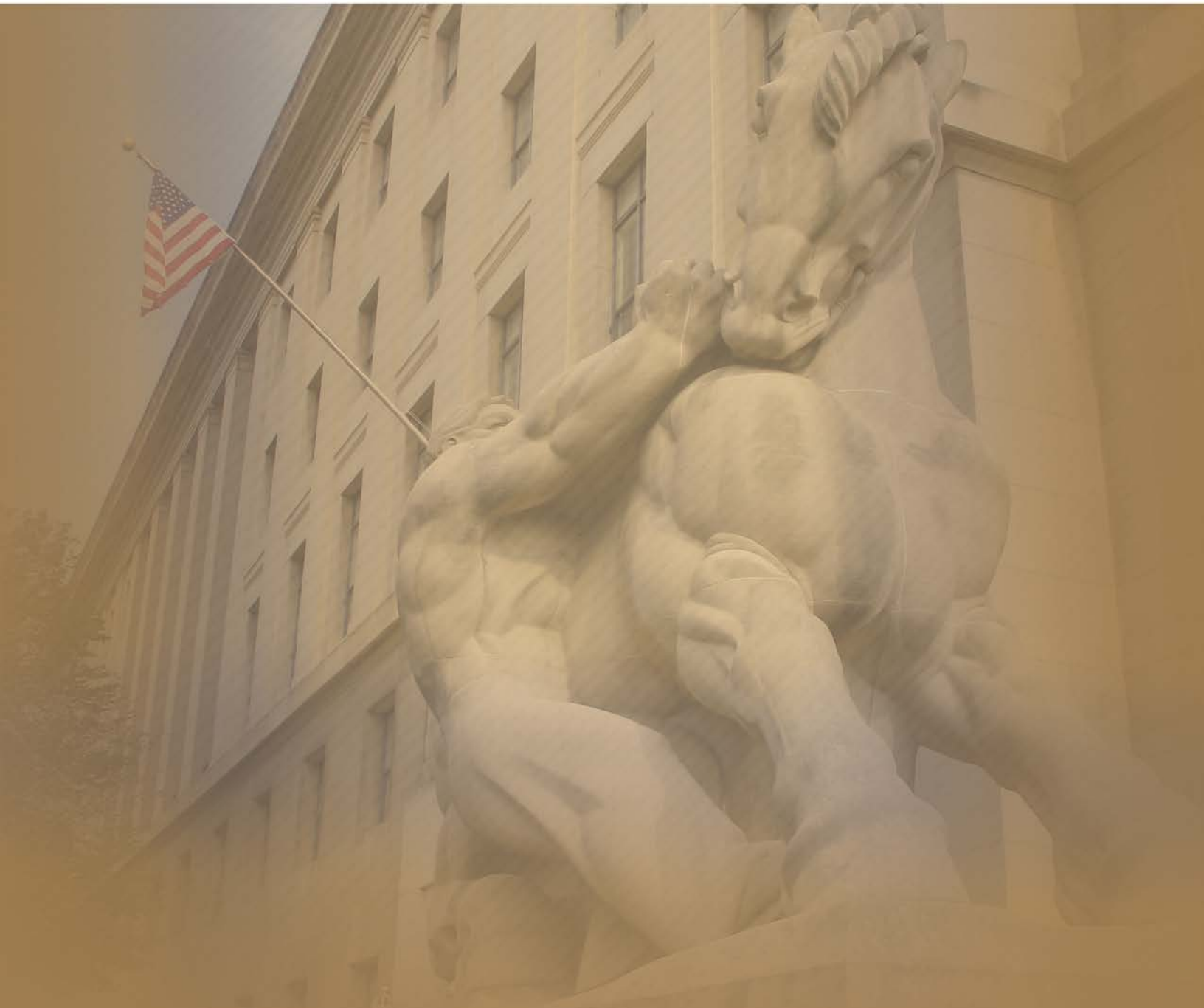
OIG Independent Evaluation

of the Federal Trade Commission's
Information Security Program and Practices for Fiscal Year 2015

Report No. AR 16-02 // March 2016



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

Office of Inspector General

February 29, 2016

MEMORANDUM

TO: Chairwoman Edith Ramirez
Commissioner Julie Brill
Commissioner Maureen K. Ohlhausen
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 Modernization Act for Fiscal Year 2015

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) 2015.

The FY 2015 evaluation showed that FTC security and privacy programs are robust, demonstrating their ability to protect FTC assets while undergoing significant organizational, physical, and technological change. As required, this report uses an assessment approach that focuses on program effectiveness instead of compliance. For the first time, it also uses the maturity model developed by the Council of Inspectors General on Integrity and Efficiency (CIGIE). This year, the CIGIE maturity model addressed the Continuous Monitoring Management topic area. In future years, the maturity model approach will be used for the remaining topic areas addressed by FISMA reviews.

The evaluation identifies opportunities for improvement and makes seven new recommendations: three to improve information security planning and monitoring; three to improve program operations; and one to ensure that the security of technology support provided from outside sources is equivalent to the security provided by FTC in-house systems. Additionally, the recommendations address the need for improved performance measurement techniques.

The Office of the Chief Information Officer (OCIO) agreed with the OIG's assessment and recommendations for improvement. The OCIO provided action plans to address each of the recommendations, with scheduled completion dates through the second Quarter of FY 2017. Management's comments are included in the Executive Summary and in Exhibit 16. The OIG concurs that OCIO actions taken and planned will improve FTC security, and we will examine the effectiveness of these improvements as part of the FY 2016 FISMA evaluation. We also will continue to monitor management progress in implementing open recommendations from previous FISMA reporting.

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

Should you have any questions or concerns, please do not hesitate to contact me or Mary Harmison.

cc: Heather Hippsley, Chief of Staff
David Robbins, Executive Director
David Shonka, Principal Deputy General Counsel
Patricia Bak, Deputy Executive Director
Monique Fortenberry, Deputy Executive Director
Jeffrey Smith, Assistant Director for Information Assurance
Katherine Brin, Chief Privacy Officer
David Rebich, Chief Financial Officer and Performance Improvement Officer
Valerie Green, Deputy Chief Financial Officer and Deputy Performance Improvement Officer
Raghav Vajjhala, Chief Information Officer

FISCAL YEAR 2015
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

February 26, 2016

Submitted by:

ManTech/Allied Technology Group, Inc.
2250 Corporate Park Drive, Suite 100
Herndon, Virginia 20171
Order Number: FTC11G1068 Requisition Number: 29-20869

EXECUTIVE SUMMARY

The Federal Trade Commission (FTC) is an independent federal government law enforcement and regulatory agency authorized to promote and protect consumer welfare through its jurisdiction over consumer protection and competition issues. FTC authorizing statutes are designed to promote competition and to protect the public from unfair and deceptive acts and practices in or affecting commerce. For example, in Fiscal Year (FY) 2015, FTC returned $444,000 to consumers who lost money to a business directory scam; settled an action against Sprint where the telecommunications company will pay a $2.5 million civil penalty to settle FTC charges that it violated the Fair Credit Reporting Act; obtained 13 settlements with companies, prohibiting them from misrepresenting the extent to which they participate in any privacy or data security program sponsored by the government or other self-regulatory or standard-setting organization; took enforcement action against a number of companies that accessed customer contact data without permission, violated consumers' privacy rights, or misled customers by failing to maintain security for sensitive consumer information, in violation of the FTC Act; and provided guidance to companies for building security into their products and services.

The Commission also issues guidance on techniques to protect consumers against identity theft or compromise of their personal information, avoid scams, address cyberbullying, and securely use the Internet. The Commission also protects consumer privacy under the Fair Credit Reporting Act and the Children's Online Privacy Protection Act and investigates mergers and practices harmful to competition.

FTC responsibilities require the accumulation of significant quantities of data, much of which is voluntarily provided, including sensitive personal, commercial, or financial information, in both digital and hard copy formats. The Commission also relies on automated files and records to pay its employees and vendors, process personnel transactions, and perform other "housekeeping" and administrative functions. All these systems collect or maintain information from FTC staff and contractors, commercial organizations, and the general public – information that must be protected from unauthorized (intentional or unintentional) access or alteration.

The FTC threat profile is continuously changing. Changes in technologies and applications introduce new vulnerabilities; FTC investigations and decisions on both competition and consumer protection matters increase the number of organizations and individuals who may seek to disrupt or compromise FTC operations; and resource limitations may have the potential to restrict FTC capabilities to identify and quickly respond to potential threats and vulnerabilities.

To increase agency capabilities to maintain effective security while restraining costs, the Office of Management and Budget and the National Institute of Standards and Technology (NIST),

under the Federal Information Security Modernization Act of 2014[1] (FISMA), provide guidance to help federal agencies establish risk-based processes to prioritize vulnerabilities and available resources and to establish a continuous monitoring program for assessing control effectiveness. The NIST emphasis on risk seeks to provide management with the tools necessary to ensure protection of information assets while maximizing use of scarce resources.

FISMA provides a comprehensive framework for ensuring the effectiveness of technical, administrative, and physical security controls over information resources that support federal operations and assets. FISMA requires an annual evaluation of compliance with requirements and related information security policies, procedures, standards, and guidelines. The evaluations provide senior management and others with the information needed to determine the effectiveness of security programs, ensure the confidentiality and integrity of data entrusted to the FTC, and to develop strategies and best practices for cost effectively improving information security.

The FTC continues to evolve its information security program toward the NIST risk-based model. At the end of FY 2011, FTC chartered Information Technology (IT) governance boards to monitor IT planning, match FTC information security control measures to its threat profile, and allocate resources to mitigate identified vulnerabilities.

In FY 2015, the Department of Homeland Security (DHS) directed Inspectors General (IG) to use a maturity model developed by the Council of the Inspectors General on Integrity and Efficiency (CIGIE) as the criteria for the annual FISMA evaluation. In this initial application, the approach is applied to the Continuous Monitoring Management topic area. Continuous Monitoring Management is a critical FISMA metric area because it has the broadest coverage scope and includes the foundation elements of effective information security and privacy control, assessed in three model domains (People, Processes, and Technology) at five maturity levels (1-Ad-hoc, 2-Defined, 3-Consistently Implemented, 4-Managed and Measurable, and 5-Optimized).[2] While FTC continuous monitoring activities have not specifically addressed the new maturity model criteria, they did follow the same concept (i.e., evolving from ad-hoc processes to a formalized model that is consistently applied, sufficiently robust to securely accommodate change, with measured results to support risk-based decision-making).

[1] The Federal Information Security Management Act of 2002 (FISMA) was replaced by the Federal Information Security Modernization Act of 2014 (FISMA)

[2] To reach a particular level of maturity, organizations should meet all of the attributes outlined in for that respective level. For instance, to reach a Level 2 for the "people" domain, an organization should meet attributes of Level 1. Similarly, to reach Level 2 for the ISCM program overall, organizations should meet attributes for both Level 1 and Level 2. When determining the overall maturity level, the lowest common denominator approach applies. For instance, if an organization is at Level 1 for the "people" domain but is at Level 3 for both the "processes" and "technology" domains, the overall maturity of the organization's ISCM program would be Level 1.

The FTC Office of the Inspector General (OIG) evaluated the capability of FTC information security and privacy programs to protect information assets and its level of adherence to FISMA requirements and OMB and NIST policy and guidance.

The FY 2015 evaluation showed that the FTC security and privacy programs are robust, demonstrating their ability to protect Commission assets while undergoing significant organizational, physical, and technological change. The programs benefit from the agency's small size, the technical competence of its staff, and the workforce's in-depth understanding of the need to protect information assets if FTC missions are to be completed.

The evaluation also identified areas where FTC security and privacy programs can be improved. As shown in the recommendations for improvement in EXHIBIT E-1, 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 practices.

Deficiencies in security planning have resulted in delayed implementation of security controls and the inability to clearly show that technological changes are accomplished and result in reduced risk. The lack of attention to detail has resulted in security artifacts that are inaccurate, incomplete, and do not satisfy their objectives (e.g., do not clearly define security controls).

Currently, the security program deficiencies have not adversely affected the capability of the FTC to protect its information assets. This has been due to the FTC workforce focus on asset protection and its low staff turnover. This compensating countermeasure cannot, however, be expected to continue for the long-term. Further, FTC efforts to accelerate modernization of its IT capabilities and the increasing volume and sensitivity of FTC information assets will stress FTC systems when preventing cyber-attacks. Continuing improvement while maintaining effective security will require increased emphasis on planning, Configuration Management, and attention to detail.

Over the past three years, OIG FISMA evaluations resulted in the same conclusions: FTC security and privacy programs are sufficiently comprehensive to protect the confidentiality, integrity, and availability of FTC information assets; FTC responds quickly to mitigate identified specific vulnerabilities and threats; and concern for security and privacy is embedded throughout the workforce. For example, in FY 2013, OIG made seven recommendations for improvement; since then, six were closed or consolidated into subsequent related recommendations. In FY 2014, OIG made six recommendations, three were closed and three remain open. In addition, we note that recommended improvements in its governance practices now provide the information necessary to identify and correct problem projects.

The FISMA evaluations also recommended improvements in governance and oversight to institutionalize security and privacy programs; increasing program maturity, consistency, and reporting. While response to the governance and oversight recommendations has been positive, progress has been slow and inconsistent, evidenced by the delay in implementing effective metrics and monitoring techniques, inconsistent compliance with planning and acquisition policies and procedures, and deficiencies in documenting decisions.

FTC needs to increase its efforts to institutionalize and mature its information security and privacy programs.

EXHIBIT E- 1: FY2015 FTC OIG FISMA Evaluation Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[3]
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
FY 2015 – 02: FTC Security Policy and Procedures/System Accreditation Boundaries	6.1.2	FTC should continue its review of Accreditation Boundaries for Minor Applications, re-designating those systems that are significant resource investments or have special	Moderate	Management concurs and has completed the installation of the Cyber Security Assessment and Management (CSAM) tool to assist in documenting our Accreditation Boundaries. Planned actions for FY16 include:

[3] OCIO comments are presented as provided.

EXHIBIT E- 1: FY2015 FTC OIG FISMA Evaluation Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[3]
		security considerations as Major Applications.		• Continue review of Accreditation Boundaries. • Based on the results of the review, designate new Minor and Major FISMA applications. **Expected Completion Date**: FY2017 Q1
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
FY 2015 – 04: Privacy	6.1.4	FTC should elevate the Chief Privacy Officer to be a full voting member of the ITGB. (Also see recommendation FY 2015 – 01 regarding organization of the governance boards)	Moderate	Management concurs. Planned actions for FY16 include: • Elevate the Chief Privacy Officer to be a full voting member of the ITGB. **Expected Completion Date**: FY2016 Q2
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. • 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 /	6.3	FTC should focus on achieving full compliance with PIV-enabled I&A so that compliance is not	Moderate	Management concurs and has enabled logical PIV access for all administrators and select users on a test basis. The technical infrastructure

EXHIBIT E- 1: FY2015 FTC OIG FISMA Evaluation Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[3]
Remote Access Management		subject to continuing delay and PIV compliance is maintained as new technologies and contracting approaches are added as part of FTC's modernization efforts.		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. • 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 Datacenter 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.

EXHIBIT E- 1: FY2015 FTC OIG FISMA Evaluation Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[3]
				• Assess current custom user performance-measuring tool. Based on the results of the 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

Table of Contents

List of Exhibits

List of Acronyms

Acronym	Definition
BCA	Business Case Analysis (analogous to BIA)
BIA	Business Impact Analysis (analogous to BCA)
C&A	Certification and Accreditation
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
DRP	Disaster Recovery Plan
DHS	Department of Homeland Security
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

List of Acronyms

Acronym	Definition
ITGB	IT Governance Board
ITMO	Information Technology Management Office (now OCIO)
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
PII	Personally Identifiable Information
POAM	Plan of Action and Milestones (also POA&M)
PSC	Privacy Steering Committee
SIEM	Security Information and Event Management
TSD	Task Solution Document

1. BACKGROUND

The Federal Trade Commission (FTC) is an independent federal government law enforcement and regulatory agency authorized to promote and protect consumer welfare through its jurisdiction over consumer protection and competition issues. FTC authorizing statutes are designed to promote competition and to protect the public from unfair and deceptive acts and practices in or affecting commerce. For example, in Fiscal Year (FY) 2015, FTC returned $444,000 to consumers who lost money to a business directory scam; settled an action against Sprint where the telecommunications company will pay a $2.5 million civil penalty to settle FTC charges that it violated the Fair Credit Reporting Act; obtaining 13 settlements with companies where the companies are prohibited from misrepresenting the extent to which they participate in any privacy or data security program sponsored by the government or other self-regulatory or standard-setting organization; took enforcement action against a number of companies that accessed customer contact data without permission, violated consumers' privacy rights, or misled customers by failing to maintain security for sensitive consumer information, in violation of the FTC Act; and provided guidance to companies regarding approaches to build security into their products and services.

The FTC also issues guidance regarding techniques to protect consumers against identity theft and compromise of the privacy of their personal information. For example, FTC provides information to help consumers –

- Avoid Scams – tips to help consumers avoid websites that seek to obtain a consumer's personal information (e.g., phishing);
- Protect their children – tips for dealing with cyberbullying and how children can more safely use Internet social networking sites;
- Safely engage in Internet commerce; and
- Protect their computers from damage or loss from attacks through network attachments or malicious software.

Privacy is a central element of the FTC's consumer protection mission and a potential element in its competition mission. 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 has implemented 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 provided 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.

FTC responsibilities require the accumulation of significant quantities of data, much of which is sensitive personal, commercial, or financial. FTC uses information technology (IT) to collect, store, and process its information assets. IT systems assist FTC staff in conducting their law enforcement and management efforts; helping distribute settlements to consumers injured by unfair or deceptive acts or practices; maintain information about individuals who want to avoid contact by telemarketers; prepare and pursue legal actions against individuals and organizations engaged in unfair or deceptive acts or practices; and examine proposed company merger data to identify potential antitrust or reduced competition concerns. The FTC also relies on automated files and records to pay its employees and vendors, process personnel transactions, and perform other "housekeeping" and administrative functions. All these systems collect or maintain information from FTC staff and contractors, commercial organizations, and the general public—information that must be protected from unauthorized (intentional or unintentional) access or alteration.

FTC often works with other agencies such as the Department of Justice (DOJ) and the Department of Commerce (DOC). In some cases, this necessitates information sharing of mission-related data and may require interconnection of FTC networks. For administrative functions FTC connects with and shares information with agencies such as the Department of Interior (DOI) and the Office of Personnel Management (OPM). These interconnections and information sharing arrangements are risk areas that require specific FTC administrative and technical controls.

The FTC threat profile is continuously changing. New technologies and applications introduce new vulnerabilities; FTC investigations and decisions on both competition and consumer protection matters increase the number of organizations and individuals who may seek to disrupt or compromise FTC operations, and resource limitations (staff, technology, or budget) have the potential to restrict FTC capabilities to quickly identify and respond to potential threats and vulnerabilities. To increase agency capabilities to maintain effective security while constraining costs, the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST), under the Federal Information Security Modernization Act of 2014[4] (FISMA), provide guidance to help federal agencies establish risk-based processes to prioritize vulnerabilities and available resources, and to establish a continuous monitoring program where the frequency of control effectiveness is evaluated based on the potential failure risk. The NIST emphasis on risk is intended to provide agency management with the tools necessary to ensure protection of information assets while maximizing use of scarce resources.

[4] The Federal Information Security Management Act of 2002 (FISMA) was replaced by the Federal Information Security Modernization Act of 2014 (FISMA).

In addition to an emphasis on risk identification and management, the NIST security model provides for establishment of security performance metrics and continuous monitoring of those metrics, i.e., an Information System Continuous Monitoring (ISCM) system. In coordination with OMB, the Federal Chief Information Officer's Council (CIOC) and the Committee on National Security Systems (CNSS) established the Joint Continuous Monitoring Working Group (JCMWG), which developed the United States Government Concept of Operations (CONOPS) for Information Security Continuous Monitoring (ISCM). This CONOPS supplements NIST guidelines by providing a roadmap and more specific implementation guidance to stakeholders across the federal government.

In Memorandum M-14-03, OMB directed Departments and Agencies (D/A) to implement a continuous monitoring program by the end of FY 2017. To that end, D/A were required to develop and begin implementation of a continuous monitoring strategy by November 2014.

As security and privacy control environments evolve, OMB and DHS, working through CIGIE, is developing cross-government approaches for examining their effectiveness and status of information security and privacy programs. These evaluation approaches are to provide guidance to D/A in implementing their ISCM solutions and to Inspector Generals (IG) in assessing them. IGs used the first phase of the new evaluation approach in conducting the FY 2015 independent FISMA assessments.

FTC continues to evolve its information security program toward the NIST risk-based model. At the end of FY 2011, FTC established a risk-based information security program by chartering IT governance boards. These boards are responsible for monitoring IT planning and matching FTC information security control measures to its threat profile, and allocating resources to mitigate identified vulnerabilities. In FY 2014, the scope of the FTC governance boards evolved as board members recognized the need to evaluate IT initiatives based on their organizational risk as well as dollar value (i.e., a low-cost IT investment could result in a significant FTC mission risk). In FY 2015, FTC developed work instructions (operating procedures) for the governance boards.

The FTC enables access to information in FTC systems and systems functionality to FTC employees, including FTC contractors, based on their organizational roles. The FTC may provide controlled access to its systems or the information in its systems to other agencies (e.g., DOJ, Federal Deposit Insurance Corporation, Department of Education, DHS, and DOI). The public may access most of the FTC's public records on a read-only basis via the Internet, such as reports describing Commission actions, descriptions of FTC cases and proceedings, information regarding the FTC refund and pre-merger programs, and procedures for filing complaints and participating in the DO-NOT-Call program.

FTC obtains IT resources using a variety of commercial and government sources to support its multiple missions: FTC maintains a datacenter to support its internal infrastructure; contracts to obtain IT resources to support applications designed and/or operated by its staff (e.g., cloud

computing capabilities); and contracts for business functions offered as an independent service (i.e., applications as a service). Contracted applications may include development, operation, and maintenance of an IT capability specifically for the FTC (e.g., "do not call list") or an application where FTC is only one of many users (e.g., payroll and accounting). FTC information security policies and procedures must address protection of its information assets regardless of the nature of those resources, where those resources are located, or how users access those resources.

The FTC Office of the Chief Information Officer (OCIO) is responsible for the technological infrastructure and the information systems that provide the agency with the tools and the data needed to conduct and manage its consumer protection and competition missions. Responsibility for maintaining the security of specific business area applications is assigned to senior agency officials in FTC Bureaus and offices.[5] Responsibility for establishing and maintaining the FTC information assurance/security[6] program is assigned to the Chief Information Officer (CIO) who "assigns and directs the activities of the Chief Information Security Officer" (CISO) to carry-out those responsibilities.[7] Responsibility for the FTC Privacy Program is assigned to the Chief Privacy Officer (CPO), who reports to the FTC Chairwoman. [8]

FISMA provides a comprehensive framework designed to ensure the effectiveness of technical, administrative, and physical security controls over information resources that support Federal operations and assets. FISMA requires an annual independent evaluation of compliance with requirements and related information security policies, procedures, standards, and guidelines. The evaluation provides agency senior management and others with the information needed to determine the effectiveness of overall security programs, ensure the confidentiality and integrity of data entrusted to the FTC, and to develop strategies and best practices for cost effectively improving information security.

DHS and OMB[9] provide guidance for conducting the annual FISMA evaluations. FISMA reporting guidance stresses that the FISMA evaluation objective is to improve the capability of federal agencies to protect their information assets (hardware, software, and data).

The annual FISMA evaluation is divided into two parts: 1) responses to specific performance metrics developed by the DHS and submitted by the CIO, the Office of Inspector General (OIG),

[5] Delegation of Authority for FTC Information Technology Security Program from Jon Leibowitz, Chairman FTC, September 2009.

[6] FISMA refers to information assurance, while NIST and OMB guidance refers to both information security and information assurance. In this evaluation, the terms "information assurance" and "information security" are synonymous.

[7] FTC Administrative Manual (December 2011), Chapter 1: Section 550 - Computer Security, Part 1, Paragraph 3.A FTC Information Security Handbook Volume 1 – Revised 9/27/2011 Sections 3.1 & 3.4.

[8] The FTC Chief Privacy Officer coordinates efforts to implement and review the agency's policies and procedures for safeguarding all sensitive information and chairs the FTC's Privacy Steering Committee and the Breach Notification Response Team. See Announcement by Federal Trade Commission Chairman Jon Leibowitz 11/13/2012.

[9] The DHS role was formalized with enactment of the Federal Information Security Modernization Act of 2014.

and the Senior Agency Official for Privacy, and 2) an independent OIG evaluation report that provides an overall assessment of an agency's security and privacy programs. The FISMA performance metrics were submitted through CyberScope and this report is the OIG independent evaluation of the FTC security and privacy programs. [10]

The OIG contracted with Allied Technology Group, Inc. (Allied Technology) to perform the OIG independent FISMA evaluation. The OIG identified specific program areas to be reviewed, subject to revision as required to accommodate FISMA metric areas issued annually by the DHS. EXHIBIT 1 provides a cross reference between FTC review requirements and DHS FISMA metric topic areas for FY 2015.

EXHIBIT 1: Cross Reference Between FTC and DHS FISMA FY 2015 Metric Areas

FTC OIG FISMA Topic Area	DHS FISMA Metric	
	Number	Topic Area
FTC security management structure	1	Continuous Monitoring Management
FTC security policy and procedures	1	Continuous Monitoring Management
Risk management process	5	Risk Management
System security plans	1	Continuous Monitoring Management
Certification and accreditation process	1	Continuous Monitoring Management
Security incident response and reporting program	4	Incident Response and Reporting
Remediation / Plans of Action and Milestones (POAM)	7	POAM
Configuration Management	2	Configuration Management
Remote Access Program	8	Remote Access Management
Agency Program to Oversee Contractor Systems	10	Contractor Systems
Contingency planning process and procedures	9	Contingency Planning
Security awareness environment	6	Security Training
Life-cycle management of security, management of personnel security	11	Security Capital Planning
Privacy	3	Identity and Access Management

[10] The FTC Senior Agency Official for Privacy is the Chief Privacy Officer (CPO).

This evaluation report has eight sections. As shown in EXHIBIT 1, there are more DHS evaluation topic areas than under the FTC Statement of Work (SOW). In prior years, the FTC SOW provided for more topics than DHS. The DHS topic areas expanded as DHS introduced the CIGIE Maturity Model to assess Continuous Monitoring Management. The CIGIE model includes a scope requirement that addresses all the control areas contained in NIST Special Publication (SP) 800-53 (see EXHIBIT 2). This approach ensures maximum coverage and increased cross-agency continuity by linking the evaluation approach to specific government-wide guidelines. The CIGIE Maturity Model is part of the government's concerted effort to standardize the implementation and assessment of security controls designed to counter Advanced Persistent Threats (APT) and manage risk via a single Assessment and Authorization (A&A) process (i.e., FISMA/RMF and NIST SP 800-37).

EXHIBIT 2: Comprehensive Scope of Security and Privacy

ISCM activities are defined and formalized through the establishment of comprehensive ISCM policies, procedures, and strategies developed consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.

The FY 2015 FISMA Report describes evaluation results in eight sections:

- Section 1.0 BACKGROUND – provides a description of the use of IT within the FTC;
- Section 2.0 SCOPE – provides a description of the scope of this assessment and the integration and compares the FTC original scope from the FTC SOW to the DHS metric reporting topics;
- Section 3.0 OBJECTIVES – describes the assessment objectives and lists the principal guidance under which it was conducted;
- Section 4.0 METHODOLOGY – describes the methodology used in conducting the assessment;
- Section 5.0 GENERAL OVERVIEW – provides a general description of the effectiveness of the FTC security and privacy programs;
- Section 6.0 OMB/DHS IG REPORTING REQUIREMENTS – provides a discussion of each of the program areas assessed for FY 2015. Section 6, integrates the coverage scope of the FTC SOW with the DHS topic areas and presents analysis and findings relative to the DHS topics to facilitate integration with CyberScope metric reporting;
- Section 7.0 STATUS OF PRIOR YEAR RECOMMENDATIONS – provides the status of prior year recommendations; and
- Section 8.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS – provides a summary of the findings and recommendations for FY 2015.

2. SCOPE

NIST guidance provides for the establishment of a security environment that includes consideration for security controls in eighteen groups or "families," shown in EXHIBIT 3 below. The control family structure and a list of controls are contained in NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

EXHIBIT 3: NIST Security Identifiers and Family Names

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

NIST SP 800-53 also includes eight families of privacy controls in Appendix J to NIST SP 800-53, as shown in EXHIBIT 4 below:

EXHIBIT 4: Privacy Controls By NIST Family

ID	PRIVACY CONTROLS
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

The OIG evaluation included a review of FTC security and privacy policies, procedures, and practices in accordance with FTC requirements and the metric topic areas specified by DHS. The FTC and DHS topic areas were integrated as shown in EXHIBIT 5 below. The primary headings

(in bold) are the topic areas where DHS and FTC evaluation areas coincide. Subsections are FTC topic areas that are not specifically identified as a DHS FISMA primary metric. EXHIBIT 5 also includes a reference to the FTC FY 2014 reporting section for the associated topic area.

EXHIBIT 5: Scope of OIG FTC Security and Privacy Program Evaluation

Section	Topic area	FY 2014 Report Section
6.1	Continuous Monitoring Management	6.2
6.1.1	Security Management and Governance Structure	6.1
6.1.2	Security Policy and Procedures / System Accreditation Boundaries	6.1.1
6.1.3	Certification and accreditation process (Including System Security Plans)	6.4 6.1.1
6.1.4	Privacy	6.8
6.2	Configuration Management	6.3
6.3	Identity and Access Management / Remote Access Management	6.5
6.4	Incident Response and Reporting	None
6.5	Risk Management / Security Capital Planning	6.1.2
6.6	Security Training	6.7
4.0	Plan of Action and Milestones (POAM) (No findings or recommendations, discussion included in Section 4.0, Methodology)	4.0
6.7	Contingency Planning	6.6
6.8	Contractor Systems	6.3

The scope of the OIG evaluation provides an assessment of the FTC information security and privacy programs, relative to the NIST security and privacy control families. The DHS assessments are intended to cover the same NIST control families, but through specific, annually-defined metrics.

The OIG evaluation of the FTC information security and privacy programs was conducted to cover FTC activities for FY 2015 and address both the DHS metrics and an assessment of the level of assurance provided by the FTC information security and privacy programs. The evaluation included examination of information security and privacy documentation, reviews of FTC risk assessments and other security testing, discussions with key program officials, and selected testing of security controls.

3. OBJECTIVES

The primary objective of this evaluation was to determine the status of the FTC information and privacy programs at September 30, 2015, as required under FISMA and associated guidance (*FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.2)* 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). [11] The FY 2015 FISMA reporting metrics were uploaded into CyberScope, the designated reporting tool, on November 12, 2015, meeting the OMB November 13, 2015 reporting deadline. The FTC FISMA agency report is due to the appropriate Congressional Oversight Committees by March 1, 2016.

The evaluation has two secondary objectives:

- To improve the overall effectiveness of FTC information security. In accordance with OMB direction, weaknesses or areas for improvement were reported 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; and

- To provide an independent assessment to identify areas for improvement.

[11] DHS annual reporting guidance may be modified through the CyberScope application. The CyberScope guidance takes precedence over published guidance.

4. METHODOLOGY

Maintaining effective information security is an ongoing process. Threats and vulnerabilities are continually changing as are the control measures agencies implement to protect their information assets. Government-wide policy and guidance evolves to address the changing risks and to ensure that the best, reasonable security practices are applied across all federal agencies. Further, the government seeks to establish public/private partnerships to ensure that consideration for effective security is consistent and embedded in all critical infrastructures.

Initial FISMA control metrics and security analysis practices followed requirements established by OMB in 1978[12]. These practices assumed that a three-year "snapshot" of agency security measures was adequate. However, the snapshot approach did not address the rapid changes in the level and type of threats facing federal systems, nor did it provide agency decision-makers with information necessary to effectively monitor and plan their information architecture. As a result, beginning in 2010, NIST revised its security guidance to emphasize a risk management framework that agencies could tailor to their mission needs and IT architecture.[13] Central to the revised approach are risk-based decision-making, control baselines tailored to mission-based requirements, and continuous monitoring of control measures with monitoring frequency based on mission impact.[14] OMB and DHS, working through the JCMWG and CIGIE developed an Information Security Continuous Monitoring Maturity Model. The CIGIE maturity model provides a consistent approach for evaluating the effectiveness of agency continuous monitoring programs that can be applied and compared across agencies. For FY 2015, the CIGIE maturity model is the basis of assessment of agency continuous monitoring programs.

DHS guidance continued to emphasize that the OIG independent security environment evaluation is a cooperative effort that is intended to strengthen agency information security and privacy programs. OIGs are not expected to duplicate agency controls, but to evaluate program effectiveness. Guidance for OIG independent evaluations is intended to "empower" OIGs to focus on analyzing "how Agencies are evaluating risk and prioritizing security issues." 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. Further, 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 make and document reasonable, risk-based decisions. For example:

[12] Transmittal Memorandum No. 1 — "OMB Circular No. A-71" on "Security of Federal Automated Information Systems," July 1978.

[13] Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, SP 800-37, February 2010.

[14] Continuous does not mean instantaneous. According to NIST SP 800-137, the term "continuous" means that "security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information."

- An agency's failure to record changes to documentation in the document change log would not be a high priority item for deficiency reporting if the organization can demonstrate that it made appropriate changes, even though not logged;[15] and

- While NIST guidelines suggest agencies develop configuration guidelines, it is generally not cost-effective to eliminate all deviations or to require individual waivers for each deviation on each machine. Thus, the mere presence of such deviations should be presumed insignificant, unless the overall level of deviations threatens adequate security.

This security and privacy program evaluation focused on the tools and techniques the FTC uses to protect its information assets. The scope of analysis included management and planning of the information environment as well as day-to-day operations. Further, policy, procedures, and operations were evaluated against the CIGIE maturity model for continuous monitoring. The objective of this approach is to determine whether the FTC has fully implemented a risk-based security approach and to evaluate the maturity of that approach (i.e., whether FTC has appropriate security controls in place and provides FTC management with the information necessary to determine whether those controls are effective). This approach also allows assessment of the security level of the total FTC information security environment within a compressed timeframe and at reduced costs.

The evaluation included a number of data collection and analysis activities, including: review of FTC information security and privacy policies and procedures; review of FTC governance structures and planning procedures; examination of FTC Privacy Impact Assessments; examination of select FTC Certification and Accreditations (C&A) for both FTC and contractor-owned systems; examination of information and systems made available through the FTC public Internet website and private Intranet; examination of the FTC continuous monitoring program; examination of configuration management practices; discussions with key officials of the FTC and support service contractors with security and privacy responsibilities; and the FTC's own assessment of the status of FY 2014 FISMA evaluation recommendations.

Information security and privacy programs are not constant, fixed processes. Information security and privacy programs are always changing as they are adapted to changes in threat/vulnerability profiles, government-wide guidance, resource availability, and organizational priorities. In this environment, there is always the potential that vulnerabilities may be overlooked or the security impacts of an event may not be recognized. During the conduct of this evaluation, identified areas of concern were brought to the attention of the OCIO as they arose. Concerns resolved by September 30, 2015 may not be described in this evaluation report,

[15] FY 2015 Inspector General Federal Information Security Management Act Reporting Metrics, Department of Homeland Security, Office of Cybersecurity and Communications, Federal Network Resilience, June 19, 2015.

although their impact was considered in determining the overall effectiveness of the FTC security program.

Recommendations for improvements to the FTC information security or privacy programs identified in this report are rated as Low, Moderate, or High, using the scale contained in NIST Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*:

- 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.

Recommendations provided in this report are included in the appropriate FTC POAM and completion is monitored as part of the OIG FISMA assessment process. OMB provides a weakness severity rating scale for classifying weaknesses identified in FISMA evaluations. In this report, a NIST **severe or catastrophic** adverse effect is classified as an OMB "significant deficiency,"[16] 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. In prior evaluations, FTC management has quickly resolved the few such weaknesses escalated in this manner.

[16] 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 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 other 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 Memorandums M-04-25 and M-14-04 and Circular A-123, *Management's Responsibility for Internal Control*).

Significant deficiencies and reportable conditions must be internally tracked and monitored. In FY 2015, all weaknesses identified were determined to be "other" weaknesses under the OMB criteria.

5. GENERAL OVERVIEW

The status of the FTC information security and privacy programs was summarized in the DHS FISMA reporting metrics submitted through CyberScope. Under the CyberScope metrics, the OIG independent evaluation determined that the FTC information security and privacy programs provide reasonable assurance that FTC information assets are adequately protected with Continuous Monitoring Management between level 2 and 3 under the CIGIE Maturity Model. This determination means that the FTC continuous monitoring practices are well defined and formalized, but that control application is not consistent and performance analysis is deficient. This assessment aligns with prior OIG FISMA assessments for FY 2013 and 2014. Prior OIG assessments determined that the FTC needed to improve the depth and breadth of its information security planning and management practices if it is to continue to maintain adequate asset protection as threats increase and vulnerabilities change with the introduction of new technologies and expansion of mission requirements.

FTC has been working to improve its governance practices. FTC governance boards are now integrated as working components of information security planning and risk management, but as shown in this year's evaluation, there is significant room for improvement. Governance processes and continuous monitoring practices in general need to be consistently and effectively applied if the FTC is to advance its implementation of the CIGIE maturity model. For example, governance processes need tailoring to ensure appropriate independence, and that decisions are appropriately documented with supporting rationale.

FTC has substantial documentation for its security and privacy programs. However, this documentation is typically required to support ongoing operations and is not in a format that can easily support enterprise-level planning and risk management (key governance requirements).

For example, the OCIO could not easily provide high-level documentation of the FTC IT architecture to support enterprise-level planning at the CIO and Executive Director level. The OCIO was able to provide a description of the current FTC enterprise architecture, but not a description of the planned architecture proposed to support future operations and in process IT modernization initiatives.

OCIO efforts to modernize the FTC IT environment highlighted the adverse impacts that can result from inadequate planning. For example:

- In FY 2013, FTC planned to establish an infrastructure architecture that provided for a single campus structure supported on two data centers. This architecture would provide needed resources with an approach that also resolved a long-standing FTC need for an alternate data center for backup operations. This approach was changed in FY 2014 such that the alternate data center capability is now to be only an extension of the existing facility. In FY 2015, FTC advised that a cold site disaster strategy was being pursued in

place of the previously planned alternate data center, to satisfy the FISMA requirement for a disaster recovery capability. The disaster recovery plan provided was out-of-date and assumed the existence of alternate processing capabilities. [17] Currently, the FTC does not have a viable approach for restoring its IT support should it experience a disaster that affects its Headquarters computing facility.

- In February 2014, the OCIO briefed an *IT Modernization: Strategic Vision*, proposing a number of IT modernization initiatives and activities through FY 2018. Based on the artifacts reviewed for FY 2015, this modernization effort proceeded without the compliance with FTC security and acquisition planning policies.[18] For example, no documentation was provided that demonstrated use of risk-based decisions and security planning processes, as required under FTC policy and the NIST risk management framework. Complicating FTC's conduct of the modernization initiatives was the CIO's resignation at the end of December 2014. A new CIO was appointed July 2015, but the management change resulted in reducing the focus on the modernization plan with some initiatives slowed or placed on hold, including governance and oversight, to allow the incoming CIO to implement a modernization plan to which he had contributed. This resulted in delays initiative to mature FTC security and privacy program planning and implementation.

In prior FISMA evaluations, FTC information security and privacy environments were assessed as strong and robust. This determination was based on the capability of controls to protect FTC information assets and the ability of FTC staff to compensate for identified deficiencies. While planning had been an ongoing deficiency, it was improving. In FY 2014, planning became an increasing concern. While policies were established, procedures for implementing those policies had not been effectively tailored to the FTC environment. Thus, they do not provide a workflow that automatically scales to project size, complexity, and organizational risk, ensuring decisions are risk-based and adequately documented without creating impediments to secure introduction of new technologies and approaches.

The problems associated with the planning deficiencies became evident in FY 2015. Significant initiatives were identified that did not follow FTC procedures, resulting in information systems that did not deliver the anticipated benefits and at higher costs than estimated. For example,[19]

[17] Federal Trade Commission, Disaster Recovery and IT Contingency Planning, Disaster Recovery Plan, March 24, 2014 Version 2.1.

[18] The Federal Trade Commission, Office of the Chief Information Officer, *Acquisition Strategy for Information Technology*, Dated September 7, 2011.

[19] We were informed that the new CIO, on arrival in July 2015, instituted the use of project workbooks to fully document all issues for the two example projects and scheduled techstats to determine next steps.

- the deployment of "smart phones" was undertaken in FY 2014 without the planning, user-based requirements, testing, and documentation required for an information system under FTC (e.g., OCIO Acquisition Strategy for Information Technology) and NIST requirements. [20] Instead, FTC relied on lessons learned from other GSA smart phone implementations. This resulted in phones that did not operate within FTC facilities; phones that did not provide anticipated functionality, and phones deployed with known deficiencies; and

- the e-Discovery Support System (eDSS), BCA approved November 2011, was acquired without the functional or performance baselines and tools necessary to quickly identify, resolve, and test errors. FTC did conduct market research to identify suitable commercial software products. This effort, however, focused on functionality and did not collect the information to construct performance metrics or pricing practices to support an acquisition. This resulted in poor product performance (e.g., extended search times and inability to accommodate FTC workloads), the need to devote FTC resources to resolve product deficiencies, and a higher risk of unidentified errors than reasonable for a Commercial, Off-The-Shelf product. Poor product performance also delayed replacement of the legacy system, further increasing operations and maintenance costs.

While the problems implementing new technologies impacted performance and cost, it did not have a significant adverse impact on security. FTC has traditionally followed a conservative technological approach. For example, FTC isolates its critical systems (e.g., Mobile Internet Lab, Secure Investigation Lab) to reduce the potential for information compromise. This plus the smaller scale of FTC IT systems allowed FTC staff to use compensating countermeasures to reduce security risks.

FTC is again embarking on a number of initiatives to increase and modernize its IT capabilities. These changes will place an increasing burden on FTC staff to effectively manage the new environment and the transition to that environment. The continuing environment of change places an increasing stress and workload burden on FTC staff. The staff cannot be expected to continue to compensate for process deficiencies. Thus, if process and technologies are not improved, the risk to the FTC mission and assets will increase. FTC has the necessary policies and basic structures in place, but consistency must be improved and objective monitoring implemented if the FTC security and privacy programs are to achieve the maturity and risk reduction levels targeted by OMB and DHS.

FTC also needs to improve the consistency of its planning and risk management processes. This increased focus will help the FTC to continue to modernize and improve its security and privacy

[20] Smart phones are hand-held computing devices that provide voice, video, and text communications and have the capability to support a variety of business functions.

programs as it addresses mission changes and new threats and initiatives to resolve identified vulnerabilities. The recommendations provided in Section 6 will help FTC mature its processes and improve the performance while reducing the level of effort required to maintain its security and privacy programs.

6. EVALUATION REPORTING REQUIREMENTS

As discussed in Section 2, Scope, this evaluation of the FTC information security and privacy programs is intended to cover topic areas identified by the FTC OIG and those specified by the DHS. The topic areas are presented in the interrelated subchapters within Section 6 that align with the DHS CyberScope reporting topics.

6.1 Continuous Monitoring Management

The Information Technology Committee of the Council of Inspectors General on Integrity and Efficiency (CIGIE), in coordination with DHS, OMB, NIST, and other key stakeholders, developed a maturity model to provide perspective on the overall status of information security within and across federal agencies. The purpose of the CIGIE maturity model 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 OIG FISMA reports about what has been accomplished and what still needs to be implemented to improve the information security program to the next maturity level; and (3) help ensure consistency across the OIGs in their annual FISMA reviews.

FY 2015 is the first year in which the OIG independent assessment is using the maturity model criteria. In this initial application, the approach is applied to the Continuous Monitoring Management topic area. Continuous Monitoring Management is a critical area because it has the broadest coverage scope and includes the foundation elements of effective information security and privacy control, assessed in three model domains (People, Processes, and Technology) at five maturity levels (1-Ad-hoc, 2-Defined, 3-Consistently Implemented, 4-Managed and Measurable, and 5-Optimized).[21] While FTC continuous monitoring activities have not specifically addressed maturity model criteria, they did follow the same concept (i.e., evolving from ad-hoc processes to a formalized model that is consistently applied, sufficiently robust to securely accommodate change, with measured results to support risk-based decision-making).

The OIG assessed FTC Continuous Monitoring Management as meeting the criteria for Maturity Model Level 2, but not meeting all the criteria for Level 3 (i.e., Defined and documented policies, procedures and practices are in place, but implementation is inconsistent).

[21] To reach a particular level of maturity, organizations should meet all of the attributes outlined in for that respective level. For instance, to reach a Level 2 for the people domain, an organization should meet attributes of Level 1. Similarly, to reach Level 2 for the ISCM program overall, organizations should meet attributes for both Level 1 and Level 2. When determining the overall maturity level, the lowest common denominator approach shall apply. For instance, if an organization is at Level 1 for the people domain but at Level 3 for both the processes and technology domains, the overall maturity of the organization's ISCM program would be Level 1.

Use of the CIGIE Model

The OIG evaluation focuses on the effectiveness of FTC security controls to protect FTC assets. Continuous monitoring is one aspect of that assessment. The CIGIE model is intended to demonstrate that security risk is reduced as continuous monitoring programs mature through the 5 performance levels. DHS uses a scoring approach where scores increase only when an organization meets all the requirements for the next level. The difference in evaluation approach means that the OIG assessment includes the impact of continuous monitoring controls at all maturity levels when assessing the effectiveness of the FTC security and privacy control environment.

A summary of the rationale for assessing the FTC maturity level was included in the CyberScope reporting (see Appendix A). The detailed rationale for this assessment is contained in EXHIBITs 6 and 7 below. EXHIBIT 6 provides the OIG assessment for Level 1, and EXHIBIT 7 provides the OIG assessment for Level 2.

The subsections of Section 6.1 provide recommendations for improving FTC Continuous Monitoring Management.

EXHIBIT 6: Assessment of FTC Continuous Monitoring vs Level 1 Maturity Model Criteria

ISCM Program Maturity Level	Definition	People	Processes	Technology
Level 1 Ad-hoc	1. ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.	1.1.1 ISCM stakeholders and their responsibilities have not been fully defined and communicated across the organization. **Response:** FTC developed an ISCM strategy that is integrated within the existing policy. Stakeholders and their roles are defined in the strategy document. The strategy and roles are communicated across the FTC through the published policies and the governance boards which have active participation by FTC Bureaus and offices.	1.1.5 ISCM processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. **Response:** FTC has security and privacy policies in place that are aligned with NIST guidance. The initial copy of the FTC ISCM strategy was dated May 2014. This version was reviewed by the OIG and comments were provided.	1.1.9 The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. Use of ISCM technologies in the following areas is ad-hoc. -Patch management -License management -Information management -Software assurance -Vulnerability management -Event management -Malware detection -Asset management -Configuration management -Network management -Incident management **Response:** FTC identified tools to automate support for its ISCM strategy. Currently. FTC has acquired tools to perform a variety of security tasks such as scanning for known vulnerabilities in software, Section 8

ISCM Program Maturity Level	Definition	People	Processes	Technology
			The strategy document was revised to accommodate recommendations received and Version 3 was issued in 10/22/2014. Version 4 was issued to accommodate changes through 11/9/2014. The strategy was designed to build on established practices based on the prior 1/3 X 3 assessment approach that can be carried forward into an ISCM approach coupled with new assessment and monitoring practices. For example, FTC makes use of security monitoring and assessment services provided by the Department of Homeland Security (DHS). This approach allows the FTC to evolve its practices into a mature ISCM while constraining costs and maximizing the use of in place security practices. FTC has consistently maintained a comprehensive inventory of its information assets and has acquired the DOJ CSAM product to modernize and better manage	compliance, server configuration and status, and Help Desk/trouble reporting. Among the products FTC is using or is in process of implementing are – --Solar Winds - enterprise information technology infrastructure management software; -- Remedy for trouble reporting and analysis; -- Blue Coat security software; and -- DOJ Cyber Security Assessment & Management (CSAM) system. FTC is still in process of installing and tailoring the tools acquired to the full range of capabilities available and to support cross-domain analyses.

ISCM Program Maturity Level	Definition	People	Processes	Technology
			the inventory. CSAM is in process of implementation. FTC tailoring performance data collection products to enable cross-domain analyses. The FTC POA&M process is used to track vulnerabilities from identification to resolution. The FTC is developing a Dashboard to communicate the status and health of the security environment to managers and stakeholders with security. Information is obtained from existing products such as Solar Winds and results of DHS IT hygiene services.	
		1.1.2 The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Key personnel do not possess knowledge, skills, and abilities to successfully implement an effective ISCM program. **Response:**	1.1.6 ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **Response:** FTC formalized its information security and privacy programs a number of years ago. The objective was to establish programs that were consistently	1.1.10 The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Response:** FTC maintains a complete inventory of its IT assets.

ISCM Program Maturity Level	Definition	People	Processes	Technology
		FTC has the staff with the necessary technical skills. The issue is not the skill level, but the fact that systems are changing and maturing and FTC is modernizing their infrastructure. This places a strain on the level of resources available. These issues are being addressed by ongoing role-based training and phasing in the new processes and techniques with a target completion of FY 2017.	applied across the Commission and that would ensure a consistent level of protection of FTC assets regardless of whether service was provided through in house or contracted resources. The procedures were consistently applied with a system focus, in accordance with then current OMB policy and NIST guidance. Variations identified were random and were typically the result of inadvertent error. FTC analyses all errors for a root cause and establishes corrective measures as appropriate. The system-based control environment is being leveraged to provide the agency risk perspective. FTC also implements automated measures where possible, cost effective, and with a risk perspective. FTC has implemented automated techniques to perform a variety of security tasks such as scanning for known vulnerabilities in software and Section 8 compliance, server	This includes its infrastructure hardware, software, and applications; websites hosted on commercial services; and social media subscriptions / presences. FTC identified several products that will be or are currently used to maintain its asset inventories (e.g., Remedy and CSAM). Both systems are currently being configured. The objective is to provide a near real time inventory of its infrastructure and point-in-time inventories of other assets, principally its information assets. FTC is designing a consolidated inventory that will support both its fixed asset and information asset inventories.

ISCM Program Maturity Level	Definition	People	Processes	Technology
			configuration and status, and Help Desk/trouble reporting. Among the products FTC is using or is in process of implementing are -- --Solar Winds - enterprise information technology infrastructure management software; -- Remedy for trouble reporting and analysis; -- Blue Coat security software; and -- DOJ Cyber Security Assessment & Management (CSAM) system. FTC has also directed that its support services contractor develop cross-domain analyses. FTC is still in process of installing and tailoring the tools acquired to the full range of capabilities available.	
		1.1.3 The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions.	1.1.7 The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk.	

ISCM Program Maturity Level	Definition	People	Processes	Technology
		Response: The FTC governance process includes participation by the primary individuals with significant responsibility for evaluating and making risk-based decisions. The information sharing practices are being improved as the impact of the FTC governance boards is recognized and the members provide more detail regarding the type and level of detail required to make and document risk-based decisions.	**Response:** The FTC has a dashboard program in process that is used to monitor projects. The dashboard is using standard metrics to provide consistency. A similar standardized metric approach is used in the monitoring tools used by DHS to evaluate the FTC IT environment. The governance program is developing improved estimating procedures and standard metrics to support planning and monitoring through the SDLC. The qualitative and quantitative metrics will be tuned and extended as the governance processes mature. FTC initiated its governance and security modernization in FY 2011.	

ISCM Program Maturity Level	Definition	People	Processes	Technology
		1.1.4 The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. **Response:** FTC developed its governance structure in FY 2011 and began implementation in FY 2012. The governance board process is used for developing risk tolerances, identifying organizational priorities and ensuring that risk-based decision-making is applied consistently across the FTC.	1.1.8 The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes. **Response:** FTC evaluates adverse events to identify a root cause as part of its incident response procedures. The results of the root cause analyses are used to implement procedural or technical change as necessary to prevent a recurrence. For example, FTC has made changes to its acquisition policies, on boarding practices, and patch management practices as part of its lessons learned practices. The results of lessons learned and root cause analyses are disseminated through a variety of practices such as awareness messages, role-based training, e-mail announcements, and the governance boards.	

EXHIBIT 7: Assessment of FTC Continuous Monitoring vs Level 2 Maturity Model Criteria

ISCM Program Maturity Level	Definition	People	Processes	Technology
Level 2 Defined	1.2 The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization.	1.2.1 ISCM stakeholders and their responsibilities have been defined and communicated across the organization. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement ISCM activities. **Response:** Stakeholders have been defined and governance board actions were taken to approve acquisitions necessary to support implementation of ISCM activities. The size and centralized nature of FTC governance practices minimizes the difficulty in communicating policies and practices across FTC.	1.2.5 ISCM processes have been fully defined for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. However, these processes are inconsistently implemented across the organization. **Response:** ISCM processes have been defined in accordance with the FTC strategy and security and privacy policies and procedures. The ISCM is centrally implemented and	1.2.9 The organization has identified and fully defined the ISCM technologies it plans to utilize in the following automation areas. In addition, the organization has developed a plan for implementing ISCM technologies in these areas: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. However, the organization has not fully implemented technology is these automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some ISCM activities, the tools may not be interoperable.

ISCM Program Maturity Level	Definition	People	Processes	Technology
			thus will apply across the agency. The processes may not be consistently applied, but FTC has taken action to improve consistency as the processes mature and stakeholders become more familiar with their operation and organizational impact.	**Response:** FTC has identified a set of products and services to support its ISCM strategy. The products are in various stages of implementation and tailoring. The products will feed data into the FTC dashboard and reporting processes. This will provide consolidated reporting for the FTC ISCM. Currently, FTC uses performance data provided by the tools implemented and manually performs cross-domain analyses of any incidents, should they occur (FTC has had no significant incidents in the past two years). FTC experienced events tend to be random and the result of an unintentional error with little operational or cost impact. The critical risk item for the FTC is reputational risk.
		1.2.2 The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. In addition,	1.2.6 ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used.	1.2.10 The organization has defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and

ISCM Program Maturity Level	Definition	People	Processes	Technology
		the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective ISCM program. **Response:** FTC has the staff with the necessary technical skills. The issue is not the skill level, but the fact that systems are changing and maturing and FTC is modernizing their infrastructure. This places a strain on the level of resources available. These issues are being addressed by ongoing role-based training and phasing in the new processes and techniques with a target completion of FY 2017.	**Response:** Methods and tools used are consistent across the FTC. The variance is in the training and experience FTC staff have with procedures that are defined, but not yet fully implemented. Based on prior performance, once the staff are fully trained and have experience using the ISCM practices, application will become consistent across the agency.	software on its network and the security configuration of these devices and software. However, the organization does not consistently implement the technologies that will enable it to manage an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Response:** FTC maintains a complete inventory of its IT assets. This includes its infrastructure hardware, software, and applications; websites hosted on commercial services; and social media subscriptions / presences. FTC identified several products that will be or are currently used to maintain its asset inventories (e.g., Remedy and CSAM). Both systems are currently being configured. The objective is to provide a near real time inventory of its infrastructure and point-in-time inventories

ISCM Program Maturity Level	Definition	People	Processes	Technology
				of other assets, principally its information assets. FTC is designing a consolidated inventory that will support both its fixed asset and information asset inventories.
		1.2.3 The organization has defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. However, ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions. **Response:** The FTC governance process includes participation by the primary individuals with significant responsibility for evaluating and making risk-based decisions. The information sharing practices are being improved as the impact of the FTC governance boards is recognized and the members provide more detail regarding the type and level	1.2.7 The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. **Response:** The FTC has a dashboard program in process that is used to monitor projects. The dashboard is using standard metrics to provide consistency. A similar standardized metric approach is used in the monitoring tools used by DHS to evaluate the FTC IT environment. The governance program is developing improved estimating procedures and	

ISCM Program Maturity Level	Definition	People	Processes	Technology
		of detail required to make and document risk-based decisions. Timeframes for information dissemination are consistent with stakeholder needs.	standard metrics to support planning and monitoring through the SDLC. The qualitative and quantitative metrics will be tuned and extended as the governance processes mature. FTC initiated its governance and security modernization in FY 2011. As the measuring practices are fully implemented and become repetitive, consistency will improve.	
		1.2.4 The organization has defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. However, ISCM activities are not consistently integrated with the organization's risk management program. **Response:** FTC developed its governance structure in FY 2011 and began implementation in FY 2012. The governance board process is used for	1.2.8 The organization has a defined process for capturing lessons learned on the effectiveness of its ISCM program and making necessary improvements. However, lessons learned are not consistently shared across the organization and used to make timely improvements to the ISCM program. **Response:** FTC evaluates adverse events to identify a root cause as part of its incident response procedures. The results of the root cause	

ISCM Program Maturity Level	Definition	People	Processes	Technology
		developing risk tolerances, identifying organizational priorities and ensuring that risk-based decision-making is applied consistently across the FTC. FTC ISCM activities are directly integrated with FTC risk management activities.	analyses are used to implement procedural or technical change as necessary to prevent a recurrence. For example, FTC has made changes to its acquisition policies, on boarding practices, and patch management practices as part of its lessons learned practices. The results of lessons learned and root cause analyses are disseminated through a variety of practices such as awareness messages, role-based training, e-mail announcements, and the governance boards.	

6.1.1 Security Management and Governance Structure

The FTC is headed by five Commissioners supported by an Executive Director who reports to the Chairwoman and serves as the chief operating officer and manager, responsible for such matters as administrative services, financial management, procurement, human resources management, information and technology management, as well as overall FTC program and policy execution. The Chairman delegated information security/FISMA responsibilities to the CIO in a September 2009 memorandum. The delegation of FISMA responsibilities was reiterated in a memorandum from the Chairman issued in August 2011. The current Executive Director assumed his position in August 2013, and the current CIO assumed his position in July 2015.

FISMA defines a management structure for agency information security programs. Under the FISMA structure, the responsibility for the agency information assurance program is assigned to the CIO, reporting to the head of the agency, who is required by FISMA to delegate operational responsibility to the Senior Agency Information Security Officer (Chief Information Security Officer (CISO)). The CISO, through the information security program, assigns information security program responsibilities to the appropriate organizational components. The objective of the FISMA structure is to ensure that information assurance concerns receive senior management attention in planning, program compliance, and resource allocation.

In the latter part of FY 2011, the FTC CIO delegated responsibility for IT planning by through an Information Technology Governance Program Charter. The FTC governance process is evolving, taking on larger roles in IT planning including providing input on budget allocation decisions and evaluating business cases for IT investments. The original Governance Program Charter focused on investment management. The current August 2014 Charter, shown in EXHIBIT 8, provides an expanded scope that includes risk management. The Governance Board structure is shown in EXHIBIT 9. EXHIBIT 10 provides a summary of the characteristics of this structure and responsibilities of each Board.

EXHIBIT 8: Governance Program Scope

To increase transparency and proactively manage risk, all IT investments are within the scope of IT governance, regardless of the estimated cost and the organization managing the investments. This includes the acquisition, development, upgrade or maintenance of all hardware, software, applications, systems, and related services investments supporting FTC business lines and management processes. While the scope of IT governance covers all types of IT investments, the level of oversight depends on type of investment and should be commensurate with its complexity and risk.

EXHIBIT 9: Framework for FTC Governance Structure August 2014

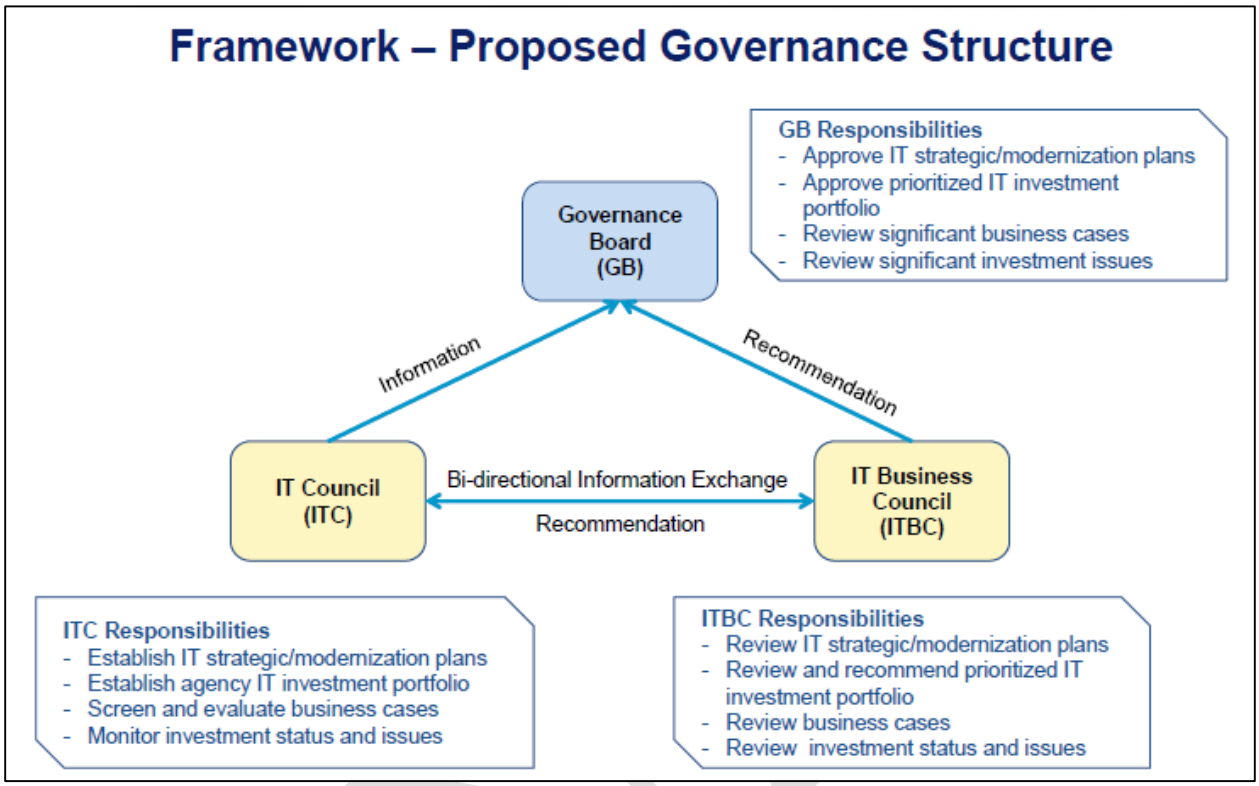
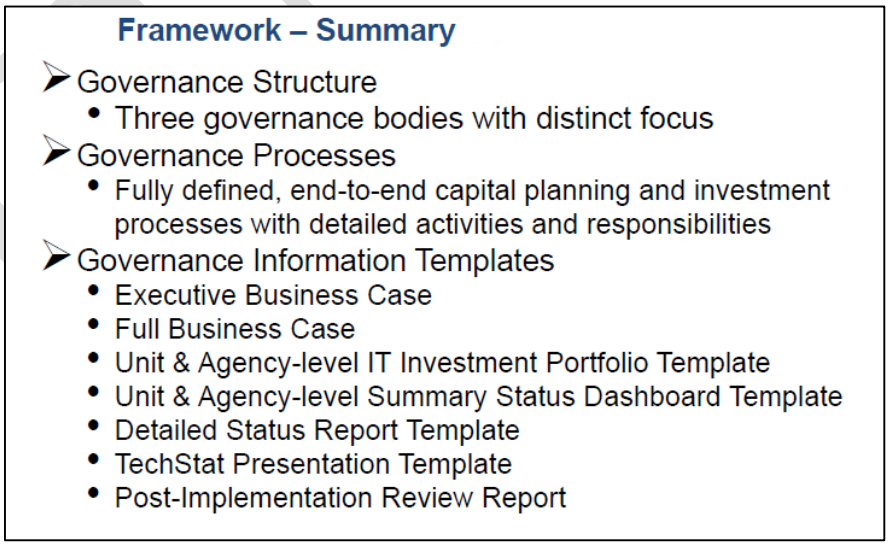


EXHIBIT 10: Governance Board Overview



The current governance structure supports an analytical approach that considers risk as well as the cost factors that are the typical focus of investment analysis.

In FY 2014, OIG recommended (Recommendation – FY 2014 – 01: Security Management Structure) that FTC continue to evolve its governance practices, expanding the use of CPIC and investment analysis techniques and improving documentation of risk-based decisions. While there have been improvements, implementation continues to be inconsistent and documentation is still not adequate. For example, the FTC project to implement "smart" phones did not include preparation of required planning and security artifacts; reports intended to monitor performance of Datacenter services have limited utility; the eDSS suffers from the lack of testable functional and performance baselines; and available tools are not yet configured to perform cross-domain security analyses.

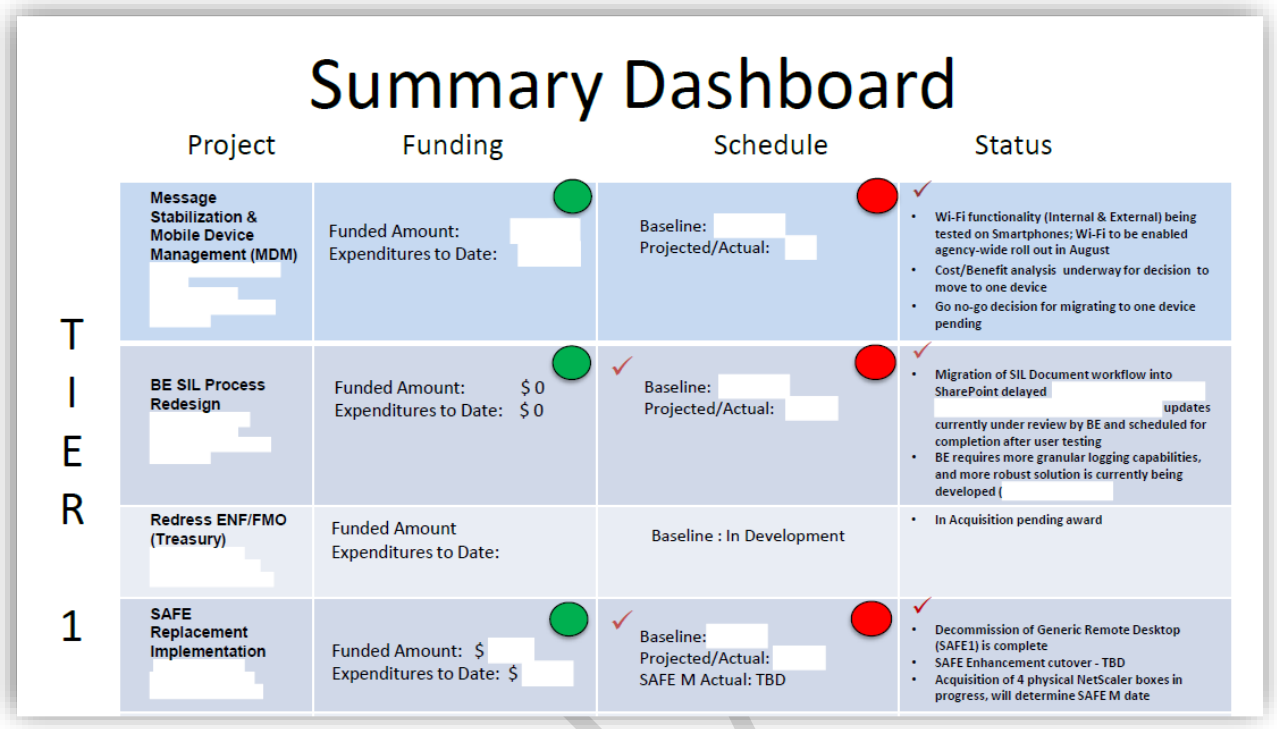
FTC corrects documentation, management and monitoring weaknesses as staff become aware of problems. This is a characteristic of Level 2 within the Maturity Model where weakness identification is more likely to result from staff observation than from automated analysis techniques.

FTC is taking action to improve its capabilities to monitor project status as part of its governance procedures. In FY 2015, FTC implemented a Project Dashboard that provides summary information regarding project funding, schedule, and status. EXHIBIT 11 provides the criteria used to classify project status, and EXHIBIT 12 provides a redacted example of a status report.

EXHIBIT 11: Project Dashboard Performance Classification Criteria

Project Status Dashboard Legend			
Schedule	Schedule is on target or delayed less than 10% for Expected Delivery.	Schedule delay is between 10% and 20% of Expected Delivery.	Schedule delay is greater than 20% of Expected Delivery.
Cost	Cost is on target or cost over-run is less than 10% for Funded Amount.	Cost over-run is between 10% and 20% of Funded Amount.	Cost over-run is greater than 20% of Funded Amount.
✓	Denotes that an area has been changed since the previous update		

EXHIBIT 12: Example FTC Summary Dashboard Reporting Project Status



Summary Dashboard

	Project	Funding	Schedule	Status
TIER 1	Message Stabilization & Mobile Device Management (MDM)	Funded Amount: Expenditures to Date:	Baseline: Projected/Actual:	• Wi-Fi functionality (Internal & External) being tested on Smartphones; Wi-Fi to be enabled agency-wide roll out in August • Cost/Benefit analysis underway for decision to move to one device • Go no-go decision for migrating to one device pending
	BE SIL Process Redesign	Funded Amount: $ 0 Expenditures to Date: $ 0	Baseline: Projected/Actual:	• Migration of SIL Document workflow into SharePoint delayed updates currently under review by BE and scheduled for completion after user testing • BE requires more granular logging capabilities, and more robust solution is currently being developed (
	Redress ENF/FMO (Treasury)	Funded Amount Expenditures to Date:	Baseline : In Development	• In Acquisition pending award
	SAFE Replacement Implementation	Funded Amount: $ Expenditures to Date: $	Baseline: Projected/Actual: SAFE M Actual: TBD	• Decommission of Generic Remote Desktop (SAFE1) is complete • SAFE Enhancement cutover - TBD • Acquisition of 4 physical NetScaler boxes in progress, will determine SAFE M date

FTC efforts to mature its governance and Continuous Monitoring Management capabilities will not be a short-term effort. Governance and management must address all the technological capabilities used to support the FTC mission. Reporting and oversight practices must be sufficiently resilient to securely and efficiently adapt to change as new technologies are adopted and use of technology is expanded for increased mission support. Further, FTC needs to ensure that it avoids situations where monitoring and management controls implemented are not overly restrictive and resource-intensive, constraining FTC's ability to quickly react to threat and mission changes.

Governance Board responsibilities and workflow procedures must be carefully documented to ensure responsibilities of the Boards and other stakeholders are clear and coordinated; ensure that the workflow process serves as a mechanism to direct and escalate issues to the appropriate decision-making organization; and to serve as a baseline to management and monitoring of the governance process itself. For example, changes in the roles and activity of the Governance Boards can be used to demonstrate maturation of FTC governance, risk management, and investment analysis processes.

Governance Board responsibilities are expected to change as the program matures and adapts to changing requirements. For example, the FY 2011 Governance Program Charter defined two bodies, a "Governance Board which provides a strategic, agency-wide perspective and guidance to the Commission for long-term IT investment" and a Technology Council that "ensures sound

decision-making with input from throughout the agency with attention to life-cycle costs, information security, and enterprise architecture." The current, FY 2014, Governance Program Charter provides for three Boards. This reflects the need for expanded input from FTC Business units.

The scope of responsibility of the Governance Boards has also changed. In FY 2011, projects required to have Governance Board approval were limited to those "IT investments for new and significant upgrades to existing enterprise-wide applications or systems with life-cycle costs of $500,000 or more." The FY 2014 Governance Board Program Charter expands the scope to all "IT investments," but then limits the scope by separating requirements into Operations and Maintenance/Steady-State (O&M/SS) and Development/Modernization/Enhancement (DME). O&M investments are to follow Financial Management Office (FMO) budget guidance. DME projects require full business case support if they meet one or more of the following criteria:

- Five-year life cycle cost ≥$1M
- High-impact on business processes
- High-risk of not completing execution and delivery

The OIG anticipates that the Governance Program Charter and implementing Work Instructions will continue to change to address OIG recommendations, resolve internal conflicts, address changing requirements, and continue to mature. For example, the Charter and Work instructions contain requirements that are inconsistent and may not result in efficient, effective Board operations:

- Organizational Conflict of Interest and Absence of Clearly Defined Roles and Responsibilities;

  The Governance Boards are monitoring, oversight, and decision-making entities; they are not operational. Reflecting their roles, Governance Board membership is typically comprised of senior management staff. For example, IT Council (ITC) membership consists of OCIO Assistant Directors and IT Governance Board (ITGB) membership consists of "career deputies" from the following offices:

  - Executive Director (ED)
  - Bureau of Consumer Protection (BCP)
  - Bureau of Competition (BC)
  - Bureau of Economics (BE)
  - Office of the General Counsel (OGC)

  The ITC, however, has also been assigned responsibilities such that it appears to serve as an operational component of the OCIO. For example, the ITC is charged with the responsibility to "develop enterprise architecture," "support synthesis and development of business cases," "develop standardized investment status summary dashboards,"

"develop IT operations dashboard," and "…develop plans of actions and milestones." These are necessary functions, but they should be assigned to operational components of the OCIO instead of the ITC which, as an oversight Board, would be expected to review the operational decisions and recommendations of OCIO and also would have limited resources. By comingling Governance Board and OCIO responsibilities, it becomes more difficult to evaluate and optimize performance of either. Further, comingling responsibilities increases the potential for inconsistent implementation and demonstrates a lack of program maturity – key evaluation characteristics of the CIGIE maturity model.

- Overly Complex or Unclear Work Instructions; and

  The OIG reviewed the Work Instructions for the administrative functions of the ITGB, IT Business Council (ITBC), and ITC. We understand that the documents are still in Draft, but the processes described may cause compliance problems and have a high potential for delaying Governance Board activities. For example, Meeting Minutes are intended to document decisions and reasons for decisions, and capture action items for tracking or later action. The procedure for review of ITC Meeting Minutes provides for a multi-step review by an "ITC Support Team" and several specified individuals over a four-day period. After this review, the Meeting Minutes are finalized, converted to pdf, and sent to the meeting participants. There appears to be no provision for corrections by the meeting participants or use of more parallel processes such as creating a single Meeting Minutes draft and sending it to all meeting participants for review and comment.

  As another example, the ITC Pre-Meeting Activities provide for decision points where the decision criteria are questions such as, "is idea still viable," and "is idea a project." These types of questions would be expected to be resolved by a project sponsor prior to submission for ITC review or decision by the ITC itself. Further, in this instance, the individual making these determinations is not identified. For an oversight entity, the procedures should focus more on the criteria for determining what will be submitted for ITC review and what documentation is expected.

- Documentation Guidance.

  The governance processes need a number of standard documents and templates to support their activities, such as Business Case Analyses (BCA), resource and cost estimates, and functional/mission requirements. FTC provides guidance for some items such as the BCA and security artifacts. Guidance is not provided for other documentation, such as developing cost/resource estimates, developing risk estimates, and scaling documentation to project size and complexity. Instead, cost estimates and other documentation is generally based on prior experience. As FTC matures its processes to mitigate delays caused by inevitable staff turnover and ensure consistency and accountability over a

project's lifecycle, it will need to provide improved guidance as to the level and type of documentation that is required for use within its governance process.

FTC should continue evolution and improvement of its IT governance process as part of its efforts to mature its Continuous Monitoring Management program. The improvements should emphasize guidance that would help FTC staff prepare the documents needed to support the Board activities where the focus is on what is to be provided and on what schedules (e.g., preparation of a Basis of Estimate to support resource and cost estimates). FTC should also review its Governance Program Charter and Work Instructions to ensure that they are sufficiently detailed for a monitoring and oversight function.

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. 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. – Estimated program impact – Moderate

(Also, see recommendation FY 2015-04 to elevate the CPO to voting membership on the ITGB)

6.1.2 FTC Security Policy and Procedures/System Accreditation Boundaries

A key element in establishing an effective security environment is ensuring that responsibilities for data and system protection are appropriately assigned to responsible organizations and individuals. FISMA provides for this assignment through a certification and accreditation process included as part of the NIST Risk Management Framework (RMF). Under FISMA requirements, all information systems (regardless of implementing approach) must be covered by an Approval/Authorization To Operate (ATO) and be assigned to a specific System Owner. [22] Similarly, information/data must have an assigned owner who ensures that security and privacy controls are appropriate for the data for which they are responsible.

NIST security and privacy guidance provides for the establishment of an accreditation boundary for an information system. A system accreditation boundary is to encompass the data, hardware, software, and administrative processes and procedures required to accomplish the system's defined mission objectives. A System Owner has responsibility for ensuring that a system

[22] All information systems must be covered by a system security plan and labeled as a major application or general support system. Specific security plans for other applications are not required because the security controls for those applications or systems would be provided by the general support systems in which they operate. (NIST SP 800-18)

achieves its mission objectives and that appropriate security and privacy controls are in place and effective. The system accreditation boundaries are also used by the Designated Approving Authority in making a determination (ATO) regarding the acceptability of system controls to reasonably protect FTC assets and fulfill its authorized missions. Accreditation boundaries may encompass more than one system with multiple System Owners and their own accreditation boundary. In such cases, the security controls of a supporting system may be leveraged in the Accreditation Boundary for a supported system. For example, FTC obtains information services from the Department of the Interior (DOI). The FTC must issue an ATO that documents a determination that this arrangement appropriately protects FTC information and mission. In this instance, FTC establishes an Accreditation Boundary that encompasses functions directly performed by the FTC as well as the services provided by the DOI. The FTC leverages the DOI control determination (ATO) in making its determination to issue an FTC ATO.

NIST guidance allows D/A wide discretion in establishing Accreditation Boundaries. The primary determinant is that there must be a reasonable supporting rationale such as the systems are under the same direct management responsibility (e.g., multiple services provided by the DOI), they perform an equivalent mission (e.g., REDRESS vendors), and FTC smart phones with the associated management service, because they support the same mission objective (see NIST SP 800-18 Rev 1, Chapter 2).

Establishing appropriate Accreditation Boundaries will be especially important as the FTC moves forward with its modernization efforts. FTC's modernization plan will incorporate a variety of different support approaches (e.g., cloud, software as a service, managed hosting, and application as a service).

FTC has established reasonable accreditation boundaries for the majority of its information systems. In FY 2014, the OIG recommended that the FTC review its accreditation boundaries for Minor Applications (FY 2014 – 04: Certification and Accreditation) included within the FTC Datacenter Accreditation Boundary (e.g., Constitution Center, smart phones, and websites) to ensure they properly reflect their Datacenter relationship, management responsibility, and importance to the FTC. [23] For example, it may be more appropriate to place FTC use of social media within an Accreditation Boundary for web-based systems.

FTC should continue its assessment of system Accreditation Boundaries. Minor Applications should be reclassified as Major Applications where they are significant investments and require special security consideration because of their impact on FTC activities. For example, FTC

[23] NIST Special Publication 800-37 defines a minor application as an application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system. In those cases where the minor application is not connected to a major application or general support system, the minor application should be briefly described in a general support system plan that has either a common physical location or is supported by the same organization.

should consider designating its new smart phone service and eDSS systems as Major Applications. As a Major Application, each of these efforts would have required, at a minimum, a Security Plan, a Security Assessment Report, and Plan of Action and Milestones (POA&M), a Business Impact Analysis, and an Acquisition Plan. Preparing these artifacts and conducting the associated reviews would have increased the potential that the identified weaknesses would have been identified prior to production, and the POA&M process would have provided a mechanism for tracking and monitoring actions taken to resolve identified weaknesses.

Recommendation – FY 2015 – 02: **FTC Security Policy and Procedures/System Accreditation Boundaries** - 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. – Estimated Program Impact - Moderate

6.1.3 Certification and Accreditation

FTC has a Certification and Accreditation (C&A) policy in place that is compliant with NIST guidance.[24] The number of FTC systems and their security categorization and C&A status (i.e., ATO) were validated as part of the FY 2014 and FY 2015 OIG FISMA evaluations. FTC includes the ATO status of each application as an element in its system inventory. This approach ensures that FTC staff have the information available to determine when a system requires renewal of its ATO and facilitates focusing OIG assessment activities on systems with significant impacts or that have undergone recent changes.

The FY 2014 OIG FISMA evaluation determined that FTC C&A practices for internally-managed systems (e.g., *Data Center General Support System (GSS)*; *Mobile/Internet Lab (MIL)*; *Virtual Litigation Support Lab (VLSL) General Support System (GSS)*; and the *Secure Investigations Lab*) are substantially complete, but contain inaccuracies, inconsistencies, and insufficient detail. These deficiencies did not affect the level of security provided, but result in unnecessary effort to ensure that it is the document error and not a control weakness.

To resolve accuracy and consistency concerns, FTC initiated an action to convert C&A artifact development and maintenance to the DOJ Cyber Security Assessment & Management (CSAM) system. The DOJ CSAM provides Federal agencies with a web-based secure network capability to assess, document, manage, and report on the status of IT security risk assessments and implementation of NIST IT security control standards and policies. DOJ offers CSAM as a shared service (Line of Business) to federal agencies. Among CSAM users are the DOJ, the Department of Transportation, and the Department of Labor. CSAM was selected because it is designed to prepare the security artifacts required under NIST SP 800-37 in formats specific to

[24] OCIO-12-CA-100.

the federal government. Once converted, the CSAM process should impose discipline that improves artifact accuracy and consistency and allows FTC staff to focus on identifying and resolving system weaknesses. Even after conversion to CSAM, FTC will maintain its own system inventory that will add reporting for those data elements that are not within CSAM (e.g., tracking of CUI). FTC will also need to make accommodations to link CSAM reporting to its continuous monitoring strategy. CSAM currently does not support continuous monitoring, and continuous monitoring practices are typically tailored to individual agencies and systems.

In its FY 2015 evaluation, OIG reviewed a selection of artifacts supplied by other organizations to support FTC ATO determinations. The specific documents reviewed were accepted by another federal agency, implying a level of trust that often results in a less detailed review than FTC would performed without a federally-issued provisional ATO. This assessment showed that the documentation provided contained inconsistencies and errors that were typically related to references to obsolete or inappropriate guidance. The assessment also showed that there were instances where the Assessor developing the documents made statements that were problematic. For example, the Assessor performing the risk assessment for the smart phone management service summarized the risk analysis findings as follows:

> "… 4 vulnerabilities classed as High and an additional 75 classed as Moderate. In addition, the Security Controls Assessment found 6 Control implementation weaknesses classed as Priority 1, 1 Control implementation weaknesses classed as Priority 2 and 1 Control implementation weaknesses classed as Priority 3. The Penetration test found no exploitable vulnerabilities. As a result of the assessment 20 new items have been added to the product POA&M document."
>
> "Clearly, the unclassified DoD requirements are a higher bar than can be justified for a commercial operation under a risk-based, cost-effective standard, but [vendor name deleted] can use these results as a jumping on point. The purchase of a database scan tool and implementation of a program of consistent configuration of SQL servers and databases, to include business justifications for the required operational settings, should be prioritized."

This opinion implies a potential vulnerability. DoD and civilian federal agencies follow the same security requirements for unclassified information. Security controls are based on impact as defined in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems.* The FTC smart phones and their associated management system are categorized as Moderate. Thus, a scanning tool that tests against the requirements for a Moderate system is appropriate regardless of whether the system supports DoD or a civilian agency. FTC needs to be informed about any deficiencies and their risk impact.

This issue and similar issues regarding the quality of third-party document quality were discussed with the CISO. The FTC, as with other federal agencies, is increasingly incorporating software and services where it leverages security assessments performed by other federal organizations. Reliance on the security work of other federal agencies will continue. It is impractical and cost excessive for the FTC to independently conduct security assessments for all the products and services it acquires from other agencies. As an alternative, FTC needs to provide guidance to its staff charged with reviewing ATO documentation regarding indicators of potential vulnerabilities that warrant follow-up and resolution. For example, for the smart phone management service, addressing the concerns raised by the Assessor's conclusions described above might include a request for a statement of the actions taken to resolve reported deficiencies and an explanation as to why a federal civilian agency that handles PII and other sensitive data does not require a security control at least equal to that required for DOD unclassified information.

The OIG recommends that the FTC add specific guidance to its security staff as to the criteria to use when reviewing security assessments provided by other federal organizations. For example, all risk assessments use control criteria based on NIST SP 800-53. The risk assessment criteria may vary based on the individual agency requirements (e.g., smart phone criteria did not specify FIPS 140-2 encryption for data backup, yet this control is mandatory for FTC systems). To determine the level of risk, FTC staff should know how the criteria used in the risk assessment compare to FTC security criteria. For example, if the smart phone and associated management software have other controls that compensate for the FIPS 140-2 deficiency, FTC may elect to accept the added risk.

Recommendation – FY 2015 – 03: **Certification and Accreditation** - 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. – Estimated Program Impact - Moderate

6.1.4 Privacy

FTC continues to maintain an aggressive privacy program. The program addresses the critical components of privacy protection, including identification of privacy data, inventories of privacy data, privacy awareness and training, limited retention of privacy data, privacy incident response procedures, completion of System of Record Notices (SORNs) required under the Privacy Act, and completion of Privacy Impact Assessments (PIAs). FTC privacy practices are established under the auspices of the Chief Privacy Officer (CPO).

The CPO reports directly to the Chairwoman and coordinates efforts to implement and review the agency's policies and procedures for safeguarding all sensitive information, and chairs its Privacy Steering Committee and the Breach Notification Response Team.[25]

With the inclusion of Privacy controls into NIST SP 800-53 in 2013, FTC privacy controls were strengthened:

- The development of information security architectures are to be coordinated with the CPO and the CPO is to review authorization packages to determine that all applicable privacy requirements are met and the risk to Personally Identifiable Information (PII) is sufficiently addressed before authorizing officials make risk determination and risk acceptance decisions;[26]

- Privacy controls are now explicitly included in development of security control baselines;

- Privacy controls must be routinely assessed and their status reported as part of the FTC continuous monitoring program; and

- Privacy is a topic area in FTC annual security awareness training.

The importance of privacy issues is recognized within the FTC. FTC management and staff recognize that the FTC's reputation for protecting sensitive information is crucial to its ability to obtain and use data voluntarily provided by industry and individuals. While the CPO may participate in meetings of the ITGB and ITBC, the CPO is only included as an ex-officio member of the ITGB and not as a permanent member of the ITBC. In these roles, the CPO is limited to providing guidance, advice, and support to decisions. The CPO reports directly to the FTC Chairwoman and is responsible for implementation and review of Commission policies and procedures for safeguarding all sensitive information. Given this level of responsibility, FTC should place the CPO on a par with other members of the ITGB. This will ensure that issues regarding protection of sensitive information are addressed at the highest governance level. It will also demonstrate to all stakeholders the importance the FTC places on protecting sensitive information.

[25] The Computer Security Act of 1987, PL 100-235, defines sensitive information as information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. At the FTC, sensitive information would include information such as filings under the Hart-Scott-Rodino Premerger Notification Program, and law enforcement activities.

[26] The FTC CPO previously served as a Co-Authorizing Official. As of September 3rd, 2015, the CPO role was changed to limit the CPO area of responsibility to Privacy issues and the CPO no longer serves as a Co-Authorizing official.

Recommendation – FY 2015 – 04: **Privacy -** FTC should elevate the Chief Privacy Officer to be a full voting member of the ITGB. – Estimated Program Impact **–** Moderate

(Also see recommendation FY 2015 – 01 regarding organization of the governance boards)

6.2 Configuration Management

Recommendation FY 2014-03 in the OIG FY 2014 FISMA evaluation provided for development of a Configuration Management (CM) Plan that ensures consistent, secure change control across all FTC systems. The current schedule is to complete all the configuration documents by the end of first quarter FY 2016, with implementation in the second quarter of FY 2016.

Information systems are continually changing. Information system change may result from response to a number of factors such as implementation of new, enhanced, corrected, or updated hardware and software capabilities, patches for correcting software flaws, new security threats, and changing business functions. CM is the process for managing system change such that systems reliably perform authorized business functions and protect information assets. Under basic CM concepts, an effective CM program requires:

- Development and documentation of functional and security performance baselines and procedures for orderly, controlled changes to those baselines;
- Procedures for developing systems that comply with established baselines;
- Procedures for correcting errors (e.g., software patches) that do not affect authorized baselines;
- Version control for software, documentation, and other system components to ensure continued compliance with authorized baselines as systems evolve; and
- Reporting to decision makers that systems are performing within authorized baselines.

OMB, NIST, and DHS recognize the importance of CM. Consequently, CM is a critical element in the NIST RMF and is a specific reporting metric in the annual OIG FISMA evaluations.

FTC needs to address CM on multiple levels: at the lowest level, CM needs to ensure that the components, configuration settings, and all other attributes (e.g., security artifacts) of a system are properly baselined and that changes to that baseline are made in a controlled, orderly manner.

This lowest CM level is typically the responsibility of the System Owner where the performance of CM work steps might be the responsibility of a product owner or service supplier or a combination of FTC, product provider, and contract staff;

The second CM level addresses control and change issues associated with documentation and coordination of the administration and technology components that allow different systems with different System Owners and implementation approaches to effectively interact; and at its highest level, an agency CM plan defines the criteria and objectives for subordinate CM plans. The agency-level CM plan is designed to ensure consistent CM control across an organization and standardized CM status reporting.

Recommendation – FY 2015 – 05: **Configuration Management** – FTC should review its CM strategy to ensure that it is addressing CM from the agency perspective and not a single, system level approach. – Estimated program impact – Moderate

6.3 Identity and Access Management / Remote Access Management

FTC has in place processes and procedures that minimize the potential for a security failure originating from the FTC infrastructure, or an infrastructure-supported application. Remote access to the infrastructure is accomplished through an encrypted virtual private network (VPN) that requires two-factor authentication using a token-generated session password. The VPN is configured to isolate use of remote device capabilities from a VPN session with the FTC infrastructure. The two-factor authentication approach, while not HSPD-12 compliant, provides the strength and assurance required for FTC infrastructure remote access under NIST SP 800-63, *Electronic Authentication Guideline*. The potential impact from remote access security failures is also minimized by use of capabilities that allow remote deletion of the software and data stored on remote devices that are reported lost or stolen (e.g., laptops, smart phones, and BlackBerrys); limiting the devices and device types that may connect to the infrastructure; and requiring encrypted storage for all FTC laptops.

Implementation of PIV-compliant Identification and Authentication (I&A) at the FTC – first identified in the OIG's 2010 FISMA evaluation – continues to be deficient. Physical compliance for the FTC Headquarters and at the Constitution Center satellite facility is substantially complete. Logical PIV compliance was delayed due to other Mobile Device Management (MDM) project priorities and is still in a planning phase.

In FY 2015, two initiatives had a significant impact on FTC I&A. As part of its MDM effort, effort, FTC deployed smart phones to replace its BlackBerrys with Personal Digital Assistants (PDA) (i.e., smart phones) that provide computing capabilities as well as voice, text, and video communications; and FTC replaced its legacy SAFE remote access Virtual Private Network

(VPN) with a modern Citrix VPN. Deployment of the smart phones resulted in a number of technical issues affecting performance and utility that are still being resolved. For example, there were a number of "dead zones" in the Constitution Center requiring network reconfiguration to provide communications services, and FTC had to install certificate-based access control for required security and to resolve connection problems with phones accessing FTC and non-FTC service providers. The schedule for implementation of the Citrix-based VPN was accelerated because the legacy system was experiencing performance issues. Accelerating the VPN implementation resulted in performance issues that continued to adversely impact reliability and performance through September 30, 2015, the end of the FY 2015 FISMA evaluation period.

In response to an OIG recommendation (FY 2014 – 01: Security Management Structure), the OCIO stated that its CPIC practices had been revised to ensure that capital planning and investment control practices were aligned and supported by the IT governance process, and that procedures for documenting risk-based decisions were improved. However, available information contained in FTC's new agency performance reporting dashboard and governance practices[27] indicates that neither project fully complied with FTC security and acquisition policies. The areas of concern appeared to be in project planning and documentation of risk-based decisions, and warrant further OIG analysis. While the two projects were identified as areas of concern, use of the new FTC Dashboard-focused information displays, implemented as part of FTC's continuous monitoring program, provided the capability to make this determination, demonstrating the value of the Dashboard reporting tools.

FTC should focus on achieving full compliance with PIV-enabled I&A. While physical access compliance is nearly complete, FTC will encounter additional challenges as it modernizes its IT systems. The PIV process was originally designed to resolve I&A issues for systems within a federal enclave (i.e., all federal systems with I&A interlocking I&A environments). As new technologies are introduced through its modernization efforts (e.g., cloud, applications/systems as a service), FTC will have to integrate I&A practices associated with multiple suppliers while remaining compliant with PIV requirements.

Recommendation – FY 2015 – 06: Identity and Access Management / Remote Access Management - 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. – Estimated program impact – Moderate

[27] See FTC Dashboard 7.21.15 Tier 1 2 Only.

6.4 Incident Response and Reporting

FTC has policies and procedures for incident handling. These procedures provide for participation in reviewing and resolving incidents as necessary by the OCIO, CPO, and OIG. FTC reports potential incidents to US-CERT as required.

FTC acquired tools that will allow it to correlate data to identify potential incidents and perform cross-domain analyses. These tools are scheduled to be configured to perform such analyses by the second quarter of FY 2016.

Recommendation – None

6.5 Risk Management/Security Capital Planning

No system or business activity is without risk. The risk impact may be disruption of business function, loss of service to the customer, or unauthorized change, destruction, or loss of information assets (e.g., hardware, software, data). Risk management is the process by which management balances the costs associated with control implementation against the potential impact from a security failure and determines whether the agency's information assets are adequately protected and if not, allocates resources to ensure appropriate risk-mitigating controls are in place.

NIST requires the use of risk-based decisions when tailoring security controls to specific requirements and determining whether to implement a particular control, accept the higher risk associated with a decision to defer implementation, or to implement a compensating control. In all cases, it is the agency's prerogative how or if a particular control is implemented, as long as the decision is risked-based and properly documented.

The NIST RMF also requires that security issues be included within agency CPIC procedures to ensure security issues are given adequate consideration in funding decisions. FTC includes investment analysis within the charters of its governance boards. This provides a linkage between risk-based decisions, CPIC, and other funding processes in accordance with NIST guidance.

In its FY 2014 FISMA report, the OIG recommended that FTC should accelerate its implementation of NIST SP 800-39 compliant risk-based governance and IT investment processes (FY 2014 – 02: Risk Management/Management Structure). FTC initiated an effort to implement risk-based decision making within its governance board practices.

OIG review of documentation generated by the governance boards showed that artifacts demonstrate consideration of risk as a criterion for determining the level of Board review and oversight as well as supporting individual decisions. As discussed in Section 6.1.1, the materials

also showed that the Board procedures need improvement to effectively document critical issues and to ensure that documentation procedures do not impede effective documentation of risks and risk management decisions (see Recommendation FY 2015 – 01: Security Management and Governance Structure). In addition, FTC needs to provide staff guidance as to the format and procedures used to develop cost estimates. Current cost estimates tend to be based on prior experience, with a reliance on Rough Order Of Magnitude (ROM) estimates. While a ROM may be appropriate for planning, as an activity moves toward an acquisition, the agency's cost estimates need to have greater reliability and precision.

Recommendation – None – See FY 2015 – 01: **Security Management and Governance Structure,** Section 6.1.1

6.6 Security Training

NIST guidance requires that individuals have the awareness training necessary to recognize threats and vulnerabilities and use good security practices and take appropriate action to mitigate adverse impacts and protect information assets and role-based training to meet specific job requirements. The content and frequency of security training is established by agency policy. Security best practices provide for an agency-conducted awareness program that includes an annual requirement. Role-based training is the responsibility of the government agency for its employees and the responsibility of a contractor for its staff. Role-based training is to be sufficient in content and frequency to provide the individual with the skills necessary to securely accomplish their responsibilities.

FTC continues its in-place security awareness and training program. The process has been in place for a number of years and has been improved with regard to content and coverage (e.g., coverage of Privacy issues was added several years ago and is updated to cover FTC-specific issues). Content is reviewed to ensure that it is current and scope is reviewed to ensure it reaches the total workforce. The FTC training and awareness activities include frequent e-mail broadcasts, posters, initial and annual refresher awareness training, and role-based security training. Computer-based materials delivery is intended to reach all individuals with authorized access to FTC computing capabilities. Posters and not computer-based techniques are intended to reach the total workforce. As specified in FTC *Security Awareness and Training Policy*, OCIO 12-AT-100, role-based security training is provided to FTC personnel with significant security responsibilities. The scope, depth, delivery format, and frequency of such training varies based on individual role responsibilities.

The FTC also has an organizational emphasis on security and privacy that results in a heightened awareness of the need to protect information and system access. In addition, FTC, as part of its

mission to protect the consumer, develops and disseminates information on threats and vulnerabilities facing users of modern information systems. The information FTC makes available to the public (e.g., https://onguardonline.gov to provide guidance for safe use of the Internet and https://www.consumer.ftc.gov/features/feature-0014-identity-theft to provide hints for avoiding identity theft) is a significant expansion of awareness and training available to the FTC workforce at no additional cost.

FTC policy provides for retention of records relating to annual security and privacy awareness training received by all individuals authorized access to the FTC infrastructure by the OCIO Information Assurance (IAB). Records regarding role-based training provided to FTC staff are also maintained by the IAB. Under FTC policy, FTC contractors are required to maintain records regarding the security training level of their staff. Contractors provide to FTC reports showing the training level of their staff as required. This approach ensures that contractor staff have the training necessary to complete their assigned tasks (in compliance with contract requirements) regardless of when the training was received. The IAB also monitors role-based training provided by contractors to their staff during a contract to ensure that security skills are refreshed as necessary. The security training reports provided by the infrastructure contractor show that ongoing training is being provided.

Recommendations – None

6.7 Contingency Planning

In FY 2013, FTC initiated a program for an enterprise-wide business continuity/disaster recovery program. The focus of this effort was to develop a recovery structure for less-than-catastrophic events followed by enhancements to address catastrophic events on a cold site basis (Disaster Recovery Plan (DRP)). The Information System Contingency Plan (ISCP) was tested for less-than-catastrophic situations as FTC addressed system failures. This testing demonstrated the need for improved information system contingency planning. FTC can address less-than-catastrophic events through its O&M practices. FTC does not have a comprehensive plan to address catastrophic occurrences. FTC had planned to use the satellite office consolidation and alternate site acquisition to become fully compliant with NIST guidelines. However, in FY 2014, FTC management elected to change the approach and evaluate alternate solutions. To date, FTC has not prepared a disaster recovery plan or strategy.

In FY 2015, FTC stated that it was planning to use a cold site strategy for its DRP. However, no documents were provided that demonstrate a viable disaster recovery cold site strategy. FTC OCIO has indicated that a number of disaster recovery alternatives are also being considered.

FTC needs to have an in-place DRP that presents an effective approach for restoring service should its headquarters facility experience a catastrophic failure. The risk to FTC operations from loss of its headquarters facility is partially mitigated by the FTC practice of hosting systems

at non-FTC facilities. However, a number of high value, sensitive activities are hosted at FTC headquarters. Thus, an extended disruption on the headquarters facility will have a significant adverse impact on FTC mission performance.

FTC needs to prioritize its efforts to develop a viable, tested DRP as stated in its response to recommendation FY 2014-06.

Recommendation – FY 2014 – 06: Contingency Plans – is restated. FTC needs to implement contingency strategy that provides a DRP for the FTC headquarters facility.

6.8 Contractor Systems

FTC is dependent on contractors for the proper operation of its systems. Under its current structure, office automation and the most sensitive systems are supported by computing/communications facilities located at FTC Headquarters; administrative systems are typically provided by fee-for-service activities maintained by other federal agencies; and mission-focused systems such as Sentinel and REDRESS are supported through commercial contracts.

In prior FISMA reports, the OIG recommended that FTC use user-focused metrics to evaluate contract performance. OCIO implemented a limited number of such metrics to evaluate network performance between FTC hosted at FTC headquarters and the satellite facility at the Constitution Center.

In reviewing the system status and outage reports, the OIG identified a number of anomalies that indicated that the outage reporting was unreliable (e.g., outage reports reflected server status and not the status of the supported system). In discussing the matter with the FTC Contracting Officer's Representative (COR), we learned that he had reviewed the contractor reporting and had come to the same conclusion (i.e., the reporting was useless as a mechanism for evaluating contract performance). The COR had been developing new metrics that are user-focused and would be able to show the status and performance trends of the Headquarters facility and critical systems. The planned approach requires identification of critical systems and collection of performance data relative to those systems. This approach is a best practice for continuous monitoring and can be used to provide reporting for individual systems or the facility. FTC should continue implementation of this reporting technique and expand use of the technique to other FTC systems.

Recommendation – FY 2015 – 07: Contractor Systems – FTC should implement the user-focused metrics for the FTC Datacenter and determine whether the monitoring approach or similar approach should be expanded to other FTC systems. – Estimated program impact – Moderate

7. STATUS OF PRIOR YEAR RECOMMENDATIONS

This section provides a summary of the status of recommendations included in the OIG's FY 2014 FISMA evaluations and any prior recommendations that remain in progress (Open)[28]. Where OCIO Resolution Dates shown, they were contained in the associated FTC VULNERABILITY COMPLETION VERIFICATION FORM (CVF) used within the OCIO POAM process to close a POAM item. In some cases, POAM items were closed based on OCIO supporting information and not a CVF. [29]

As shown in EXHIBIT 13 below, all recommendations prior to FY 2013 were closed or consolidated with newer recommendations. One recommendation from FY 2013 remains Open. The FY 2014 FISMA report identified six (6) recommendations for improvement. Three recommendations were closed or consolidated through documentation provided by the OCIO.

EXHIBIT 13: OIG Assessment of OCIO POAM Status for OIG Recommendations

Reference	POAM Reference	OCIO Status	OIG Status
FY2011 – 11		Closed	Closed – Consolidated with FY2014-05
FY 2012 – 01	13-01	Closed	Closed – consolidated with FY 2013-01
FY 2012 – 02	13-02	Closed	Closed – consolidated with FY 2013-01
FY 2012 – 03	13-03	Closed	Closed – consolidated with FY 2013 – 03
FY 2012 – 04	13-04	Closed	Closed – Related recommendation FY 2013 – 04
FY 2012 – 05	13-05	Closed	Closed
FY 2012 – 06	13-06	Closed	Closed - Consolidate with item FY 2013-05
FY 2012 – 07	13-07	Closed	Closed
FY 2012 – 08	13-08	Closed	Closed
FY 2013 – 01	11-12	Closed	Closed - Implement an Information Security Continuous Monitoring (ISCM) program as part of an SIEM. Consolidate under FY 2014 - 02
FY 2013 – 02	AR13-002	Closed	Closed – consolidated with FY 2014-04
FY 2013 – 03	AR14-002	Closed	Closed – FY15 completion
FY 2013 – 04	13-04	Closed	Closed - New recommendation FY 2014 – 04
FY 2013 – 05		Closed	Closed – Additional CP testing scheduled
FY 2013 – 06		Closed	Closed – Metrics reviewed as part of FY 2014 evaluation
FY 2013 – 07			Open – Scheduled FY 2016 resolution
FY 2014 - 01		Closed	
FY 2014 - 02		Closed	
FY 2014 - 03		Open	
FY 2014 - 04		Open	
FY 2014 - 05		Closed	
FY 2014 - 06		Open	

[28] A recommendation is OPEN if the OCIO proposed recommendation is not sufficiently complete to mitigate the associated vulnerability.

[29] The OIG determines that a recommendation is closed when the vulnerability is mitigated even though the mitigating actions may be ongoing.

EXHIBITs 14 and 15 provide the status of prior year recommendations.

EXHIBIT 14: Status of FY 2013 OIG Recommendations

STATUS OF FY 2013 OIG RECOMMENDATIONS					
Reference	**Paragraph**	**Recommendation**	**Potential Impact**	**OCIO Action Plan[30]**	**OIG Assessment**
FY 2013 – 03: Incident Response	6.5	FTC should define development of its SIEM as an IT investment subject to oversight by the FTC IT governance boards.	Moderate	FTC will: 1. Immediately inform the Technology Council and Governance Board of OCIO's efforts to establish a Security Information and Event Management Plan (SIEM) and initiate quarterly status reporting of all SEIM activity to the Technology Council and Governance Board beginning in the second quarter FY 14. 2. Design Remedy reports to capture issues with enterprise security and availability. 3. Implement and configure the current version of our log management and event correlation tool. 4. Initiate the creation of event correlation and event alerting rules on our log management and event correlation tool. 5. Develop a procedure to correlate the Remedy reports with the events generated by our log management and event correlation tool.	**CLOSED** The FTC developed a basic strategy, but is behind schedule on the elements identified in the OCIO mitigation provided in response to FY 2013-03. OCIO is in process of developing a revised implementation approach consistent with its new strategy. Interim materials provided by OCIO indicate that its governance process is developing a SIEM under governance board oversight.

[30] OCIO comments are presented as provided

EXHIBIT 14: Status of FY 2013 OIG Recommendations

STATUS OF FY 2013 OIG RECOMMENDATIONS					
Reference	**Paragraph**	**Recommendation**	**Potential Impact**	**OCIO Action Plan[30]**	**OIG Assessment**
				Complete plan implementation by first quarter 2015.	
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** 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.

EXHIBIT 15: Status of FY2014 FTC OIG FISMA Evaluation Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[31]	OIG Assessment
FY 2014 – 01: Security Management Structure	6.1	Continue to evolve FTC governance practices and expand the use of CPIC and investment analysis processes to document investment decisions. Ensure that risk-based decisions are appropriately documented for input to Information Security Continuous Monitoring (ISCM) reporting.	Moderate	Work is underway on this recommendation. In partnership with agency stakeholders, OCIO revised its IT governance process in the summer of 2014 to ensure that capital planning and investment control practices were aligned and supported by the IT governance process. This is critical to ensuring that technology spending aligns and supports mission and business objectives. As part of the reform effort, OCIO is requiring all new IT investments for development, modernization, or enhancement be supported by a business case. The Business Council is conducting thorough reviews of all business cases, while Governance Board is reviewing the most significant of them. In the first quarter FY 15, the decision-making documentation was enhanced to better document the risk-based decisions made during the governance process and will be used to provide input to the ISCM reporting. Documents that support this include: 1) the revised Business Case template, which includes analysis of business risk attendant to the	**CLOSED** FTC governance practices are evolving. Documentation is improving and OCIO is providing "dashboard" style reporting to facilitate identification of issues that adversely impact investment performance. Subsequent OIG evaluations will continue to assess process maturation in accordance with DHS guidance.

[31] OCIO comments are presented as provided

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[31]	OIG Assessment
				investment as well as risks related to privacy and data security; 2) ITBC meeting agenda; 3) ITBC meeting minutes; 4) Status/Decision summary of all business case reviews and approvals.	
FY 2014 – 02: Risk Management / Management Structure	6.1.2	FTC should accelerate its implementation of NIST SP 800-39 compliant risk-based governance and IT investment processes. These processes should be applied to the FTC IT modernization effort and its associated activities.	Moderate	As part of developing a capital planning and investment control process to align technology-business objectives and to the meet law (Clinger Cohen Act) and other guidance, such as NIST SP 800-39, FTC is implementing a capital planning and investment control program. All modernization efforts are going through the Select process and as appropriate, governance review. Documents that support this include: 1) the revised Business Case template, which includes analysis of business risk attendant to the investment as well as risks related to privacy and data security; 2) ITBC meeting agenda; 3) ITBC meeting minutes; 4) Status/Decision summary of all business case reviews and approvals.	**CLOSED** OIG review of documentation provided by the OCIO and evaluation of FTC business cases demonstrated that FFTC governance processes are evolving toward the risk-based model defined by NIST.
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	**OPEN** The Draft CM plan has not been provided.

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[31]	OIG Assessment
				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.	
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	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	**OPEN**

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[31]	OIG Assessment
		implementation guideline, a security baseline for testing, and a reference for individuals assessing the level of control compliance.		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.	
FY 2014 – 05: Remote Access Management	6.5	FTC should apply its revised governance process to PIV implementation so that compliance is not subject to continuing delay.	Moderate	PIV implementation went through the revised IT governance process in March 2015. The business case for PIV card logical access was discussed and approved by the IT Business Council (ITBC) on March 20th, 2015. Documents supporting this include: 1) the PIV card Business Case; 2) ITBC meeting agenda; 3) ITBC meeting minutes; 4) Status/Decision summary of all business case reviews and approvals.	**CLOSED** FTC is monitoring the status of its PIV implementation. Facets of the PIV implementation are subject to revision as FTC implements new technological solutions where there is not yet a government-wide PIV solution.

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[31]	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**

8. SUMMARY OF FINDINGS AND RECOMMENDATIONS

In FY 2012, 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 introduction of security weaknesses.

In support of this initiative, FTC developed policies and procedures and instituted a governance program to provide consistent planning and oversight of FTC information security investments. Completion of this security initiative was complicated by the need to maintain normal operations turnover of Executive and Senior management, consolidation of two FTC satellite offices into one located at the Constitution Center, and changes in the FTC threat/vulnerability profile. FTC was able to maintain a security environment that protected its information assets while addressing these challenges as was evidenced by annual OIG FISMA evaluations.

OIG FISMA evaluations also showed that meeting its challenges to change came at a cost. In focusing on immediate requirements, FTC was not able to institutionalize planning and risk management practices that would improve their consistency and facilitate controlled integration of new technologies. As a result, functional requirements and security artifacts to support the facility consolidation effort were not present or current; architecture documentation was sufficient to support operational requirements, but not strategic planning; and baseline system performance metrics were not available. FTC was able to mitigate the immediate challenges through the efforts of its staff and contractor support, but the underlying programmatic issues remain. Our FY 2015 evaluation demonstrated that these shortfalls resulted in information systems that did not deliver the anticipated benefits and at higher costs than estimated.

In FY 2015, DHS directed that a maturity model be used as the criteria for the FISMA evaluation. Assessment of the FTC Continuous Monitoring Management environment showed that FTC, from a security control perspective, is operating at a Maturity Model Level 2: FTC has policies and procedures in place, but implementation of those policies and procedures is inconsistent. This results in a level of risk that is higher than desired and projects that exceed cost estimates and do not provide anticipated benefits.

As shown in EXHIBIT 16, the OIG has provided seven recommendations for improving FTC's information security practices. The recommendations emphasize the role of governance and risk-based decisions with an implementation approach that allows FTC management to modernize its information management and analysis capabilities while maintaining effective security, containing costs, and promoting use of continuous monitoring for situational awareness.

Over the past three years, OIG FISMA evaluations resulted in the same conclusions: FTC security and privacy programs are sufficiently comprehensive to protect the confidentiality, integrity, and availability of FTC information assets; FTC responds quickly to mitigate identified specific vulnerabilities and threats; and concern for security and privacy is embedded throughout the workforce. For example, in FY 2013, OIG made seven recommendations for improvement, five were closed or consolidated. In FY 2014, OIG made six recommendations, three were closed, and three remain open. In addition, improvements in its governance practices now provide the information necessary to identify and correct problem projects.

The FISMA evaluations also recommended improvements in governance and oversight to institutionalize security and privacy programs; increasing program maturity, consistency, and reporting. While response to the governance and oversight recommendations has been positive, progress has been slow and inconsistent, evidenced by the delay in implementing effective metrics and monitoring techniques, inconsistent compliance with planning and acquisition policies and procedures, and deficiencies in documenting decisions.

FTC needs to increase its efforts to institutionalize and mature its information security and privacy programs.

EXHIBIT 16: FY2015 FTC OIG FISMA Evaluation Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[32]
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.	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,

[32] OCIO comments are presented as provided.

EXHIBIT 16: FY2015 FTC OIG FISMA Evaluation Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[32]
		(Also, see recommendation FY 2015-04 to elevate the CPO to voting membership on the ITGB)		and update the FTC Administrative Manual to provide a governance guidance framework for all FTC staff. **Expected Completion Date**: FY2017 Q2
FY 2015 – 02: FTC Security Policy and Procedures/System Accreditation Boundaries	6.1.2	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.	Moderate	Management concurs and has completed the installation of the Cyber Security Assessment and Management (CSAM) tool to assist 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
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

EXHIBIT 16: FY2015 FTC OIG FISMA Evaluation Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[32]
FY 2015 – 04: Privacy	6.1.4	FTC should elevate the Chief Privacy Officer to be a full voting member of the ITGB. (Also see recommendation FY 2015 – 01 regarding organization of the governance boards)	Moderate	Management concurs. Planned actions for FY16 include: • Elevate the Chief Privacy Officer to be a full voting member of the ITGB. **Expected Completion Date**: FY2016 Q2
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. • 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. • Develop plans for further integration of PIV Card two-factor authentication as the I&A for all FTC Enterprise-wide systems.

EXHIBIT 16: FY2015 FTC OIG FISMA Evaluation Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[32]
				Expected Completion Date: FY2017 Q2
FY 2015 – 07: Contractor Systems	6.8	FTC should implement the user-focused metrics for the FTC Datacenter 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, 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

Appendix A: FTC OIG CyberScope Response

This page intentionally left blank.

Contact the OIG

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

(202) 326-2800

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.