing, but its Information Technology Governance Board is over-burdened with detailed analysis addressing implementation issues, instead of focusing on significant acquisition decisions, fully developing alternatives, and approving risk-based mitigation strategies for the selected options.

OMB Circular A-130 identifies the governance functions assigned agency CIOs. The Circular also states that agencies must –

> Define, implement, and maintain processes, standards, and policies applied to all information resources at the agency, in accordance with OMB guidance.

The Circular also states that agencies should –

> Require that the CIO, in coordination with appropriate governance boards, defines processes and policies in sufficient detail to address information resources appropriately.

Under this authority and working through their governance boards, agencies and their CIOs have the latitude to establish a governance structure where responsibilities and workloads may be tailored to meet their needs. Thus, the FTC can revise its governance structure to address new OCIO organizational structure and workload constraints. It is anticipated that the FTC will use the management discretion identified in Circular A-130 in responding to recommendation *FY 2015 – 01: Security Management and Governance Structure*, "Continue to evolve FTC Continuous Monitoring Management practices through improvements in governance practices and providing improved documentation and estimating guidance."

The OIG anticipates that the FTC will also use this management discretion in responding to our other recommendations regarding the need for improved procedures and documentation, particularly recommendations: FY 2016 – 01 - ID.AM; FY 2016 – 03 - ID.GV, ID.RA; FY 2016 – 05 – PR.IP, PR.MA; and FY 2016 – 07 – DE.CM. The OIG objective is to ensure that processes, procedures, and decisions are documented, address FTC needs, and are risk-based.

The FTC should make use of its information systems to improve performance and consistency. An objective of continuous monitoring is to change agency security and privacy from a reactive to a proactive mode, automatically reviewing data collected and reporting anomalies and other conditions that exceed FTC-specified conditions for staff action.

Expanded use of IT to collect and support FTCs security and privacy programs will facilitate institutionalization of planning and risk management practices that will improve program consistency and controlled integration of new technologies. Use of technology will also ensure that needed security artifacts are identified, current and sufficient to support operational requirements and strategic planning. Achieving these results is a complex undertaking that requires careful planning and attention to detail. Our assessment of the deficiencies of the FTC IT Strategy and Transition Plan showed that the modernization effort will be a high-risk effort unless management tools (e.g., an Enterprise Architecture, security baselines) and performance data are developed to monitor implementation and ensure that successful performance is defined and measurable.

Exhibit 21 provides a summary of the recommendations developed as part of the FY 2016 FISMA evaluation. When implemented, these recommendations will provide the planning tools and procedures necessary to support the FTC's modernization efforts while containing costs and supporting FTC risk management efforts.

Column 5 of Exhibit 21 presents an extract of management's official response to each OIG recommendation. Management's official response is included in this report as Appendix B.

The OIG cannot at this time provide detailed assessments of management's proposed actions to address the OIG's FY 2016 recommendations. The OIG will provide specific comments after we receive the Action Plans and have an opportunity to evaluate the milestones, performance measures, and plan alignment and timing of the Action Plans with the FTC's IT Strategy and Transition Plan.

The OIG's observations about management's official response are included in this report as Appendix C.

Exhibit 21: Summary of FY 2016 Recommendations

Reference	Paragraph	Recommendation	Potential Impact	Management Action Plan[25]
FY 2016 – 01 - ID.AM	6.1.3.1	*To ensure FTC has an inventory that contains the information required to describe its information systems and data holdings, FTC should document its inventory practices and validate associated databases.* The FTC should document its system inventory management system and	Moderate	Management will develop an action plan within 60 days, with overall completion expected no later than FY18 Q4.

[25] Management comments are extracted from the Management's Response included as Appendix B.

Exhibit 21: Summary of FY 2016 Recommendations

Reference	Paragraph	Recommendation	Potential Impact	Management Action Plan[25]
		validate the system, database, and management procedures, at least on an annual basis, as a trusted FTC ISCM component under configuration control.		
FY 2016 – 02 - ID.AM	6.1.3.2	*To ensure controls are properly documented and responsibility for control maintenance and testing is identified, FTC should review its information system boundaries and control inheritance practices.* The FTC should complete its evaluation of its system boundaries as it completes its CSAM implementation. FTC should eliminate use of the Minor Application designation and document leveraged/common controls in accordance with NIST RMF guidance and ensure that all FTC systems are covered by an FTC ATO, either specific to the system or under a related system.	Moderate	Management will develop an action plan within 60 days, with overall completion expected no later than FY18 Q4.
FY 2016 – 03 - ID.GV, ID.RA	6.1.3.3	*To ensure the rationale for decisions are transparent and auditable, the FTC should document decisions made and the associated risk-based supporting rationale.* The FTC should implement a formal procedure for documenting risk-based decisions as part of the FTC risk management program.	Moderate	Management will develop an action plan within 60 days, with overall completion expected no later than FY 18 Q2.

Exhibit 21: Summary of FY 2016 Recommendations

Reference	Paragraph	Recommendation	Potential Impact	Management Action Plan[25]
FY 2016 – 04 - ID.RA	6.1.3.4	*To ensure that the FTC understands the risks associated with its modernization initiative, FTC should conduct risk analyses from both the individual information system and organization levels (Tier1 and Tier 3).* The FTC should implement a formal risk management program that addresses the requirements of OMB Circulars A-123 and A-130 and the guidance contained in NIST Special Publications 800-30, 800-37, and 800-39. The FTC should conduct risk analyses for its IT Modernization Initiative.	Moderate	Management shall address this recommendation through an overall action plan to address A-123and A-130 requirements within the next 60 days as set forth under recommendation 3 above and expects that this plan shall also address and ideally consolidate or close action plans in response to the two recommendations (ER 16 – 03, 2 and 5) found in the OIG IT Governance evaluation. Management will develop an action plan within 60 days, with overall completion expected no later than FY 18 Q2.
FY 2016 – 05 – PR.IP, PR.MA	6.2.3.1	*To ensure IT investments are appropriately planned, funded, executed, and monitored, the FTC should divide its modernization initiatives into segments that provide useful products in relatively short timeframes within a defined Enterprise Architecture.* The FTC should structure modernization activities for acquiring major IT investments as useful segments that can be independently planned, acquired, and monitored.	Moderate	Management shall address this recommendation through an overall action plan to address A-130 requirements for Planning and Budgeting and IT Investment Management within the next 60 days. This plan shall include determination of enterprise architecture requirements sufficient to cost effectively meet the mission requirements of the FTC. The plan shall likely generate recurring reviews and updates every year to the IT Strategy and Transition Plan in accordance with A-130. Management will develop an action plan within 60 days, with a first iteration of updates expected no later than FY18 Q1.

Exhibit 21: Summary of FY 2016 Recommendations

Reference	Paragraph	Recommendation	Potential Impact	Management Action Plan[25]
FY 2016 – 06 – DE.CM	6.3.3.1	*To ensure it has the capability to monitor the health of its security and privacy programs, the FTC should implement a fully compliant ISCM.* The FTC should implement a fully compliant ISCM as described in its ISCM Plan in FY 2013 and its ISCM Strategy, dated November 2014.	Moderate	Management will develop an action plan within 60 days, with overall completion expected no later than FY18 Q1.
FY 2016 – 07 – DE.CM	6.3.3.2	*To ensure that the POA&M is the consolidated tracking tool required by OMB, FTC should revise and update its POA&M procedures.* The FTC should revise its POA&M process and content to ensure it meets OMB information requirements (e.g., all security weaknesses found, and in need of remediation, during any assessment done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments) and can be an effective, authoritative, agency-wide management tool.	Moderate	Management will develop an action plan within 60 days, with overall completion expected no later than FY 18 Q2.
FY 2016 – 08 – RC.RP	6.5.3.1	*To minimize the potential for and disruption from both short and long-term outages, the FTC should institute a continuing contingency planning capability.* The FTC should develop viable contingency plans for the HQ data center and hosted applications. Plans	Moderate	Management shall address this recommendation through an overall action plan within the next 60 days. This action plan shall also address and ideally consolidate or close action plans in response to prior OIG recommendations. Management will develop an action plan within 60

Exhibit 21: Summary of FY 2016 Recommendations

Reference	Paragraph	Recommendation	Potential Impact	Management Action Plan[25]
		should be tested to ensure viability and ensure staff are trained to execute them. Contingency plans should clearly define actions to be performed and individuals responsible for plan activation and other critical decisions should be identified.		days, with overall completion expected no later than FY 18 Q4.

APPENDIX A – FTC OIG FY 2016 FISMA CYBERSCOPE RESPONSE

REDACTED

APPENDIX B – MANAGEMENT'S RESPONSE

APPENDIX C - OIG OBSERVATIONS ABOUT MANAGEMENT'S RESPONSE

UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION

WASHINGTON, D.C. 20580

MEMORANDUM

DATE: March 1, 2017

FROM: Raghav Vajjhala, Chief Information Officer

TO: Roslyn Mazer, Inspector General

SUBJECT: Management's Response to OIG's FY 2016 Evaluation of the FTC's Information Security Program and Practices (FISMA Report)

The OIG's *FY 2016 FISMA Report* recognizes that "the FTC security environment continues to be strong and robust relative to its ability to protect its information assets." The report contains eight recommendations to further improve the agency's IT security maturity and modernization efforts and Management concurs with these recommendations.

In 2015, the Office of the Chief Information Officer (OCIO) established an IT Strategy and Transition Plan. That plan, along with updated IT workforce position descriptions and an IT Acquisition Strategy, was used to close all recommendations included in the OIG's *FY 2015 Evaluation Report of the Office of the Chief Information Officer*.

The current FISMA report includes a number of recommendations that reiterate past OIG recommendations for the agency to update its IT documentation practices. The agency has set forth in this response the action plans necessary to meet these concerns and close not only these recommendations but similar past recommendations.[1] As noted by the OIG in its *FY 2015 FISMA Report*, updating documentation practices requires a multi-year effort from the FTC.[2]

In 2016, OMB revised Circulars A-130 and A-123, updating expectations and outlining new requirements for areas of IT security management. At roughly the same time, CIGIE, OMB, and

[1] As noted by the OIG preceding its Section 7 in the *FY 2016 FISMA Report*, "it's common practice to consolidate recommendations assuming single action plans can address multiple items."

[2] From the OIG's *FY 2015 FISMA Report's* Executive Summary, "FTC needs to improve its security control planning, the quality of its security documentation, and the consistency of program implementation. Addressing these changes will require a concerted multi-year focus followed by consistent, monitored application and will help FTC mature its information security." (Emphasis added).

DHS updated the IG FISMA Reporting Metrics for evaluating agency security programs as reported through CyberScope.

As the FTC implements its IT Strategy and Transition Plan, the agency must consider cost-effective and streamlined changes to its IT management practices to meet requirements from OMB and DHS, as well as OIG recommendations. The FTC shall prioritize and organize its IT security efforts in the following order:

- Review and update technical security controls as appropriate to mitigate risk of compromise to the agency's information assets;
- Review documentation and modify as appropriate, to meet the requirements of OMB A-130 and A-123 guidance to manage an effective information security program that achieves cost-effective security based on the missions and risks faced by the FTC;
- Review documentation, and modify as appropriate, to improve IG FISMA Reporting Metric scores; and
- Review documentation and modify as appropriate to address OIG open recommendations that may remain after addressing A-130, A-123, and IG FISMA Reporting Metrics. (Management anticipates that updates in response to A-130, A-123, and IG FISMA Reporting Metrics should address most if not all FTC OIG recommendations.)

Management notes the FISMA evaluation includes no findings or recommendations for its privacy program. The IG Cyberscope metrics direct IGs "to conduct an annual independent evaluation to determine the effectiveness of the *information security* program and practices of their respective agency" (emphasis added) and thus are aligned with the CIO information security metrics, not the Senior Agency Official for Privacy (SAOP) metrics.[3]

[3] Although NIST 800-53, rev. 4 includes both security and privacy controls, the IG FISMA metrics leverage 800-53 to "define[] security control effectiveness and the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies." Moreover, as OMB acknowledged in A-123, footnote 21, "many of the existing NIST standards and guidelines that detail how to implement an agency-wide risk management framework do not fully address the role of privacy and agencies' privacy programs. In the future, NIST may revise or develop standards and guidelines to further clarify how privacy and agencies' privacy programs are integrated into the Risk Management Framework."

OIG Recommendation 1: FY2016 – 01 – ID.AM

To ensure FTC has an inventory that contains the information required to describe its information systems and data holdings, FTC should document its inventory practices and validate associated databases.

The FTC should document its system inventory management system and validate the system, database, and management procedures, at least on an annual basis, as a trusted FTC ISCM component under configuration control.

Responsible Official: Raghav Vajjhala

Action Plan: Management concurs with this recommendation.

Management notes that the OIG rated the FTCs current practices for system inventory management as "Met" in response to FY 2016 IG Reporting Metrics Indicator 1.1.1:

> Identifies and maintains an up-to-date system inventory, including organization- and contractor-operated systems, hosting environments, and systems residing in the public, hybrid, or private cloud. (2016 CIO FISMA Metrics, 1.1; NIST Cybersecurity Framework (CF) ID.AM.1, NIST 800-53: PM-5).

Management recognizes, however, the need to mature its current documentation so that the FTC has an inventory that contains up to date information required to describe its information systems and data holdings and has a process to keep the inventory current.

Management will initiate an annual process whereby the CIO and CPO assess, review, and accept for use system inventory information.[4] The process will enable the agency to maintain a system inventory that is complete, regardless of the technology hosting the system inventory -- CSAM or otherwise.

By establishing a process that enables the CIO and CPO to repeatedly assesses and improves the system inventory information, Management will establish a related process that assesses its completeness of system security control documentation to identify areas for improvement or areas of system control documentation acceptance as appropriate to inform decisions by the CIO and CPO.

[4] The Privacy Office already has documented procedures for updating the inventory of systems containing personally identifiable information (PII) at least annually.

This plan shall require a multi-year effort to complete. Management shall use FY 2017 to complete its review and acceptance of inventory management data. From FY 2017 through FY 2018, Management shall review and update system definitions, boundaries, and controls so inheritance of controls can be assessed and accepted for use across systems and sub-systems by the CIO, CPO, authorization officials, and system owners as appropriate. The effort shall likely require several steps and coordination with other efforts required by the IT Strategy and Transition Plan.

Expected Completion: Management will develop an action plan within 60 days, with overall completion expected no later than FY18 Q4

OIG Recommendation 2: FY 2016 – 02 – ID.AM

To ensure controls are properly documented and responsibility for control maintenance and testing is identified, FTC should review its information system boundaries and control inheritance practices.

The FTC should complete its evaluation of its system boundaries as it completes its CSAM implementation. FTC should eliminate use of the Minor Application designation and document leveraged/common controls in accordance with NIST RMF guidance and ensure that all FTC systems are covered by an FTC ATO, either specific to the system or under a related system.

Responsible Official: Raghav Vajjhala

Action Plan: Management concurs with this recommendation.

Management notes that this recommendation will be incorporated into much of the work outlined in the first recommendation. Management will address this recommendation through a multi-year action plan to address NIST SP 800-37 Rev.1, A-123, and A-130 employing the discretion within this guidance to create controls that meet the agency's risk assessments and needs.

Further, its proposed action plan will be devised to incorporate and address prior OIG recommendations regarding similar issues from *FY 2015 Evaluation: Opportunities Exist to Accelerate Maturation of the FTC's Information Technology Governance Practices* such as*: ER 16-03, Recommendation 13* for the development of a System Security Plan for the mobile device project.

As the current OIG recommendation notes, recent OMB guidance no longer uses terms such as major and minor applications. Accordingly, Management shall assess and modify its inventory data as appropriate such that it has sufficient information to inform Management's determination

on system boundaries and sub-systems as per NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach". We hope to work with the OIG to shortly close and consolidate the below outdated FISMA report recommendations:

> *AR 15-02 FY 2014 – 04: FTC should revise its process for determining Minor Applications and documenting security controls. Minor Applications should be differentiated from system services/functions and should be documented in a format that supports the ability to assess the security impact of a Minor Application as well as its impact on the associated GSS. SSPs should adequately document control environments so that they can serve as an implementation guideline, a security baseline for testing, and a reference for individuals assessing the level of control compliance.*
>
> *AR 16-02 FY 2015 – 02: FTC should continue its review of Accreditation Boundaries for Minor Applications, re-designating those systems that are significant resource investments or have special security considerations as Major Applications.*

Expected Completion: Management will develop an action plan within 60 days, with overall completion expected no later than FY18 Q4.

OIG Recommendation 3: FY 2016 – 03 – ID.GV, ID.RA

To ensure the rationale for decisions are transparent and auditable, the FTC should document decisions made and the associated risk-based supporting rationale.

The FTC should implement a formal procedure for documenting risk-based decisions as part of the FTC risk management program.

Responsible Official: Raghav Vajjhala and David Rebich

Action Plan: Management concurs with the recommendation.

Management believes that the work it undertook in its current IT Strategy and Transition Plan and its efforts to close all the recommendations in the 2015 OIG evaluation of OCIO has addressed much of the concern voiced in this recommendation. However, Management concurs that documentation of IT governance and the agency's cost-benefit and risk assessment of its IT decision making can be improved.

Management shall address this recommendation through an overall action plan that incorporates guidance on this issue found in OMB circulars A-123 and A-130 within the next 60 days. This action plan shall also address and ideally consolidate or close action plans in response to similar and recent 2016 recommendations in the OIG's *FY 2015 Evaluation: Opportunities Exist to Accelerate Maturation of the FTC's Information Technology Governance Practices*:

> *ER 16-03, Recommendation 2 - Accurately and consistently capture Information Technology Governance Board planning decisions related to business needs and supporting rationales for those decisions. Information documenting Board decisions may be included in separate documentation or meeting minutes.*
>
> *ER 16-03 Recommendation 5 - Require the development of FTC Information Technology and security organizational priorities to guide Governance Board review and approval of projects and investments by identifying and ranking topic areas where information systems or processes need improvement to reduce costs or improve performance; establish risk thresholds by identifying the level of risk of a system failure or data breach that the FTC is willing to tolerate; and periodically review and revise organizational priorities and risk thresholds.*

Expected Completion: Management will develop an action plan within 60 days, with overall completion expected no later than FY 18 Q2

OIG Recommendation 4: FY 2016 – 04 – ID.RA

To ensure that the FTC understands the risks associated with its modernization initiative, FTC should conduct risk analyses from both the individual information system and organization levels (Tier1 and Tier 3).

The FTC should implement a formal risk management program that addresses the requirements of OMB Circulars A-123 and A-130 and the guidance contained in NIST Special Publications 800-30, 800-37, and 800-39. The FTC should conduct risk analyses for its IT Modernization Initiative.

Responsible Official: Raghav Vajjhala and David Rebich

Action Plan: Management concurs with this recommendation.

As noted in the previous recommendation, the agency intends to update its documentation of its

risk management program using the OMB circulars A-123 and A-130 guidance. Management believes that the IT Strategy and Transition Plan largely mitigates the organizational, or Tier 1, risk to availability measures from use of legacy IT in the FTC's data center. Current services hosted in the FTC data center require significant maintenance downtime to meet the agency GPRA target of 99.5% availability whereas leading FedRamped cloud vendors regularly target 99.9%. Management concurs other risks mitigated through projects within the IT Strategy and Transition Plan, such as agency modernization of its litigation services or PIV card integration should also be categorized and monitored appropriately as mission (Tier 2) or system (Tier 3) level risks. Categorization should lead to more effective and timely reporting of variances against desirable thresholds to agency-designated risk officials such as the CIO or the ITGB.

Management shall address this recommendation through an overall action plan to address A-123 and A-130 requirements within the next 60 days as set forth under recommendation 3 above and expects that this plan shall also address and ideally consolidate or close action plans in response to the two recommendations (ER 16 – 03, 2 and 5) found in the OIG IT Governance evaluation.

Expected Completion: Management will develop an action plan within 60 days, with overall completion expected no later than FY 18 Q2

OIG Recommendation 5: FY 2016 – 05 – PR.IP, PR.MA

To ensure IT investments are appropriately planned, funded, executed, and monitored, the FTC should divide its modernization initiatives into segments that provide useful products in relatively short timeframes within a defined Enterprise Architecture.

The FTC should structure modernization activities for acquiring major IT investments as useful segments that can be independently planned, acquired, and monitored.

Responsible Official: Raghav Vajjhala and David Rebich

Action Plan: Management concurs with this recommendation

Management notes and appreciates the OIG's recognition of the segments already identified in the IT Strategy and Transition Plan, and recognizes proper segmentation requires ongoing improvement throughout multi-year lifecycles.

Management shall address this recommendation through an overall action plan to address A-130 requirements for Planning and Budgeting and IT Investment Management within the next 60 days. This plan shall include definition and subsequent completion of an enterprise architecture sufficient to cost effectively meet the mission requirements of the FTC. The plan shall likely

generate recurring reviews and updates every year to the IT Strategy and Transition Plan in accordance with A-130.

Further, Management completed an Acquisition Strategy as part of its IT Strategy and Transition Plan which led to the closure of one of several recommendations from the OIG's *FY 2015 Evaluation Report of the Office of the Chief Information Officer*:

> *Using established Office of Management and Budget, Federal Acquisition Regulation, Federal Acquisition Institute, and other guidance, and in coordination with the development of the IT Strategic Plan, develop an acquisition strategy that reduces the complexity of current procurements and increases stakeholder visibility into contractor performance.*

The IT Strategy and Transition Plan identified a BPA as the mechanism by which stakeholders will receive increased visibility into contractor performance and which reduces overall complexity of current procurements. Since approval of the IT Strategy and Transition Plan, OCIO and Acquisitions have created and released a cloud oriented BPA for bid. In addition to meeting the objectives of the original OIG recommendation, this contract vehicle allows for the flexibility needed to acquire IT services in segmented fashion. Once awarded, the BPA will create a pool of vendors that can become familiar with the FTC enterprise architecture and its vision for future modernization, while also providing for competition of task orders as they arise.

This action plan shall also address and ideally consolidate or close action plans in response to similar and recent OIG recommendations in the *FY 2015 Evaluation: Opportunities Exist to Accelerate Maturation of the FTC's Information Technology Governance Practices* :

> *ER 16-03, Recommendation 1 - Complete applicable Business Case Analysis elements, including a description of security requirements and how they will be met, functional requirements document, Return On Investment (ROI) analysis, and risk assessment; and document instances where a BCA requirement is waived or revised, with supporting justification and risk mitigations. Ensure the BCA considers related FAR requirements.*

> *ER 16-03, Recommendation 3 - Develop and institute standard operating procedures with associated work instructions to support acquisition proposals and decisions, including workflows, milestones, escalation criteria, and project monitoring and tracking procedures.*

ER 16-03, Recommendation 4 - Issue guidance for developing and documenting reliable cost and workload estimates used to support acquisitions. The guidance should include selection and documentation of cost and workload models, development of a basis of estimate that documents procedures used to develop the estimates, and factors affecting estimate reliability.

ER 16-03, Recommendation 6 - Implement an escalation process that promotes, though FTC's continuous monitoring processes, identification of potential performance problems or opportunities for improvement; identifies organizations with the skills and skill levels necessary to research and resolve project issues by problem area and skill level; implements problem tracking from identification to resolution; and establishes timelines for problem resolution and for routine (e.g., weekly, monthly, quarterly) monitoring of compliance with those timelines.

Expected Completion: Management will develop an action plan within 60 days, with a first iteration of updates expected no later than FY18 Q1

OIG Recommendation 6: FY 2016 – 06 – DE.CM

To ensure it has the capability to monitor the health of its security and privacy programs, the FTC should implement a fully compliant ISCM.

The FTC should implement a fully compliant ISCM as described in its ISCM Plan in FY 2013 and its ISCM Strategy, dated November 2014.

Responsible Official: Raghav Vajjhala

Action Plan:Management concurs with this recommendation.

While OIG notes that "the FTC security environment continues to be strong and robust relative to its ability to protect its information assets", OIG also notes and Management agrees that "the FTC information security program relies on legacy systems and manual controls to protect its information assets."

To move towards continuous monitoring, Management has already procured and installed monitoring tools in its environment to cover the many components identified in NIST 800-137 Appendix D regarding ISCM. Management shall now focus on the documentation and implementation of configurations necessary to automate monitoring and reduce the reliance on manual controls.

Lastly, the text preceding the recommendation in the OIG's report implies that ISCM also addresses privacy. Management contends that continuous monitoring for Privacy controls exists as a separate discipline.

A-130 defines information security continuous monitoring as:

> …maintaining ongoing awareness of information security, vulnerabilities, threats, and incidents to support agency risk management decisions.

A-130 defines privacy continuous monitoring separately as:

> …maintaining ongoing awareness of privacy risks and assessing privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks.

Regarding privacy and information security continuous monitoring, A-130 states that Agencies shall:

> Conduct and document security and privacy control assessments prior to the operation of an information system, and periodically thereafter, consistent with the frequency defined in the agency information security continuous monitoring (ISCM) and privacy continuous monitoring (PCM) strategies and the agency risk tolerance;

Otherwise, Management has already started the process of reviewing the Information Security Continuous Monitoring (ISCM) strategy and plan. Additionally OCIO will update the ISCM documentation where necessary. OCIO will implement ISCM as described in its updated ISCM documentation.

Expected Completion: Management will develop an action plan within 60 days, with overall completion expected no later than FY18 Q1

OIG Recommendation 7: FY 2016 – 07 – DE.CM

To ensure that the POA&M is the consolidated tracking tool required by OMB, FTC should revise and update its POA&M procedures.

The FTC should revise its POA&M process and content to ensure it meets OMB information requirements (e.g., all security weaknesses found, and in need of remediation, during any assessment done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments) and can be an effective, authoritative, agency-wide management tool.

Responsible Official: Raghav Vajjhala

Action Plan: Management concurs with this recommendation.

Management recognizes its practices in sharing information on POA&Ms requires ongoing monitoring. However, Management also notes that historic practices have been sufficient for tracking actions on specific systems; the OIG rated the FTC's practices as "Met" in response to FY 2016 IG Reporting Metrics Indicator 1.1.14:

> Centrally tracks, maintains, and independently reviews/validates POA&M activities at least quarterly. (NIST SP 800-53 :CA-5; OMB M-04-25)

Management shall address this recommendation through an overall action plan to address A-123 and A-130 within the next 60 days. This action plan shall also address and ideally consolidate or close action plans in response to similar and recent recommendations in the OIG's *FY 2015 Evaluation: Opportunities Exist to Accelerate Maturation of the FTC's Information Technology Governance Practices*:

> *ER 16-03, Recommendation 2 - Accurately and consistently capture Information Technology Governance Board planning decisions related to business needs and supporting rationales for those decisions. Information documenting Board decisions may be included in separate documentation or meeting minutes.*
>
> *ER 16-03 Recommendation 5 - Require the development of FTC Information Technology and security organizational priorities to guide Governance Board review and approval of projects and investments by identifying and ranking topic areas where information systems or processes need improvement to reduce costs or improve performance; establish risk thresholds by identifying the level of risk of a system failure or data breach that the FTC is willing to tolerate; and periodically review and revise organizational priorities and risk thresholds.*

Expected Completion: Management will develop an action plan within 60 days, with overall completion expected no later than FY 18 Q2

OIG Recommendation 8: FY 2016 – 08 – RC.RP

To minimize the potential for and disruption from both short and long-term outages, the FTC should institute a continuing contingency planning capability.

The FTC should develop viable contingency plans for the HQ data center and hosted applications. Plans should be tested to ensure viability and ensure staff are trained to execute them. Contingency plans should clearly define actions to be performed and individuals responsible for plan activation and other critical decisions should be identified.

Responsible Official: Raghav Vajjhala

Action Plan: Management concurs with this recommendation.

Management's approach to contingency planning is based on a pragmatic assessment of the options available for minimizing the potential for and disruption from both short and long-term outages. Given the agency's limited resources, it has been Management's long-standing decision to accept the risks associated with a datacenter outage in our HQ facility while we work to incrementally improve our exisiting capabilities, and to identify more permanent and sustainable options to cost-effectively migrate to a different environment. To this end, the FTC's IT Strategy and Transition Plan focuses on the cloud, which will enable the FTC to not only improve our ability to avoid major outages, but will serve to increase the availability of core services throughout the year.

For example, fundamental to minimizing disruption from outages is the prevention of outages in the first place. Current target service levels of 99.5% uptime fall short of targets for federally secured cloud services at 99.9% uptime - hence the direction towards cloud services in the FTC IT Strategy and Transition Plan.

As to the recent outage noted in the OIG's narrative, Management has already alerted the OIG to the infrastructure operations as the root cause to many issues per its response to OIG's *FY 2015 Evaluation: Opportunities Exist to Accelerate Maturation of the FTC's Information Technology Governance Practices*[5]. The outage events reference analysis documented by the OCIO staff and shared with the IT Governance Board (ITGB). The analysis echoed concerns on day-to-day infrastructure operations and reinforced the need to prioritize resources towards adoption of mor reliable and available cloud services.

In addition, the FTC ITGB reviewed and approved a Business Impact Assessment (BIA) and Disaster Recovery Techstat in April 2016. The corresponding memo stated cloud services as the preferred strategy and reiterated concerns that building a DR solution for all services in an

[5] From the Management Response to OIG's *FY 2015 Evaluation: Opportunities Exist to Accelerate Maturation of the FTC's Information Technology Governance Practices*: "limitations in current infrastructure operations greatly impede the ability of the FTC to adopt emerging technology"

alternate data center (ADC) would lead to a cost prohibitive risk management approach. This memo was provided to the OIG.

Management appreciates theOIG's comments on these plans, takes seriously the feedback provided, and notes that the OIG rated the FTC's practices as "Met" in response to FY 2016 IG Reporting Metrics Indicator 5.1.2:

> Incorporates the system's Business Impact Analysis and Business Process Analysis into analysis and strategy toward development of the organization's Continuity of Operations Plan, Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). (NIST SP 800-34)

Importantly, Management already has released acquisition vehicles that target use of federally secured cloud service to both improve availability and mitigate risks associated with current services. Access to vendors with the capability to process FTC data at alternate facilities materially mitigates the FTC's need to establish and maintain a fully redundant alternate data center of its own.

Management shall address this recommendation through an overall action plan within the next 60 days. This action plan shall also address and ideally consolidate or close action plans in response to prior OIG recommendations:

> *AR 15-02, FY 2014 – 06 - FTC should develop a disaster recovery strategy and implementation plan.*

In terms of immediate updates to its documentation, Management shall prioritize assessment of supply chain risks identified in the OIG's CyberScope assessment. The OIG rated as "Not Met" for FY 2016 IG Reporting Metrics describes Indicator 5.1.10:

> Contingency planning that considers supply chain threats.

The OIG supported its rating of "Not Met" with the following comment:

> *Supply chain threats are minimal for FTC but they still need to be considered.*

With a "Met" rating on assessment of supply chain risk, Cyberscope would have scored the FTC as a "3" for Recover based on OIG ratings elsewhere for the Recover Function. Work still remains to achieve a "4", but supply chain assessments act as a prerequisite for further maturity model scoring.

Expected Completion: Management will develop an action plan within 60 days, with overall completion expected no later than FY 18 Q4

Office of Inspector General

OIG OBSERVATIONS ABOUT MANAGMENT'S OFFICIAL RESPONSE

We are pleased that management concurred in the eight recommendations set forth in our report; however, we note the following areas of concern that potentially could affect the FTC's ability to effectively implement our recommendations.

AREAS OF CONCERN:

1. **As of September 30, 2016, the FTC had not completed replacement of its legacy inventory system and was unable to provide a comprehensive inventory of its information assets – a foundational element of information security and policy.**

   OIG Recommendations FY 2016 – 02 and FY 2016 – 01 recommend completion and improvement of the FTC's system and information holdings inventory. In its response, management focuses on the change in terminology used in the revised OMB Circular A-130, rather than on the need to review all FTC systems previously designated as "Minor Applications" and document all information systems in accordance with the new NIST approach in SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* (RMF).

   To ensure OMB Circular A-130 and NIST requirements are met and that the FTC's information assets are protected with suitable controls, the FTC must promptly review applications previously identified as Minor Applications and document their baseline controls in appropriate artifacts. All FTC systems (i.e., any system or discrete subsystem supporting the FTC, regardless of acquisition method or implementation approach) should be included in the systems inventory. Further, the inventory should support monitoring of FTC information holdings, as required under new National Archives and Records Administration (NARA) guidance and existing privacy requirements.

2. **While management states its new action plan will comply with OMB Circulars A-130 and A-123, unless its action plans commit to intermediate milestones identified in the OIG's specific recommendations, the risk of impact to FTC information security could deteriorate from "moderate."**

   Compliance with OMB Circulars is a continuing process that will require a multi-year effort to achieve baseline requirements. Subsuming OIG recommendations as general

guidance for the FTC's longer term information security efforts would effectively nullify the OIG's critical recommendations to improve the FTC's information security posture. For example, Recommendation FY 2016 – 01 recommends that the FTC complete and document its information system inventory. If improvement of the systems inventory is subsumed into the general OMB policy compliance activities, the Office of the Chief Information Officer (OCIO) will not be able to properly document its corrective actions as Plan of Action and Milestones (POA&M) items and Investment Decisions, as required by OMB and NIST guidance. Further, if improvement of the systems inventory is deferred, in addition to increasing security risk, the FTC's CyberScope score will be reduced in FY 2017 because maintenance of a complete, comprehensive inventory of information assets is a fundamental component of DHS FISMA CyberScope metrics.

Critically, as we state in connection with Recommendations FY 2016 – 04, FY 2016 – 05, and ER Recommendation 4, the FTC needs to improve its capability to plan, estimate costs and workloads, and evaluate risk associated with its IT investments and then monitor those investments to completion. By suggesting that it will defer implementation of OIG recommendations until it proceeds with the multi-year effort to address OMB guidance, management risks a situation in which significant, imminent IT Modernization efforts cannot be monitored or effectively managed. In accordance with OMB Circular A-130, management should prioritize information security and privacy improvements through *a risk-based approach* that would also include addressing Cross Agency Priority (CAP) goals as a priority. Management's response does not identify development of a risk management program with associated risk thresholds and consistent analysis processes as a precursor to the risk-based analysis needed for the multiple technological and acquisition decisions that will need to be made as part of FTC's IT Modernization initiative. Without risk-based decisions, FTC management will not be assured that its decisions are effectively balancing the competing objectives of minimizing cost while maximizing performance and security.

3. **The FTC has not performed a risk analysis to support the technological approach or the acquisition method used for the IT Modernization effort.**

   Reasonable and consistent evaluation of risk and documenting those risks and FTC mitigation efforts are crucial elements in OMB, DHS, NIST, and NARA guidance for maintaining effective security of federal information assets. OIG recommended implementing a formal risk management program and conducting risk analyses for the *IT Modernization and Transition Plan* initiatives. Management appears to commit only to improving documentation of its risk management program, not to implementing a formal program or to performing the recommended risk analyses. Instead, management assumes that the discussion of risk is adequately addressed in the *IT Strategy and Transition Plan*.

   As noted in the body of our report, management makes only limited reference to risk analysis and mitigation actions in the *IT Strategy and Transition Plan*. The Plan identified the Chief Information Security Officer as the individual assigned responsibility for ensuring that risk is properly documented and reported to the Commission, and that risk tolerance is defined. However, the *IT Strategy and Transition Plan* did not properly describe or provide risk-based support for the alternative technological and acquisition

approaches selected for implementation. Further, the Plan identified several other areas that will require risk-based analyses to support modernization decisions, including selection of the contracting methodology; a Business Process Re-engineering (BPR) review to assess current mission needs and evaluate technology solutions to meet future needs; policies and standard operating procedures that will change FTC to a proactive risk-based, continuous prevention and monitoring posture versus inspecting for compliance; and selection of alternative investments that will most likely lead to improved customer experience.

To fully and effectively address the OIG's recommendations, management will need to implement a formal risk management program in accordance with OMB and NIST requirements and apply that process to the multiple decisions that will need to be made as part of its IT investment process and the IT Modernization effort.

4. **The FTC does not commit to segmenting its modernization efforts into interrelated segments, under an Enterprise Architecture, that can be individually planned, monitored, and implemented.**

   Management proposes to develop within 60 days one action plan to address all OMB Circular A-130 requirements for Planning and Budgeting and IT Investment Management. Management anticipates that it may have to make changes to its *IT Strategy and Transition Plan*. This implies that management assumes that the *IT Strategy and Transition Plan* includes an Enterprise Architecture. This assumption is incorrect. The *IT Strategy and Transition Plan* does not include an Enterprise Architecture, nor its associated Security Architecture.

   In OMB Circular A-130, OMB defines an enterprise architecture as follows:

   > 'Enterprise architecture' (a) means – (i) a strategic information asset base, which defines the mission; (ii) the information necessary to perform the mission; (iii) the technologies necessary to perform the mission; and (iv) the transitional processes for implementing new technologies in response to changing mission needs; and (b) includes – (i) a baseline architecture; (ii) a target architecture; and (iii) a sequencing plan (44 U.S.C. § 3601).

   Section 2.4 of the FTC's *IT Strategy and Transition Plan* clearly shows that the focus of the strategy is FTC Headquarters Data Center operations. While this Current State Architecture names externally-hosted applications, it does not show the security architecture, the communications network structure, or the external connectivity that supports FTC missions. Without a complete Enterprise Architecture, the FTC will not be able to implement or effectively maintain the Risk Management Framework, envisioned by NIST guidance: –

   > An effective implementation of the Risk Management Framework ensures that managing information system-related risks is consistent with the agency's mission or business objectives and overall risk management strategy, and risk tolerance established by the senior leadership through the risk executive function as discussed in NIST SP 800-39. It also ensures that the requisite security and

privacy requirements and controls are integrated into the agency's Enterprise Architecture and system development life cycle processes. Finally, the Risk Management Framework supports consistent, well-informed, and ongoing authorization decisions, transparency of risk management information, reciprocity, and information sharing.

OMB recognizes in Circular A-130 that a primary value of an Enterprise Architecture is the planning process as well as the artifacts developed, with the statement that –

> The process of describing the current and future state of the agency, and laying out a plan for transitioning from the current state to the desired future state, helps agencies to eliminate waste and duplication, increase shared services, close performance gaps, and promote engagement among Government, industry, and citizens.

The FTC is apparently planning to complete its modernization without an underlying structure. This approach has a high-performance risk because, without an Enterprise Architecture and associated Security Architecture, contracts will continue to be issued without consideration for integration across all areas of IT services; contractor development could become an inherently governmental function if not properly managed; and the capability to identify and assess the impact of single-points-of-failure will be reduced.

The OIG welcomes the opportunity to continue to work with FTC management to discuss our concerns with management's mitigation approach.

Contact the OIG

Promote integrity, economy, & efficiency
Report suspected fraud, waste,
abuse or mismangement

(202) 326-2034
Fax (202) 326-2034
OIG@ftc.gov

600 Pennsylvania Avenue, NW. CC-5206
Washington DC 20580

Complaints may be made anonymously.

Any information you provide will be held in confidence. However, providing your name and means of communicating with you may enhance our ability to investigate

FINAL REPORT
REDACTED FOR PUBLIC RELEASE