OIG Independent Evaluation

of the Federal Trade Commission's
Information Security Program and Practices
For Fiscal Year 2017

Report No. AR 18-03// March 2018

FINAL REPORT
REDACTED FOR PUBLIC RELEASE

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

Office of Inspector General

February 27, 2018

MEMORANDUM

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

FROM: Roslyn A. Mazer
Inspector General

SUBJECT: Transmittal of *the Final Report Assessing the Federal Trade Commission's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2017*

As required by the Federal Information Security Modernization Act of 2014 (FISMA), attached is our annual independent evaluation of the FTC's Information Security Program and Practices for Fiscal Year (FY) 2017.

We contracted with TACG LLC (TACG) to conduct this independent evaluation. TACG conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation.

TACG is responsible for the evaluation and the conclusions expressed in the report. In connection with the contract work, we monitored TACG's work and progress and reviewed TACG's report and supporting documentation. This independent evaluation did not constitute an engagement in accordance with *Government Auditing Standards.*

Purpose

The objective of this independent evaluation was to assess the effectiveness of the FTC information security and privacy programs at September 30, 2017. Through our analyses of FTC policies, procedures, supporting systems, and products produced, we assessed the level of maturity of the FTC information security and privacy programs and the FTC's compliance with the FISMA statute

and guidance from the Office of Management and Budget, Department of Homeland Security, and the National Institute of Standards and Technology.

Results

For more than five years, the OIG assessed the FTC information security and privacy programs as strong and robust, but overly dependent on manual operations and with planning and governance deficiencies. The FTC gradually improved its information security and privacy control environments and evolved toward the NIST information security approach that focuses on defined, documented, and repeatable processes with risk-based decisions. For example, the FTC completed its Personal Identity Verification (PIV) implementation. Individual access to FTC systems is now controlled through the common credentialing and standard background investigation process required by Homeland Security Presidential Directive 12 (HSPD-12). The HSPD-12 process requires strong individual authentication for issuance of PIV credentials and two-factor authentication to validate individual access. The implementation of PIV significantly strengthens access control for FTC systems.

The OIG assessed that the current state, legacy systems remained effective for FY 2017 in providing protection for FTC information assets. However, the FTC can expect increased system outages and lost productivity and associated costs as its legacy systems exceed their projected life span and management focuses on the IT modernization instead of operations and maintenance of its in place systems. We note that while the data collection period for this evaluation closed on August 31, 2017, management continued to address improving its information security and privacy programs. Our FY 2018 FISMA evaluation will assess those efforts.

Our FY 2017 FISMA assessment showed that the FTC information security program continues to decline. In our FY 2017 evaluation, using the maturity model created by the Council of the Inspectors General on Integrity and Efficiency, we assessed four of the five functional areas as Defined and only one as Consistently Implemented. This demonstrates a decline in two of the five functions (Identify and Respond), and no improvement in the other three. The OIG identified vulnerabilities and areas of weakness in the FTC information security program and developed recommendations for their mitigation. TACG reported nine recommendations within three of the five CyberScope cybersecurity functions. These recommendations address weaknesses that have been repeatedly identified in previous FISMA reports.

The following chart shows when the OIG raised these concerns over the past three years.

Distribution of OIG FISMA Recommendations by NIST Cybersecurity Function

	Total Count	FY 2015	FY 2016	FY 2017
Identify	14	5 recommendations	4 recommendations	5 recommendations
Protect	6	2 recommendations	1 recommendation	3 recommendations
Detect	2		2 recommendations	
Respond	1			1 recommendation
Recover	1		1 recommendation	
	24	7	8	9

Notable Concerns

- The scheduled FY 2017 award for the IT modernization support contract is delayed. Delay to the IT modernization effort increases the need to continue use of the agency's legacy systems.
- The FTC elected to accept increased availability risks of its legacy systems to increase resource allocations to the IT modernization effort. Deficient configuration management of its legacy systems contributed to increased time and costs associated with recovery from FY 2017 service disruptions.
- The FTC does not have an effective, compliant Plan of Actions and Milestones (POA&M). A deficient POA&M process limits the FTC's ability to know if all vulnerabilities are being mitigated and at what cost.
- Because the information security program and privacy programs are closely related, requiring specific program coordination, deficiencies in the FTC information security program result in a decrease in the effectiveness of the FTC privacy program. The FTC privacy program relies on the information security program for maintenance of an effective control environment for the FTC's sensitive data, specifically, information subject to the Privacy Act and Controlled Unclassified Information.
- The FTC needs to ensure that its information security program is operating effectively for its legacy systems as it proceeds with its multi-year IT modernization effort. FTC information assets are protected by the information security controls inherent in its legacy systems. If its

information security program effectiveness continues to decline, the FTC can anticipate a decrease in its ability to protect its information assets, resulting in an increase in lost productivity costs and work force frustration. For example, the OIG reviewed the two significant outages the FTC experienced in FY 2017. Based on FTC impact estimates, these outages together may have resulted in lost productivity costs of more than $700,000.

The OIG developed nine recommendations to improve the FTC's information security program. We compared our FY 2017 recommendations to our prior recommendations that the FTC has not yet implemented. We then aligned the open recommendations with our FY 2017 recommendations to encourage programmatic mitigations. Our alignment resulted in the consolidation of 12 prior recommendations with eight FY 2017 recommendations. This consolidation will preserve the agency's work to address our prior recommendations and facilitate resolution of all OIG recommendations.

Management concurred in the nine recommendations in this year's report and committed to provide action plans to address them within 60 days. We appreciate the cooperation from management and staff and acknowledge the commitment of the Office of the Chief Information Officer, Chief Privacy Officer, Chief Financial Officer, and Office of the Executive Director to ensuring information security and privacy protections at the FTC.

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

Cc: Svetlana Gans, Chief of Staff to the Acting Chairman
David B. Robbins, Executive Director
David Rebich, Chief Financial Officer
Raghav Vajjhala, Chief Information Officer
David C. Shonka, Acting General Counsel
John Krebs, Acting Chief Privacy Officer
Patricia Bak, Deputy Executive Director
Joseph D. Oleska, Jr., Deputy Chief Financial Officer
Tonia Hill, Internal Control/Risk Management Program Lead
Jaime Vargas, Chief Information Security Officer
Jacalyn Johnson, Assistant Director for Risk and Policy Management
Jeanne Bumpus, Director, Office of Congressional Relations
Donald S. Clark, Secretary of the Commission

FISCAL YEAR 2017
FEDERAL TRADE COMMISSION
INDEPENDENT EVALUATION
OF THE
FTC'S INFORMATION SECURITY PROGRAM AND PRACTICES

CONDUCTED UNDER THE
FEDERAL INFORMATION
SECURITY MODERNIZATION ACT OF 2014

Submitted to:

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

March 1, 2018

Submitted by:

TACG, LLC
Contract Number: 29FTC116C0050

EXECUTIVE SUMMARY

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

- protects consumers by stopping unfair, deceptive or fraudulent practices in the marketplace, and

- promotes competition by enforcing antitrust laws and helping to keep our marketplace open and free.

For Fiscal Year (FY) 2017, the FTC requested funding of $342,000,000 and staffing of 1,211 Full Time Equivalent (FTE) staff. The FTC budget allocates approximately 54% of its requested resources to consumer protection activities and 46% to promoting competition. Fifty-eight percent (58%) of the FTC budget is appropriated from the General Fund and approximately forty-two percent (42%) is provided through Offsetting Collections through the Hart-Scott-Rodino Act for compliance with its mergers and acquisitions review requirements and "Do Not Call Fees."

FTC consumer protection and competition promotion activities result in the collection, retention, and use of large volumes of sensitive information such as Personally Identifiable Information (PII); competition sensitive information; intra-agency and interagency reports; and internal memoranda, correspondence, work papers; and records compiled for law enforcement proceedings. The FTC uses manual and automated controls to ensure the confidentiality, integrity, and availability of its information assets. The FTC recognizes that its reputation for protecting its information assets is paramount to its continued ability to collect the information it needs to successfully complete its missions.

Evaluation Objective

In 2014, the Congress passed and the President signed the Federal Information Modernization Act (FISMA), Public Law 113–283. Through FISMA, Congress recognized that federal information must be effectively managed as strategic assets to ensure effective operation and completion of agency missions. FISMA assigned responsibility for developing information protection policies, standards, and guidelines to the Office of Management and Budget (OMB), the Department of Commerce (DOC), and the Department of Homeland Security (DHS). FISMA requires that all federal agencies implement information security and privacy programs that comply with OMB, DOC, and DHS requirements and provide reasonable assurance that their confidentiality, integrity, and availability is adequately protected.

FISMA requires an annual independent evaluation of the effectiveness of agency information security programs. These evaluations are conducted by Inspectors General (IG) appointed under the Inspector General Act of 1978 or by an independent external auditor, as determined by the Inspector General of the agency. The independent assessment includes testing of the effectiveness of information security policies, procedures, and practices of a representative

subset of the agency's information systems; and an assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

CyberScope Metrics vs OIG FISMA Independent Evaluation

The DHS issues reporting guidance, maintains the CyberScope reporting system, and supports OMB analysis of CyberScope OIG reporting. The annual independent FISMA evaluation assesses the maturity of agency information security and privacy programs using a Council of Inspectors General on Integrity and Efficiency (CIGIE) maturity model (CyberScope Metrics) and a written report (FISMA Report) with content and format determined by the agency IG.

In FY 2015, the DHS revised its OIG reporting metrics with the CIGIE maturity model to evaluate the maturity of agencies' information security programs on a 5-level scale: Level 1- Ad Hoc; Level 2 – Defined; Level 3 – Consistently Implemented; Level 4 - Managed and Measurable; and Level 5 - Optimized. The CyberScope metrics are used to measure FTC progress in establishing and improving its information security and privacy programs by comparing metrics between fiscal years. The OIG focused its FY 2017 FISMA Report on the asset protection effectiveness of the FTC information security and privacy programs.

Both the FISMA and CyberScope reports use the five functional areas (Identify, Protect, Detect, Respond, and Recover) of the National Institute of Standards and Technology (NIST) Cybersecurity Framework as a reporting structure. This facilitates analysis of information security and privacy controls. Alignment of the CyberScope and FISMA Report allows comparison of CyberScope results with FISMA evaluations and comparison with CyberScope results for FY 2016 and FY 2017.

Overview of the FTC IT Environment

The FTC protects its information assets through: the FTC information security program under the Chief Information Officer (CIO) and the FTC privacy program under the Chief Privacy Officer (CPO). The FTC information security program ensures that the FTC has a secure and reliable information infrastructure, providing connectivity and computing capability for FTC staff and mission partners. The FTC's CPO coordinates efforts to implement and review the FTC's policies and procedures for safeguarding all sensitive information; information subject to the Privacy Act; and information identified as Controlled, Unclassified Information. The FTC's information security program and privacy programs operate as interrelated programs under guidance issued by the National Institute of Standards and Technology (NIST). Under the NIST guidance, the FTC information security program ensures information systems implement CPO standards and practices for maintaining and managing sensitive information.

The FTC information technology environment consists of a networked central computing facility for primary mission support to all FTC offices. The FTC augments its central facility with support systems provided through other federal agencies (e.g., Department of Interior, General Services Administration) and commercial contractors.

In FY 2015, the FTC initiated a major modernization effort for its information technology infrastructure. The modernization effort is described in the FTC's *Strategy and Transition Plan*

Security and Technology Services FY 2016 – FY 2019 (Transition Plan) dated September 30, 2016. The Transition Plan focused on replacing the FTC centralized computing facility with commercial cloud-based services. The modernization is in progress, but critical elements of the plan are delayed. For example, in its Transition Plan, the FTC estimated award of a Blanket Purchase Agreement (BPA) to support the effort by the second quarter of 2017. As of September 30, 2017, the contract had not been awarded; and risk assessments and enterprise architecture plans were deferred until after BPA award. The FTC also has not updated its Transition Plan to reflect delays encountered or changes to its IT environment.

OIG FY 2017 Independent Evaluation

Supported by TACG, LLC, the OIG conducted the FY 2017 evaluation of FTC information security and privacy programs as required under the *FY 2017 Inspector General Federal Information Security Management Act of 2014 Reporting Metrics*.[1] The primary source documents for baseline information security and privacy requirements are OMB Circular A-130, *Managing Information as a Strategic Resource*, 7/28/2016; and NIST Special Publication (SP) 800-53, Revision 4, 1/22/2015, *Security and Privacy Controls for Federal Information Systems and Organizations*. Data collection was conducted from May 15, 2017 through August 31, 2017. We worked with the FTC to clarify data inconsistencies and information gaps as necessary in developing our FISMA report.

The objective of this year's FISMA evaluation is to assess the effectiveness and status of the FTC information security and privacy programs at September 30, 2017, as required under FISMA and the *FY 2017 Inspector General Federal Information Security Modernization Act Reporting Metrics* V1, prepared by the DHS, Office of Cybersecurity and Communications, Federal Network Resilience and OMB Memorandum M-18-02, Fiscal Year 2016-2017 *Guidance on Information Security and Privacy Management Requirements*.[2] The OIG uploaded its reporting metrics into DHS CyberScope by the October 31, 2017 OMB reporting deadline. The FTC FISMA evaluation report is provided by March 1, 2018 to OMB through CyberScope and directly to the appropriate Congressional oversight committees.

Results of the Evaluation

For more than five years, the OIG assessed the FTC information security and privacy programs as strong and robust, but overly dependent on manual operations and with planning and governance deficiencies (See Exhibit ES 1 for a distribution of recommendations by Cybersecurity Function). The FTC gradually improved its information security and privacy control environments and evolved toward the NIST information security approach that focuses on defined, documented, and repeatable processes with risk-based decisions. For example, the FTC completed its Personal Identity Verification (PIV) implementation. FTC completed this

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

[2] M-18-02, Fiscal Year 2017-2018 *Guidance on Federal Information Security and Privacy Management Requirements* replaced M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements.*

action at 9/30/2017, which addressed our FISMA recommendation *FY 2015 – 06: Identity and Access Management / Remote Access Management.*[3] Individual access to FTC systems is now controlled through the common credentialing and standard background investigation process required by Homeland Security Presidential Directive 12 (HSPD-12). The HSPD-12 process requires strong individual authentication for issuance of PIV credentials and two-factor authentication to validate individual access. The implementation of PIV significantly strengthens access control for FTC systems.

FTC progress, however, has been hampered by frequent senior management turnover, reliance on informal practices, and deficient planning and governance. Further, the Transition Plan to modernize FTC IT capabilities was initiated without sufficient planning (e.g., no enterprise architecture, security architecture, or risk assessment was used in planning the modernization) and FTC elected to prioritize its resources to support the modernization and decrease resources available for its in place legacy systems. We also note that while the data collection period for this evaluation closed on August 31, 2017, management continued to address improving its information security and privacy programs. Our FY 2018 FISMA evaluation will assess those efforts.

Assessment of the FTC Information Security and Privacy Programs

In our FY 2017 evaluation, the OIG assessed that the FTC information security program maturity was declining. Our assessment showed vulnerabilities in all five of the Cybersecurity Framework Function areas:

1. **OIG Assessment of the Identify Function**

   The Identify Function is a foundational element of the Cybersecurity Framework. Activities in the Identify Function are used to develop the organizational understanding needed to manage cybersecurity risk to systems, assets, data, and capabilities. Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

   The FTC information security program is weak in areas related to the Identify Function.

[3] The OIG categorized FY 2015 – 06: Identity and Access Management / Remote Access Management as Completed based on PIV project status information broadcast through the FTC Intranet to the FTC workforce.

Exhibit ES 1: Distribution of OIG FY 2015 - FY 2017 Recommendations by Cybersecurity Framework Functions

Distribution of FISMA Recommendations by Cybersecurity Function and Category					
		Count	FY 2017	FY 2016	FY 2015
IDENTIFY (ID)	Asset Management (ID.AM):	6	FY 2017 – 01 - ID.AM FY 2017 – 02 - ID.AM	FY 2016 – 01 - ID.AM FY 2016 – 02 - ID.AM	FY 2015 – 02: FTC Security Policy and Procedures/System Accreditation Boundaries FY 2015 – 03: Certification and Accreditation
	Business Environment (ID.BE):				
	Governance (ID.GV):	5	FY 2017 – 03 - ID.GV	FY 2016 – 03 - ID.GV, ID.RA	FY 2015 – 01: Security Management and Governance Structure FY 2015 – 04: Privacy FY 2015 – 07: Contractor Systems
	Risk Assessment (ID.RA):	2	FY 2017 – 04 - ID.RA	FY 2016 – 04 - ID.RA	
	Risk Management Strategy (ID.RM):	1	FY 2017 – 05 - ID.RM		
PROTECT (PR)	Access Control (PR.AC):	1			FY 2015 – 06: Identity and Access Management /Remote Access Management
	Awareness and Training (PR.AT):				
	Data Security (PR.DS):				
	Information Protection Processes and Procedures (PR.IP):	2	FY 2017 – 06 - PR.IP FY 2017 – 07 - PR.IP		
	Maintenance (PR.MA):	1		FY 2016 – 05 – PR.IP, PR.MA	
	Configuration Management (PR.CM)	2	FY 2017 – 08 - PR.CM		FY 2015 – 05: Configuration Management
	Protective Technology (PR.PT):				
DETECT (DE)	Anomalies and Events (DE.AE):				
	Security Continuous Monitoring (DE.CM)	2		FY 2016 – 06 – DE.CM FY 2016 – 07 – DE.CM	
	Detection Processes (DE.DP):				
RESPOND (RS)	Response Planning (RS.RP):	1	FY 2017 – 09 - RS.RP		
	Communications (RS.CO):				
	Analysis (RS.AN):				
	Mitigation (RS.MI):				
	Improvements (RS.IM):				
RECOVER (RC)	Recovery Planning (RC.RP):	1		FY 2016 – 08 – RC.RP	
	Improvements (RC.IM):				
	Communications (RC.CO):				
	Total	24	9	8	7

○ *Governance, Risk Assessment, and Planning*

FTC IT Governance is assessed as deficient. There are no formalized governance structures with applicable policies and procedures. The FTC created a number of Boards, Councils, and Project Management Authorities in addition to the FTC's mission-focused organization. Yet there currently is no artifact that clearly describes the roles and responsibilities of these entities and their interrelationships. Moreover, the FTC defers security planning until an acquisition is imminent. The FTC anticipates contracting for development of security planning artifacts such as an enterprise architecture, enterprise security architectures, and risk assessments. This means that the FTC does not have the information needed to evaluate whether a proposed solution or delivered system meets

FTC needs, provides needed security controls, and effectively interconnects with other FTC systems. Acquiring or building information systems without planning typically results in systems that do not meet user needs or provide appropriate security controls. For example, had the FTC conducted a risk assessment of its decision to accept the availability risks associated with its legacy systems, it would have shown that the FTC mission and information assets are dependent on proper operation and control of its legacy systems; any loss of availability or data compromise will immediately impact on FTC information assets. Planning for future FTC systems would not have an immediate impact on the availability of current information assets.

- *Asset Management*

Documentation of and planning for the information system inventory system/process is deficient.

In FY 2016, the FTC revised its project to replace its legacy information systems inventory system and Approval To Operate (ATO) process. The replacement system documentation was deficient as it did not contain a description of the system coverage (i.e., what systems will be included), data elements collected, processes for consolidating data from multiple disparate databases to support enterprise level inventory reporting, and assignment of responsibility for ensuring inventory data is current. Also, FTC had no plan for validating data from the legacy system.

- *Risk Assessment/Risk Management Strategy*

The IT Strategy and Transition Plan discussed risks as something that will need to be addressed, but had no risk analysis to support its technological approach or acquisition method.

As with any significant change, the Transition Plan has associated risks: risks that change will introduce new vulnerabilities, solutions will not provide anticipated benefits, schedules will not be met, or information assets are compromised during transition. Risk assessments are intended to identify such risks and allow management to plan mitigations to allow successful Transition Plan completion should the risks be realized.

2. OIG Assessment of the Protect Function

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

In our FY 2017 evaluation, the OIG determined that the FTC information security program continues to rely on legacy systems and manual controls to protect its information assets. The OIG assessed that the current state, legacy systems remained effective for FY 2017 in providing protection for FTC information assets. However, the FTC can expect increased system outages and lost productivity and associated costs as its legacy systems exceed their projected life span and management focuses on the IT modernization instead of Operations and Maintenance of its in place systems.

- *Information Protection Processes and Procedures*

The FTC recognized that its IT infrastructure required modernization. On September 30, 2016, the FTC issued a *Strategy and Transition Plan* (Transition Plan) for modernization of the FTC IT environment. The Transition Plan is the FTC guide for planning, acquiring, implementing, and operating the IT capabilities that will form the foundation for the future FTC IT processing and information security environment. To be successful, the Plan must provide a "roadmap" and structure that ensures FTC assets are adequately protected during the transition to the modernized environment and after completion.

The OIG reviewed the Transition Plan as part of our FY 2016 evaluation. We determined that the Plan provides reasonable objectives for the modernization effort. However, the Plan does not provide sufficient definitive information or risk analyses to demonstrate that the modernization can be successfully completed within the planned timeframe or cost. We concluded that the FTC modernization, as described, is a high-risk effort that requires heightened management attention. According to documents made available to the OIG during our review, the FTC has not updated its Transition Plan to reflect delays encountered or to address our FY 2016 recommendations. Instead, the FTC is replacing the Transition Plan with the Information Resource Management (IRM) Strategic Plan required under OMB Circular A-130. An FTC IRM Plan that fully addresses Circular A-130 requirements will not provide the specific guidance and direction necessary for successful completion of the FTC modernization effort. Similarly, if the FTC maintains an IRM Strategic Plan that addresses the management needs of the modernization effort, it will not address the Circular A-130 requirements.

- *Configuration Management*

Configuration Management is used to describe those processes that ensure that changes to information system components are orderly, tested, and documented. Two key features of an effective configuration management program are the ability to identify the current status of all components of an information system at any point in time, and change management that applies to system documentation and security artifacts.

In prior FISMA evaluations the OIG determined that Configuration Management (CM) practices for individual systems were generally adequate, but there were ongoing issues regarding quality control (e.g., FTC did not have CM quality practices that ensure consistent levels of monitoring and change control across the agency). We also assessed that CM practices were not modified appropriately as systems scaled in complexity and scope (i.e., as systems got larger and more complex, the quality of and compliance with FTC CM implementations decreased). In FY 2017, the FTC experienced two significant service disruptions: an e-mail system outage and a data center HVAC outage. The FTC concluded that lack of effective configuration management was a significant contributing factor to its ability to quickly identify and resolve the e-mail system outage. The OIG

reviewed the artifacts for both incidents and determined that deficient configuration management practices was a contributing factor in both outages.

The FTC needs to improve its configuration management practices. This is especially important for the FTC modernization effort where the FTC will be replacing or reengineering most of its information systems.

3. OIG Assessment of the Detect Function

The Detect Function enables timely discovery of cybersecurity events. The cornerstone of the Detect Function is an effective Information Security Continuous Monitoring (ISCM) system. The OIG has no new recommendations for the Detect Function. In prior evaluations, the OIG recommended that the FTC implement ISCM and POA&M processes. Without an ISCM, the FTC will not have near real-time status of the effectiveness of its information security and privacy programs it needs to manage risk on a continuous basis and must reissue ATO's through a three-year reaccreditation cycle. Without a POA&M, the FTC will not have the consolidated document needed to record and manage the mitigation and remediation of identified weaknesses and deficiencies.

- *ISCM System*

The FTC does not have an Information Security Continuous Monitoring (ISCM) system. The FTC approved an ISCM strategy and implementation plan several years ago, but has not implemented an ISCM or developed a revised plan; OMB requires that all agencies implement an ISCM system. [redacted] The FTC developed a Privacy Continuous Monitoring Plan in FY 2017. The OIG assessed this plan as adequate, but dependent on the FTC information security plan. Deficiencies in the information security plan adversely impact the Privacy Continuous Monitoring Plan.

- *Plans of Action and Milestones*

The FTC does not have effective, compliant Plans of Action and Milestones (POA&M). OMB requires that agencies maintain a POA&M to track the mitigation status for any vulnerabilities identified in agency information security programs or individual systems (regardless of source). When Privacy controls were added to NIST guidance, the POA&M requirement became applicable to Privacy controls. As part of its modernization-related activities, the FTC replaced its legacy POA&M with a non-compliant process. The replacement system does not provide the FTC with the capability to identify and track the mitigation status all vulnerabilities of its information security controls.

4. OIG Assessment of the Respond Function

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

- *Response Planning*

For more than three years, the OIG recommended that the FTC should implement a viable disaster recovery plan for its Headquarters Data Center. In our FY 2016 assessment, we emphasized that Headquarters Data Center contingency planning should include plans for its Headquarters Data Center and the systems it hosts. The FTC has previously provided viable contingency strategies, but none was implemented. The FTC effort to replace its centralized computing facility with cloud-focused solutions, with its introduction of communications-centric computing and multiple supplier environments, increases the need for comprehensive contingency planning.

In our prior FISMA evaluations, we assessed the FTC incident response plans as acceptable, but needed to be tested. The impact of the lack of testing was evident during outages experienced by the FTC in FY 2017. In these events, the FTC did not activate any of its contingency plans. While deficient contingency planning did not cause the service disruptions, it did significantly increase the service restoration timeframe and associated costs. Lack of effective contingency planning also resulted in FTC's failure to properly report service availability disruptions to US-CERT.

5. OIG Assessment of the Recover Function

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

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

The FTC has not developed a disaster recovery plan and does not have an alternate processing site. The FTC anticipates that its modernization initiative will mitigate its disaster recovery requirements as the FTC shifts its processing to cloud services environments. As previously recommended by the OIG, the FTC must address its capability to recover from significant outages as part of its contingency planning activities. Recovery planning will be critical as the FTC implicitly shifts to the shared security responsibility model used within cloud-based IT environments. The OIG has no new recommendations for the Recover Function.

Recommendations for Improvement

In our FY 2016 evaluation, the OIG made eight recommendations to resolve the identified deficiencies. FTC management concurred with our assessments and planned mitigations had completion dates extending through FY 2019. As shown in ES-1 above, our recommendations address programmatic/systemic vulnerabilities and, as described in NIST documentation, are intended to establish a single information security and privacy program structure. Thus, all OIG recommendations are related to multiple open deficiencies/recommendations provided by the OIG since FY 2015.

Our FY 2017 FISMA assessment shows that the FTC information security program continues to decline. Our FY 2016 evaluation assessed three of the five functional areas as Consistently Implemented with the remaining two areas assessed as Defined. In our FY 2017 evaluation, we assessed four of the five functional areas as Defined and only one as Consistently Implemented (see Exhibit ES 2). DHS/OMB calculated the FTC information security and privacy programs Risk Management Assessment (RMA) rating as "At Risk." The OMB/DHS calculated RMA differs from the OIG assessment of Effective for FY 2017 because the RMA evaluates program maturity whereas the OIG assessment evaluates the *effectiveness* of the FTC Programs to protect FTC information assets; an assessment that considers the security provided by the FTC's legacy systems and compensating countermeasures.

The FTC privacy program relies on the information security program for maintenance of an effective control environment for FTC sensitive data: information subject to the Privacy Act and requirements for Controlled Unclassified Information. Thus, deficiencies in the FTC information security program are reflected with an effectiveness decrease in the FTC privacy program.

Exhibit ES 2: Comparison of FY 2017 and FY 2016 FISMA Maturity Assessments

Cybersecurity Framework Function	FY 2017 Assessment	FY 2016 Assessment	FY 2017 OMB/DHS RMA Rating[4]
Overall	Effective	Effective	At Risk
Identify	Defined	Consistently Implemented	At Risk
Protect	Consistently Implemented	Consistently Implemented	At Risk
Detect	Defined	Defined	Managing Risk
Respond	Defined	Consistently Implemented	At Risk
Recover	Defined	Defined	At Risk

Using the CIGIE maturity model, the OIG assessed the FTC information security program at Level 2, Defined and the privacy program at level 3, Consistently Implemented. In its program evaluation, the OIG determined that basic information security policies and procedures are

[4] Risk Management Assessment (RMA) rating.

present, the effectiveness of the FTC information security program is declining: legacy security practices are being replaced with less-effective practices; the FTC elected to accept increased availability risks of its legacy systems to increase resource allocations to the modernization effort; the modernization effort is behind schedule increasing the need to continue use of its legacy systems; and the reduced performance of the FTC information security program is adversely impacting its privacy program. Thus, when combined, the FTC information security and privacy programs are assessed as Defined.

To strengthen its information security program and resolve OIG-identified deficiencies, the FTC must improve its IT governance, investment analysis, configuration management, and its IT planning and Operations and Maintenance. The FTC must also ensure that consideration for information security is included in investment decisions and governance board oversight of approved projects (e.g., implementation of the Information Security Continuous Monitoring System).

The OIG developed nine recommendations (See Exhibit ES 3) to improve the FTC information security program. We compared our FY 2017 recommendations to our prior recommendations that remain Open. Our analysis showed that while our recommendations were different, they often identified weaknesses in the same programmatic areas. We then aligned the open recommendations with our FY 2017 recommendations to encourage programmatic mitigations. Our alignment resulted in the consolidation of 12 prior recommendations with eight FY 2017 recommendations. Our recommendation consolidation will preserve the work that the FTC has taken to address our prior recommendations, facilitate resolution of all OIG recommendations, and strengthen the FTC information security and privacy programs in a timely manner.

The FTC needs to ensure that its information security program is operating effectively as the agency completes its modernization effort. If its information security program continues to decline, the FTC can anticipate a decrease in its ability to protect its information assets and an increase in lost productivity costs.

Management concurred in our nine recommendations in this year's report and our consolidation of prior recommendations that addressed related vulnerabilities. Management committed to provide action plans to address our recommendations within 60 days of our March 1, 2018 submission of our final report. Management's response to our report is included in its entirety in Appendix B.

Exhibit ES 3: FY 2017 Recommendations

Reference	Recommendation Synopsis	Consolidated Prior Recommendations
FY 2017 – 01 - ID.AM Systems Inventory	*To ensure the FTC has an inventory that contains the information required to describe all its information systems and data holdings, the FTC should document its inventory practices and validate associated databases.*	FY 2016-01-ID.AM

Exhibit ES 3: FY 2017 Recommendations

Reference	Recommendation Synopsis	Consolidated Prior Recommendations
	The FTC should document its system inventory management system and validate the system, database, and management procedures as a trusted FTC ISCM component under configuration control and that supports continuous monitoring. The FTC should also implement a capability to view its inventory as a single database even though it may be constructed as three separate components.	
FY 2017 – 02 - ID.AM ATO Process	*To ensure the FTC has the artifacts required to support decisions to grant Approvals to Operate, the CSAM implementation should be documented, integrity controls implemented, and all artifacts be subject to 100 percent review until data integrity can be established.* The FTC should institute configuration management of its CSAM process; produce security artifacts that support effective analysis of CSAM security controls and granting of an FTC ATO; and validate the CSAM database.	FY 2016-02-ID.AM FY 2015-02: FTC Security Policies and Procedures/Systems FY 2014 – 04 Certification and Accreditation
FY 2017 – 03 - ID.GV IT Governance	*To ensure the FTC has a formal IT governance process in compliance with NIST and OMB requirements, the FTC should revise its IT Governance practices.* The FTC governance documentation should include a Charter that describes the scope and purpose of the governance program and the roles and responsibilities of those entities responsible for its execution and a graphic or other documentation that shows the FTC entities with information governance responsibilities. The governance documentation should show how risk and information security requirements are identified and resolved. Governance artifacts should be subject to configuration management with change management and a formal process for rescinding and or replacing artifacts that are no longer in effect or are replaced.	FY 2015-01: Security Management and Governance Structure
FY 2017 – 04 - ID.RA Modernization Risk Assessments	*To ensure it has a thorough understanding of the risks associated with its IT modernization initiative, the FTC should evaluate the risks associated with its IT current (legacy) state, future state, and activities needed to transition from the current to future state.* The FTC should conduct risk analyses to identify the risks associated with its modernization initiative. These risk assessments should identify the risks associated with maintaining the legacy system until its retirement, the risks associated with the proposed cloud-based target environment, and the risks associated with the transition to the target environment. The assessments should be sufficiently documented to provide for an FTC decision to mitigate,	FY 2016-04-ID.RA

Exhibit ES 3: FY 2017 Recommendations

Reference	Recommendation Synopsis	Consolidated Prior Recommendations
	transfer, or accept risk. Where a risk is accepted, the FTC should include in its documentation a description of the risk accepted and an estimate of the duration and potential impact of an event should the risk be realized.	
FY 2017 – 05 - ID.RM IT Risk Management Strategy	*To ensure it has a comprehensive risk management strategy, the FTC should implement and follow an information security risk management program. The information security risk management program should operate as a component of the FTC ERM.* The FTC should implement an information security risk management strategy that operates as a component of the FTC Enterprise Risk Management program and is applied to all the FTC information systems operated by the FTC or under contract to support the FTC.	FY 2016-03-ID.GV
FY 2017 – 06 - PR.IP Modernization Performance Metrics	*To ensure FTC has the tools it needs to monitor its IT modernization plan, the FTC should establish and follow a routine process for evaluating cost and schedule performance using the September 2016 version of the Strategy and Transition Plan as the baseline.* FTC should collect metrics describing the status and progress of its modernization effort. These metrics should be used to routinely (at least every 6 months) report project cost, schedule and performance status using the September 2016 version as the baseline.	FY 2016-05-PR.IP
FY 2017 – 07 - PR.IP IRM Strategy	*To ensure that the FTC complies with OMB A-130 planning requirements, the FTC should prepare an IRM Strategy that comports with OMB requirements.* The FTC should develop an IRM Plan that addresses the topics OMB identified for inclusion. The FTC should incorporate metrics into its IRM Plan that allow the performance and cost to be monitored. The FTC should monitor IRM Plan status and costs at least on an annual basis	
FY 2017 – 08 - PR.CM Configuration Management	*To ensure that the FTC knows the authorized and actual component status of its information systems at any point it time, it should establish a policy that defines agency-wide configuration management requirements. The agency-wide policy should be augmented by system specific practices. The FTC configuration practices should also be applied to system documentation and security artifacts.* The FTC should develop an agency-wide configuration management policy that applies to any information systems	FY 2014-03:Infrastructure Documentation FY 2015-05: Configuration Management FY 2016-08-RC.RP

Exhibit ES 3: FY 2017 Recommendations

Reference	Recommendation Synopsis	Consolidated Prior Recommendations
	supporting the FTC. The policy should require development of procedures that are specific to individual systems. The FTC configuration management policy should also require configuration control for all system and information security artifacts.	
FY 2017 – 09 - RS.RP Contingency Planning	*To ensure that it has effective contingency planning, the FTC should revise incident response plans and information system contingency plans to ensure that they have tested approaches that are focused on incident response and recovery.* The FTC should revise its incident response and information system contingency plans to ensure they provide viable procedures for responding to system outages and potential sensitive information compromises. The revised plans should include policies and protocols for US-CERT reporting, maintaining activity logs, communications with stakeholders, and After-Action reporting that includes root cause analyses, activity log analyses, and timely reporting. Plans should be tested at least annually.	FY 2014-06: Contingency Planning FY 2016-08-RC.RP

LIST OF ACRONYMS

Acronym	Definition
ATO	Authorization to Operate / Approval to Operate
BCA	Business Case Analysis (analogous to BIA)
BIA	Business Impact Analysis (analogous to BCA)
C&A	Certification and Accreditation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information Security Officer (analogous to IAM)
COR	Contracting Officer Representative
COTS	Commercial-off-the-shelf
CPO	Chief Privacy Officer
CUI	Controlled, Unclassified Information
DRP	Disaster Recovery Plan
DHS	Department of Homeland Security
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014 Previously Federal Information Security Management Act of 2002
FTC	Federal Trade Commission
FTE	Full Time Equivalent
IAB	Information Assurance Branch
IAM	Information Assurance Manager (analogous to CISO)
IG	Inspector General
IRM	Information Resources Management
ISCM	Information Security Continuous Monitoring
ITBC	IT Business Council
ITC	IT Council
ITGB	IT Governance Board
ITMO	Information Technology Management Office (now OCIO)
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally, Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones (also POAM)
PMA	Program Management Authority
PSC	Privacy Steering Committee
SAOP	Senior Agency Official for Privacy
SIEM	Security Information and Event Management
SORN	System of Records Notice
TSD	Task Solution Document

TABLE OF CONTENTS

LIST OF EXHIBITS

Table of Figures

1. INTRODUCTION/BACKGROUND

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

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

For Fiscal Year (FY) 2017, the FTC requested funding of $342,000,000 and staffing of 1,211 Full Time Equivalent (FTE) staff. The FTC budget allocates approximately 54% of its requested resources to consumer protection activities and 46% to promoting competition. Fifty-eight percent (58%) of the FTC budget is appropriated from the General Fund and approximately forty-two percent (42%) is provided through Offsetting Collections through the Hart-Scott-Rodino Act for compliance with its mergers and acquisitions review requirements and "Do Not Call Fees."

FTC FY 2017 accomplishments included:

- Collection of approximately $9 million for return to victims of a Chicago-area fake debt collection scheme;

- A favorable ruling on its complaint to prohibit unfair practices where a company could instruct search engines to restrict or prohibit any seller's use of any keyword (a word or phrase used to instruct a search engine to display specified search advertising), or to require any seller to use any negative keyword (a word or phrase used to instruct a search engine not to display specified search advertising);

- Settlement agreements with operators of two tech support scams that tricked consumers into believing their computers were infected with viruses and malware, and then charged them hundreds of dollars for unnecessary repairs. In some cases, the scams were also used to install malware into consumer's computers; and

- Participation with State Law Enforcement Partners on a Nationwide Crackdown on Student Loan Debt Relief Scams.

FTC consumer protection and competition promotion activities results in the collection, retention, and use of large volumes of sensitive information such as Personally Identifiable Information (PII), competition-sensitive information, intra-agency and interagency reports, and internal memoranda, correspondence, work papers, and records compiled for law enforcement purposes. The FTC uses manual and automated controls to ensure the confidentiality, integrity, and availability of its information assets. The FTC recognizes that its reputation for protecting its

information assets is paramount to its continued ability to collect the information it needs to successfully complete its missions.

In 2014, the Congress passed and the President signed the Federal Information Security Modernization Act (FISMA), Public Law 113–283. Through FISMA, Congress recognized that federal information assets are strategic assets that must be effectively managed to ensure effective operation of agency missions. Congress also recognized that agency controls need to be strengthened and continually improved to ensure the confidentiality, integrity, and availability of our information assets.

The security and privacy controls that FISMA requires to protect federal systems and information assets are described in policies, standards, and guidelines issued by the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the General Services Administration (GSA), and the National Archives and Records Administration (NARA). FISMA requires that all federal information assets be protected by controls that provide reasonable assurance that their confidentiality, integrity, and availability are adequately protected.

FISMA requires an annual independent evaluation of the effectiveness of agency information security programs. These evaluations are to be conducted by Inspectors General (IG) appointed under the Inspector General Act of 1978 or by an independent external auditor, as determined by the Inspector General of the agency. The independent assessment includes testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems; and an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. OMB and DHS issue guidance for these annual independent evaluations.[5]

DHS evaluation guidance provides for two complementary assessments: one, an evaluation of the maturity of an agency's information security and privacy program. The maturity evaluation uses a model developed through a cooperative effort led by the Council of the Inspectors General on Integrity and Efficiency (CIGIE) that evaluates whether agency security and privacy programs are evolving toward an environment where controls are defined, repeatable, measured,

[5] M-18-02, Fiscal Year 2017-2018 *Guidance on Federal Information Security and Privacy Management Requirements* replaced M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements. See 5.f.1)a)* Establish and maintain a comprehensive privacy program that ensures compliance with applicable privacy requirements, develops and evaluates privacy policy, and manages privacy risks; and *Appendix II to OMB Circular A-130 Responsibilities for Managing Personally Identifiable Information* that states "The main body of this Circular establishes general policies for Federal agencies managing information resources. Appendix I to this Circular establishes requirements for information security and privacy programs and provides guidance on how agencies should take a coordinated approach when managing Federal information resources. This Appendix and Appendix I are companion documents; it is important to review the appendices together in order to understand the coordination between privacy and security."

and continuously monitored and improved; and two, a written report where the content and format is at the discretion of the agency IG. The FTC Office of Inspector General (OIG) contracted with TACG LLC to conduct the FTC FISMA independent evaluation for FY 2017.

1.1 FTC Information Technology Environment

The FTC information technology (IT) environment consists of a networked central computing facility that provides information resources for primary mission support to all FTC offices. The FTC augments its central facility with information system support provided through other federal agencies (e.g., Department of Interior, General Services Administration) and commercial contractors. The FTC also promotes a telework environment for FTC staff and contractors.
In 2015, the FTC initiated a major modernization effort for its information technology infrastructure, which is described in the FTC's *Strategy and Transition Plan Security and Technology Services FY 2016 – FY 2019* (IT Strategy and Transition Plan or Plan) dated September 30, 2016. The Transition Plan focuses on replacing the FTC centralized computing facility with commercial cloud-based services. The critical path for this effort includes award of a supporting Basic Purchase Agreement (BPA) originally scheduled for completion by the second quarter of 2017 (see Figure 1). Thus, the modernization effort is currently behind schedule, necessitating continued mission support through its legacy systems.

Figure 2 provides the estimated cost for the transition effort. The estimates include costs associated with the addition of new features and to decommission legacy technology. FTC requested $12,064,000 for FY 2017 to continue implementation of the agency's information technology modernization and optimization plan.

1.2 FTC Information Security

For more than five years, the OIG assessed the FTC information security and privacy programs as strong and robust, but overly dependent on manual operations and with planning and governance deficiencies. The FTC gradually improved its information security and privacy control environments and evolved toward the NIST information security approach that focuses on defined, documented, and repeatable processes with risk-based decisions. For example, FTC completed its Personal Identity Verification (PIV) implementation.[6] Individual access to FTC systems is now controlled through the common credentialing and standard background investigation process required by Homeland Security Presidential Directive 12 (HSPD-12). The HSPD-12 process requires strong individual authentication for issuance of PIV credentials and two-factor authentication to validate individual access. The implementation of PIV significantly strengthens access control for FTC systems.
FTC progress, however, has been hampered by frequent senior management turnover, reliance on informal practices, and deficient planning and governance.

[6] The OIG categorized FY 2015 – 06: Identity and Access Management / Remote Access Management as Completed based on PIV project status information broadcast through the FTC intranet to the FTC workforce.

1.2.1 FY 2015 FTC Information Security Status

In FY 2015, the OIG assessed that while the FTC information security program provided protection for its information assets, FTC needed to improve its security control planning and the quality of its security documentation. We also determined that implementation of the FTC information security program was inconsistent. We assessed that without improvement in these areas, the FTC would not be able to mature its information security program and, as a result, its capability to protect its information assets would deteriorate.

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 an agency, as well as across agencies. The purpose of the CIGIE maturity model is to summarize the status of agencies' information security programs and their maturity on a 5-level scale, and how it is maturing over time. Developing a maturity model is a significant undertaking; DHS and CIGIE segmented the effort into manageable components. Thus, the FY 2015 initial maturity model segment only reflected the status of the Information Security Continuous Monitoring (ISCM) domain. CIGIE would complete maturity models for the remaining four domains in later years. Thus, the FY 2015 results of the maturity model analysis applied only to the ISCM domain.

Using the CIGIE maturity model, the OIG assessed in FY 2015 that the FTC ISCM was at Level 2, Defined. FTC's policies, strategies, and procedures will support a repeatable ISCM program consistent with existing law, policy, standards, and guidelines. OIG also determined that while basic ISCM policies and procedures were present, their implementation is inconsistent and metrics are inadequate to effectively monitor control effectiveness. Our assessment showed that, should FTC ISCM continue its current implementation approach, the FTC ISCM would not mature. The CIGIE model stresses rigorous planning and formal procedures, areas in which the FTC information security program is weak. To resolve OIG-identified deficiencies, FTC IT governance practices need improvement in investment analysis and must include consideration for security in investment decisions and governance board oversight of approved projects (e.g., implementation of the ISCM).

Figure 1: FTC Modernization Schedule September 30, 2016

Transition Schedule

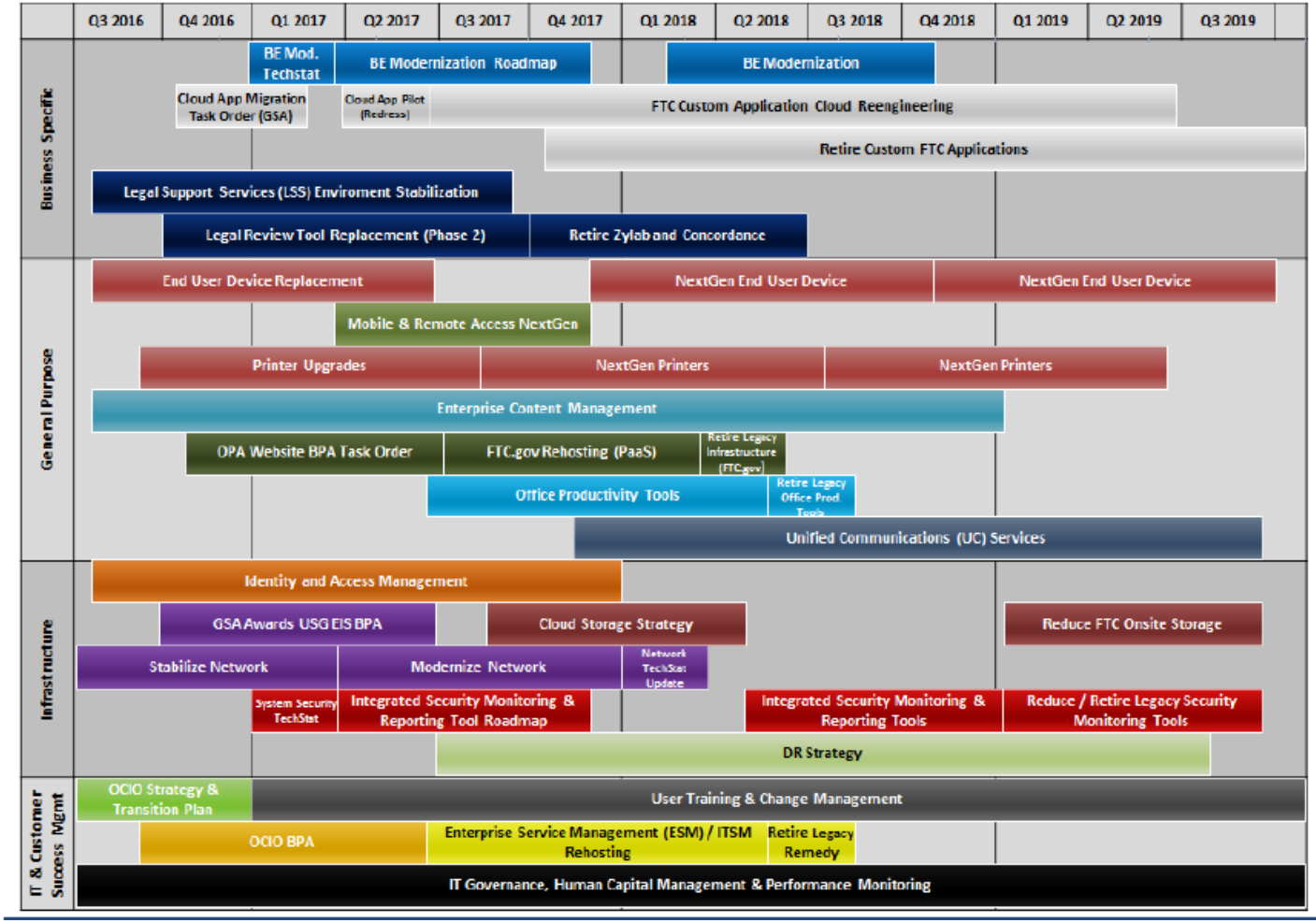


Figure 2: IT Strategy and Transition Plan - Transition Cost

1.2.2 FY 2016 FTC Information Security Status

Our FY 2016 FISMA evaluation showed that the effectiveness of the FTC information security program declined during the year. While legacy controls continued to protect FTC information assets, the risks associated with system and information availability and integrity increased because legacy procedures were being discontinued and FTC planned improvements were delayed. Our scored assessments for the CGIE maturity model identified deficiencies in the FTC information security environment. The OIG did not assess any of the five cybersecurity functions as meeting target effective performance: Level 4, Managed and Measurable. The OIG determined that the FTC information security environment provided effective information asset protection only after consideration of FTC legacy policies, procedures, and systems as compensating countermeasures. Exhibit 1 shows the CyberScope scoring for FY 2016.

Exhibit 1: FY 2016 CyberScope Scored Assessment

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

In FY 2016, the FTC continued its Information Technology (IT) modernization efforts. However, FTC's modernization effort was delayed and suffered from deficient planning and execution. For example, FTC's replacement for its legacy system inventory/Approval to Operate (ATO) process was not supported by a transition plan.[7] At the end of FY 2016, the resulting information systems inventory/ATO processes were not complete and could not provide a complete information systems inventory or support the FTC ATO process. The lack of a transition plan with appropriate quality testing was a major contributor to creation of a system that does not achieve desired results and is now behind schedule.

The approved ***IT Strategy and Transition Plan*** was deficient in that it does not effectively address risks associated with the effort. The Plan describes risk as something that will need to be addressed, but risk assessments would be included in task order solicitations under the pending BPA – and no risk assessments for the *IT Strategy and Transition Plan* were performed as of August 31, 2017. The Plan did not provide an assessment of the risks associated with the Plan's proposed strategy, technological approach, or acquisition method. Further, FTC made little progress in implementing its Information Security Continuous Monitoring (ISCM) system. The FTC acquired software tools that could be used to support continuous monitoring, but there was little progress in configuring those tools to implement this critical security monitoring system.

[7] Approval to Operate (ATO) is an explicit decision by an agency official that authorizes operation of an information system and to explicitly accept the risk to agency operations.

1.3 FY 2017 FISMA Evaluation - Objectives

Our FY 2017 FISMA evaluation assessed the effectiveness of the FTC information security and privacy programs at September 30, 2017. We examined the changes in program maturity through the CIGIE maturity model (CyberScope Report), which is now complete. All FY 2017 metrics are now tailored to the maturity model approach in all five security domains: Identify, Protect, Detect, Respond, and Recover. We examined the scope, quality, and effectiveness of the information security and privacy programs and used that information to respond to the maturity metrics. Through our analyses of FTC policies, procedures, supporting systems, and products produced, we assessed the level of maturity of the FTC information security program and its compliance with the FISMA statute and OMB, DHS, and NIST guidance. Our FISMA Report consists of six Sections:

- Executive Summary – brief overview of the FISMA Report and the findings and recommendations of the evaluation;
- Section 1 – Introduction/Background – Describes the FISMA evaluation process and provides an overview of the FTC information security environment and prior assessments
- Section 2 – Methodology
- Section 3 – FY 2017 Findings and Recommendations – Findings and Recommendations are presented using the NIST Cybersecurity Framework
- Section 4 – Summary of Prior Year Findings
- Section 5 – Summary of FY 2017 Recommendations

2. METHODOLOGY

The OIG conducted this evaluation in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency. Our data collection extended from May 15, 2017 through August 31, 2017. We worked with the FTC to clarify data inconsistencies and information gaps as necessary in developing our FISMA report.

We conducted our FTC FISMA evaluation as two separate but interrelated and complementary assessments:

- First, we assessed the maturity of the FTC information security and privacy programs. This entails an evaluation of the capability of the FTC programs to address the 61 CIGIE metrics distributed across the 5 security Functions/Domains defined in the NIST Cybersecurity Framework (see Exhibit 2). Our maturity assessment examined whether information and Privacy control processes are appropriately defined and formalized and are consistently implemented, measured, and monitored across the agency; and

- Second, we assessed whether in place (current state) security controls effectively protect FTC information assets (data and systems) from intentional or unintentional threats to those assets from internal or external sources, protect against adverse impacts from those threats, and recover information assets should those threats be realized.

Exhibit 2: CIGIE Metrics by NIST Cybersecurity Framework Function

IG Metrics by NIST Cybersecurity Framework Function	
Function (Domains)	**Number of IG Metrics[8]**
Identify (Risk Management)	12
Protect	
Protect (Configuration Management)	8
Protect (Identity and Access Management)	9
Protect (Security Training)	6
Detect (Information Security Continuous Monitoring)	5
Respond (Incident Response)	7
Recover (Contingency Planning)	7
General questions	7
Total Metrics	61

For both assessments, we collected information to align with the Cybersecurity Framework as shown in Exhibit 3.

[8] The CIGIE metrics include a general question for each of the 7 domains.

Exhibit 3: CIGIE Maturity Levels Aligned with FISMA Criteria

Maturity Designation	Level	Description	Assessment Criteria
Ad-Hoc	1	The program is not formalized and activities are performed in a reactive manner.	No policies or procedures are in place.
Defined	2	The organization has formalized its program through the development of comprehensive policies, procedures, and strategies.	The organization has artifacts that are managed and subject to change control. The artifacts define – • An organizational structure where security responsibilities are described and knowledge, skills, and abilities required for role performance are identified and used as a basis for staff assignment and training. • Policies and procedures that comprise an information and technological architecture within an enterprise architecture with an embedded information security architecture. • Information systems are developed, operated, maintained, and retired in accordance with established NIST guidelines, including NIST SP 800-53 required controls. Control measures are equally applied to administrative and mission-focused information systems. • Inventories of all information systems and data collections are maintained. Data collections and data elements are associated with metadata that allows identification and implementation of appropriate CUI categorizations and control measures. • Control measures are tested as required in NIST guidelines. Information systems are subject to a formal Approval To Operate (ATO) process. • Identified vulnerabilities are tracked from identification to resolution through a formal Plan Of Action and Milestones (POA&M) process.

Exhibit 3: CIGIE Maturity Levels Aligned with FISMA Criteria

Maturity Designation	Level	Description	Assessment Criteria
Consistently Implemented	3	Formalized program and controls are consistently implemented across the agency. Qualitative and quantitative measures and data on program and control effectiveness are defined and implemented but are not captured and used to support risk-based decisions.	The program and associated controls are consistently implemented across the organization. Quantitative and qualitative monitoring measures are in place to ensure proper operation of in place controls.
Managed and Measurable	4	Activities are repeatable and metrics are used to measure, monitor, and manage control and program implementation. Metrics are appropriate to achieve situational awareness, control ongoing risk, and perform ongoing (continuous) system authorizations.	Monitoring metrics are routinely collected and use to monitor program and control effectiveness on an on-going basis. Metrics show that programs and program controls are repeatable and provide management the information needed to make and review risk-based decisions.
Optimized	5	The organization's program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.	Program controls produced the information necessary to show the health of the information security control environment relative to established risk acceptance thresholds. Controls and control parameters may be securely modified on a near real-time basis to address changes in mission requirements, applicable threats, and implemented technologies. Adherence to and compliance with information security controls and practices is consistent at all organizational levels and locations.

We requested --

- The policies and procedure comprising the current FTC information security and privacy programs and information system architecture (in place and planned);

- Artifacts that allow us to evaluate program status, such as ATO packages for information systems approved in the current year, the current information systems inventory, migration procedures or plans move legacy systems and data to their replacement, security incident reports, trouble reports, After Action reports, Plans of Action and Milestones (POA&M), and risk assessments and other documents associated with the *IT Strategy and Transition Plan* modernization initiative; and

- Documents describing the FTC organizational structure and identifies those entities with responsibilities or authorities in operating or maintaining the FTC information security and privacy programs.

We also afforded management the opportunity to submit artifacts they believe were responsive to the CIGIE maturity model metrics. To facilitate that effort, we augmented the CIGIE metrics descriptions with specific questions and identified the types of artifacts that would have information relevant to the CIGIE metrics.

We informed management that our preference was for existing artifacts. We stressed that the CIGIE model emphasizes a formal program with defined, repeatable, measurable policies and procedures.

We reviewed all artifacts provided and identified those that were fully responsive, non-responsive, or were inconsistent with artifacts the FTC previously provided (i.e., artifacts were internally inconsistent or were inconsistent with other FTC artifacts). We also held multiple discussions with FTC staff to ensure a common understanding of information requested and to augment documentary information with interview data as appropriate. We modified our requests if the FTC did not have responsive artifacts but proposed appropriate alternatives to provide information using database extracts, summaries of control implementations, or descriptions of control conditions.

Our iterative review process continued until the FTC stated that a response was complete (i.e., the FTC determined that it had no additional information responsive to our request).

The OIG used the information collected to respond to both the CIGIE maturity metrics and prepare our FISMA report. We submitted our maturity metric assessments through the DHS CyberScope system. We used all the information collected in our overall assessment of the FTC information security and privacy programs to –

- analyze areas of concern that were not specifically addressed in the CIGIE metrics;
- assess the effectiveness of the current state information and privacy programs to protect FTC information assets; and
- assess the effectiveness of FTC planning and governance practices to protect its information assets as it modernizes its IT environment.

The OIG identified vulnerabilities and areas of weakness in the FTC information security program and developed recommendations for their mitigation. We identified only one vulnerability for the FTC privacy program: the privacy program's dependence on the FTC information security program. The FTC privacy program relies on support provided by the Office of the Chief Information Officer (OCIO) under the FTC information security program to

provide technical support (e.g., mitigate instances where sensitive data are erroneously stored without appropriate controls, identify potential instances of information compromise).[9] The CPO is responsible for ensuring that suppliers of products and services supporting the FTC privacy program (e.g., the OCIO) are in compliance with federal and FTC requirements. Implementation of the OIG recommendations for the FTC information security program will address the FTC privacy program weakness. Thus, we provided no recommendations specific to the FTC privacy program.

We associated our FY 2017 information security program recommendations with prior OIG FISMA recommendations that were not implemented at September 30, 2017. Where appropriate, we consolidated prior related recommendations in our FY 2017 recommendations. Consolidation of our outstanding recommendations will facilitate mitigation of all OIG identified vulnerabilities and address ongoing areas of concern.

We structured our FISMA report to incorporate information from the CIGIE maturity metrics and our current and future state program effectiveness assessments into a single, consolidated report. Our consolidation allows us to assess whether the FTC information security and privacy programs currently provide an appropriate level of protection and will be capable of continuing or increasing that level of protection as the IT modernization proceeds. Our report structure is also aligned with the NIST Cybersecurity Framework functions/domains shown in Exhibit 4 to facilitate cross-agency analysis.

[9] While security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements. OMB Circular A-130, 4.h.

Exhibit 4: Functions (Domains) of the NIST Cybersecurity Framework[10]

Table 1: Function and Category Unique Identifiers

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

[10] While the Cybersecurity Functions remain consistent, the categories within a function may be expanded.

3. FY 2017 FTC FISMA EVALUATION

The OIG's FY 2017 FISMA evaluation assessed that the effectiveness of the FTC information security program is declining, both in maturity and in its ability to protect FTC information assets. The current state environment (in place controls) protects FTC information assets, but its continued reliance on its legacy systems is raising security risks, primarily in the availability of information assets. Further, the ongoing IT modernization effort has experienced delays, and FTC management elected to accept availability risks associated with its legacy systems in favor of allocating resources to the modernization effort.

The OIG assessed that the FTC information security program is not adequately documented. The Program contains obsolete documents that no longer describe FTC information security practices. Moreover, artifacts intended to document new policies and procedures are frequently non-existent, incomplete, or inaccurate. For example, in FY 2015, the FTC replaced its legacy system inventory with a government-developed *Cyber Security Assessment and Management* (CSAM) product. The FTC anticipated that the CSAM product would support the FTC implementation of NIST's Risk Management Framework as well as maintaining the FTC information systems inventory. However, in implementing CSAM, the FTC did not –

- document the CSAM implementation to describe the data elements it contains, identify the system structure, and standard operating procedures for FTC use;
- analyze CSAM capabilities against FTC requirements to determine whether CSAM could maintain the FTC system inventory and support its ATO process;
- prepare a transition plan to guide implementation of CSAM and ensure the system contains complete, accurate, and current data;
- configure the CSAM product to incorporate FTC security policies; or
- ensure that CSAM correctly generates the security artifacts needed to support FTC decisions to grant information systems their required ATOs.

During the CSAM implementation, the FTC learned that CSAM could not support the FTC's inventory requirements, and the OIG's analysis of the FTC's CSAM implementation showed that the product is also not sufficiently reliable to generate the artifacts necessary for the FTC to make informed decisions to grant ATOs.

To compensate for CSAM deficiencies, the FTC established a SharePoint site to collect inventory information that CSAM could not maintain. The OIG assessed the current FTC inventory as an acceptable listing, but one that requires validation and updating. The FTC has no

procedures in place to ensure the inventory is appropriately updated; and the FTC has still not revised its system boundaries to ensure that all its information systems are appropriately defined, categorized, and approved to operate. We assessed the CSAM artifacts we reviewed to be unreliable and inadequate to support granting an ATO. Failure to maintain an accurate information systems inventory and accurate security artifacts indicates that the FTC information security program will not be capable of protecting FTC information assets as legacy systems are replaced with unknown cloud solutions. Without an enterprise information systems inventory, the FTC lacks a complete understanding of the information assets that need protection. Under FISMA, all information systems must be covered by an FTC ATO before being placed in service. The ATO must be renewed in accordance with NIST guidelines. Without the capability to grant ATOs for its information systems, the FTC will be unable to place new systems into production or to continue to use existing systems with ATOs that require renewal.

The FTC recognizes that its continued reliance on its legacy systems increases information asset risk. In its CyberScope *Risk Management Assessment Response 2017,* the FTC stated that:

> FTC accepts the risk with its aging legacy IT to focus on migration to cloud services. The Agency exercises discretion on its authorization process through changes in policy to cost effectively manage FISMA compliance.

[redacted] from the FTC Chief Information Officer (CIO) to the FTC IT Governance Board, IT Advisory Councils, and OCIO Managers regarding corrective actions for a 2-day Exchange e-mail outage in August 2017, the CIO stated the following:

[redacted]

While the FTC recognizes that there is increasing risk through continued reliance on its legacy systems, the FTC does not yet recognize the security issues that must be identified and mitigated as its IT infrastructure is modernized. For example, in its September 30, 2016 *Strategy and Transition Plan* for its IT modernization initiative, the FTC stated:

> OCIO does not record or otherwise maintain data on customer experience with IT services outside of help desk calls. Anecdotally, and with confirmation from the Office of

[11] Alternate data center (ADC) – A remotely located data center primarily used to maintain backups for FTC programs and data.

> the Inspector General (OIG), OCIO lacks a successful record of accomplishment of delivering new services in a timely fashion especially over the last several years.
>
> and
>
> While the FTC scored above most small agencies, it fell short in several measures for Cross Agency Priority (CAP) goals, and the FTC fell short of an overall "Green" rating for its practices. Most significantly, the OIG rated FTC's contingency planning in most need of improvement.

The *Strategy and Transition Plan*, however, does not identify or discuss the risk associated with the FTC modernization approach, nor does it contain an enterprise architecture (with an embedded information security architecture). For example, the *Strategy and Transition Plan* should have addressed risks associated with replacing its data center-focused architecture with cloud-based solutions offered as commodity services and the increased use of encryption that solution implies. Cloud-based infrastructures involve a combination of hardware and software technologies from different suppliers that operate under a shared responsibility model. A shared responsibility model increases customer risk as the customer must deal with multiple suppliers operating under different contract arrangements (e.g., a cloud solution under a GSA contract typically requires multiple contract arrangements, one for the cloud service acquired and one or more to provide other support services); the increased use of encryption has an associated increased risk because security scanning software does not effectively evaluate encrypted data. The FTC will need improved planning practices and support tools (e.g., risk assessments, an enterprise security architecture, and information security continuous monitoring system) to maintain the protection of its information assets in all phases of the transition to cloud services.

In August 2017, the OIG issued a *Notice of Finding and Recommendation (NFR)* to alert FTC management of our concerns about ***Potential CyberScope Reporting Deficiencies***. In our NFR, we identified that our FISMA evaluations determined that the maturity levels of three (Identify, Protect, and Detect) of the five cybersecurity Functions as Level 1, Ad Hoc. The specific areas of concern were the FTC Information Systems Inventory (Identify Function); FTC Configuration Management practices (Protect Function); and FTC Information Security Continuous Monitoring (ISCM) practices. Management responded to the NFR and made changes necessary to increase our CyberScope assessments to Level 2 – Defined. However, the areas identified in the NFR remain concerns in our FISMA report and require increased FTC management oversight until they are effectively resolved.

Further, in this evaluation we raised the risk impact level associated with the Information Systems Inventory from Moderate to High because deficiencies we identified adversely affect the FTC's ability to identify its information systems, which missions the systems support, and

the security controls they contain. Without a documented, accurate, reliable understanding of its information systems and the controls they use, the FTC will not be able to certify the adequacy of information system controls (i.e., grant an Approval to Operate (ATO)). The inability to renew existing ATOs affects FTC legacy systems. The inability to grant ATOs for new systems will compromise FTC's IT modernization effort. The inventory and ATO deficiencies, combined, indicates that the FTC does not have effective security controls for its information systems.

3.01 FTC Privacy Program

The FTC's CPO coordinates efforts to implement and review the agency's policies and procedures for safeguarding all sensitive information (e.g., Controlled Unclassified Information (CUI)). The CPO extended some privacy controls to protect FTC CUI.

In November 2016, the FTC Privacy Office formalized its privacy program plan for implementing and monitoring privacy controls. The Privacy Program Plan included those Privacy controls described in NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and* Organizations (see Exhibit 5).[12] The Privacy Program Plan describes the structure of the privacy program, its resources, the role of the Senior Agency Official for Privacy (SAOP) and other members of the Privacy Office and the Privacy Steering Committee (PSC), its strategic goals and objectives, and the program management controls and common controls in place or planned for meeting privacy requirements and managing privacy risks. The Privacy Program Plan addressed the requirements for the FTC privacy program. In August 2017, the Privacy Office issued its Privacy Continuous Monitoring Strategy.

Exhibit 5: Select FTC Privacy Program Documents

FTC Privacy Program Documents		
Reference	**Title**	**Date**
None	FTC Privacy Continuous Monitoring Strategy	August 31, 2017
None	Data Breach Notification Response Plan	July 2017
None	Privacy Program Plan	November 2016

The privacy program is dependent on effective information security controls to protect information in digital form and to take action as appropriate to address Privacy incidents. For example, Participation in the Privacy Continuous Monitoring Program (PCMP) will be limited to systems that have a current ATO.[13] Thus, the PCMP is dependent on the reliability of artifacts

[12] Specific Privacy Policies and Procedures are issued under the PSC [redacted]

produced through the FTC CSAM-based process for granting of information systems ATOs (i.e., if CSAM-produced artifacts are deficient, the PCMP will be unreliable); and OCIO practices for mitigating compromises of digital data. Thus, the effectiveness of the FTC privacy program is adversely impacted by deficiencies in the FTC information security program. For example, if an incident results in inappropriate storage of PII on digital media, it is incumbent on the OCIO to use the appropriate tools and procedures to purge the sensitive information and document its successful deletion.

Based on our analysis of an FTC FY 2017 PII incident, we determined that the procedures the FTC used to purge inappropriately stored privacy data were inadequate. In this instance, PII was incorrectly stored on a shared device, where it remained for more than a month. The OCIO procedures did not provide for overwriting the stored data (and associated backups) to ensure the PII was effectively purged, and OCIO follow-up scans did not include tools that an attacker would typically employ to scan digital media. The CPO determined the risk of harm was low in this case because the CPO did not identify any indication that the information was viewed, accessed or used by any unauthorized person; the data was in XML format, which is not easily discernable or readable to the average user; and it was saved in a folder that only two contractors readily accessed. However, while the risk of information compromise may be low in this instance, the OCIO's failure to use appropriate tools to purge the PII meant that, due to the CPO's dependence on OCIO practices, the CPO cannot authoritatively state whether inappropriately accessed or stored PII has been effectively purged from FTC information systems.

3.02 OIG Assessment of the Effectiveness of FTC Information Security and Privacy Programs

As shown in Exhibit 6, the OIG determined that the appropriate Overall Rating for the FTC information security program for FY 2017 is Effective. Based only on the OIG CyberScope submission, DHS assigned FTC a Risk Management Assessment (RMA) rating of "At Risk.". Our RMA Effective rating is a combination of our CyberScope response and our overall assessment of the FTC information security and privacy programs. Our OIG combined response recognizes the vital importance of protecting FTC information assets *in the current environment*. Our analysis therefore adjusts for the impact of compensating controls to mitigate vulnerabilities identified through the CIGIE maturity metrics.

Our evaluation of the effectiveness of FTC's Information Security program shows that it is "immature and will not provide effective protection if it continues its current practices (future state control environment)." Legacy controls and information security practices (i.e., current state control environment), while inefficient, are capable of protecting FTC information assets, but the protection they provide does not extend to the proposed modernized FTC IT environment. Our overall assessment of the FTC information security and privacy programs is therefore Effective in protecting FTC information assets in its current state, but its ability to

continue that level of protection is At Risk as its legacy systems are replaced through the IT modernization initiative. Specifically, our assessment means that the information security program can protect FTC information assets today (current state), but is subject to increasing risk as legacy systems deteriorate and the FTC shifts its resources from Operations and Maintenance of existing systems to implementing an as-yet undefined, modernized, cloud-based architecture.

Exhibit 6: FY 2016 OMB/DHS vs FTC IG CyberScope Ratings

Framework	RMA Rating	IG Rating
Overall	At Risk	Effective
Identify	At Risk	Defined
Protect	At Risk	Consistently Implemented
Detect	Managing Risk	Defined
Respond	At Risk	Defined
Recover	At Risk	Defined

The OIG assessed that FTC's privacy program as *Consistently Implemented* on an overall basis. The privacy program has a structure and focus that could be assessed at Level 4 - *Managed and Measurable*. However, the privacy program is dependent on the FTC information Security Program. As stated in OMB Circular A-130,

> "While security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements"
>
> and in SP 800-53, which "establishes a linkage and relationship between privacy and security controls for purposes of enforcing respective privacy and security requirements which may overlap in concept and in implementation within federal information systems, programs, and organizations; and demonstrates the applicability of the NIST Risk Management Framework in the selection, implementation, assessment, and ongoing monitoring of privacy controls deployed in federal information systems, programs, and organizations."

Given the linkages between the FTC information security and privacy programs, deficiencies in the Information Security program reduce privacy program effectiveness. For example, the FTC information security program does not ensure adequate documentation for risk-based decisions, documentation of incident remediation actions, and its ATO process is deficient. These inherited vulnerabilities should be identified through the reviews, tests, and monitoring reports provided through the FTC Privacy Continuous Monitoring Strategy, Privacy Control Assessment Matrix.

In the remainder of Section 3 we describe our findings and recommendations for the FTC information security program. We have no recommendations for the FTC privacy program. In those cases where there is significant overlap between current recommendations and prior recommendations, we consolidate recommendations under the FY 2017 recommendation. This approach ensures that each recommendation is based on our most current assessment of the applicable condition, cause, and criteria. While each of the five Cybersecurity Functions is addressed, we provide findings in only four of the five functional areas. We note that while the data collection period for this evaluation closed on August 31, 2017, management continued to address improving its information security and privacy programs. Our FY 2018 FISMA evaluation will assess those efforts.

3.1 OIG Assessment of the Identify Function

The Identify Function is a foundational element of the Cybersecurity Framework. Activities in the Identify Function are used to develop the organizational understanding needed to manage cybersecurity risk to systems, assets, data, and capabilities. Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

Exhibit 7 provides tabulations for the 12 metrics for the CIGIE Maturity Model Identify Function.

Exhibit 7: OIG CyberScope Metric Counts for the Identify Function

Maturity Level	Count
Ad-Hoc	1
Defined	9
Consistently Implemented	2
Managed and Measurable	0
Optimized	0
Total	12

The OIG's FISMA evaluation identified five weaknesses in the FTC information security program in the Identify Function, one each in the Asset Management, Governance, Risk Assessment, and Risk Management Strategy, as described below.

3.1.1 Information Systems Inventory – Function: Identify Category: Asset Management

Critical to maintaining an effective information security program is an understanding of the information assets that must be protected. Federal law, OMB policy, and NIST guidance require that agencies maintain an inventory of all their information systems.[14] OMB expanded the

[14] An inventory of major information systems is required in accordance with 44 U.S.C. § 3505(c). All information systems are subject to the requirements of the Federal Information Security Modernization Act (44 U.S.C. Chapter 35) whether or not they are designated as a major information system.

inventory requirement to include an enterprise-wide data inventory to account for data used in the agency's information systems.[15]

In FY 2015, the FTC decided to replace its manually-based, but effective Information Systems Inventory system with a system based on the CSAM product offered by the Department of Justice (DOJ). The FTC anticipated using CSAM to improve its inventory and ATO processes by automating creation and maintenance of required security artifacts and absorbing the FTC information systems inventory into the CSAM implementation.[16] In our FY 2016 and FY 2017 FISMA evaluations, we requested a copy of the plan the FTC used to manage the transition from the legacy inventory system to the CSAM-based systems, and for documentation that describes the CSAM implementation and the actions taken to tailor the CSAM product to the FTC environment. We also requested a sample of artifacts generated through the CSAM product for evaluation. The FTC responded that the requested artifacts did not exist.

While the FTC stated that it did not have a CSAM transition plan, we learned that the FTC determined that CSAM did not have the capability to maintain the Information Systems Inventory it needed. The FTC therefore elected to change the system design such that the resulting inventory is divided among three components: one implemented using CSAM; and two implemented using SharePoint. However, in so doing, the FTC did not adequately plan or document the inventory system as described in NIST guidance and FTC requirements. Our FY 2017 tests of security artifacts produced through CSAM identified numerous instances where data were missing or incorrect and required security controls were labeled as "not applicable." The FTC responded that the CSAM system was implemented using unknown default settings and was not configured to align with FTC security policies. Failure to properly configure the CSAM product results in generation of unreliable security artifacts. We therefore assessed the FTC information security system and its CSAM subsystem as not sufficiently reliable to support decisions to grant (or renew) an ATO or support participation in the FTC Privacy Continuous Monitoring Program. Without the capability to make informed decisions regarding the ability of its systems to protect FTC information assets, the FTC will not be able to grant Approvals to Operate to its networks and information systems.

[15] OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016).

[16] In compliance with FISMA ATO requirements, the FTC implemented the Cyber Security Assessment and Management (CSAM) tool managed by Department of Justice. In its *Fiscal Year 2017 Congressional Budget Justification*, the FTC stated that CSAM would provide FTC with a mechanism for managing FISMA compliance by: 1) providing centralized and up-to-date information, checklists, analysis, and tracking capabilities; 2) ensuring efficient and effective management of vital resources and data; 3) ensuring best practices and that resources are accessible to assess and manage risks and vulnerabilities across the organization; and 4) supporting Certification and Accreditation (C&A) of FTC's network and mission systems. The FTC added that the CSAM tool will allow the FTC to more readily access information about its systems that will in turn allow for better planning and FISMA compliance across the enterprise and afford the FTC better visibility into the status of critical security artifacts and documents.

In our FY 2016 FISMA evaluation, we assessed the FTC Information Systems inventory process as deficient. Based on our FY 2017 analysis, we expanded our FY 2016 recommendation (FY 2016 – 01 - ID.AM) and raised the potential impact from Moderate to High.[17] The deficiencies we identified in the FTC inventory system, while serious, could be mitigated through frequent review of a relatively limited data base (less than 100 information systems). The deficiencies we identified in the CSAM process will continue to have a significant adverse impact on the FTC information security and privacy programs and will disrupt and delay the FTC's ability to maintain its information security environment as it transitions to a cloud environment.

We provide our recommendations to resolve the information systems inventory concerns as two recommendations: FY 2017-01-ID.AM focuses on the functionality typically associated with an information systems inventory; and FY 2017 – 02 - ID.AM which focuses on the CSAM implementation. The FTC may elect to address these two items separately or concurrently.

Implementation of policies and procedures and appropriate configuration of the CSAM product will likely reduce our assessment of potential risk from High to Moderate. Our suggested approach allows the FTC to take short term corrective actions to resolve the systemic issues and a scheduled approach to address quality issues specific to individual artifacts.

[17] FTC information systems are only identified as High impact if –

> The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

The lack of a reliable process for developing and maintaining an information systems inventory and artifacts supporting the FTC Approval to Operate process is a significant deficiency that, if uncorrected, will have a catastrophic impact on the ability of the FTC to protect its information assets and demonstrate the effectiveness of its control environment.

Recommendation: FY 2017 – 01 - ID.AM – Replaces: FY 2016 – 01 - ID.AM

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

The FTC should document its system inventory management system and validate the system, database, and management procedures as a trusted FTC ISCM component under configuration control and that supports continuous monitoring. The FTC should also implement a capability to view its inventory as a single database even though it may be constructed as three separate components.

Potential Impact: High	Reference: OMB Circular A-130 (Jul 2016) section 5. a.1) a) Inventories Related Recommendation: FY 2016 – 01 - ID.AM

Recommendation: FY 2017 – 02 - ID.AM – Replaces: FY 2016 – 02 - ID.AM
FY 2015 – 02: FTC Security Policy and Procedures/System

To ensure the FTC has the artifacts required to support decisions to grant Approvals to Operate, the CSAM implementation should be documented, integrity controls implemented, and all artifacts be subject to 100 percent review until data integrity can be established.

The FTC should institute configuration management of its CSAM process; produce security artifacts that support effective analysis of CSAM security controls and granting of an FTC ATO; and validate the CSAM database.

Potential Impact: High	Reference: NIST SP 800-37 describing the requirements of the NIST Risk Management Framework Related Recommendation: FY 2016 – 02 - ID.AM FY 2015 – 02: FTC Security Policy and Procedures/System

3.1.2 Planning and Governance – Function: Identify Category: Governance

As stated in NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, the purpose of information security governance is to ensure that agencies are proactively implementing appropriate information security controls to support their mission in a cost-effective manner, while managing evolving information security risks. Information security governance can be defined as the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws

and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.

The FTC Information Technology (IT) Governance Program Charter currently in effect was last updated August 20, 2014. This Charter defined an IT governance structure that consisted of three Boards: an IT Governance Board (ITGB), an IT Business Council, (ITBC), and an IT Council (ITC). The Charter described the purpose, role, and responsibilities of the IT governance structure and its three supporting boards. The Charter explicitly stated that:

> 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.

The FTC IT Governance Program, as stated in the Charter, addressed the requirements of IT Governance as defined by NIST in SP 800-100. The Governance Boards were improving oversight of investment development and award as described in the Charter. The Charter required updating to ensure consistency with specific areas of OMB concern, defined in OMB Circular A-130, *Managing Federal Information as a Strategic Resource* (July 28, 2016), such as formalized governance policies and procedures; maximize use of agile development practices, open standards, and replacement of obsolete or unsupported systems equipment or components; and formalized processes for governance, investment analysis, and investment performance.

The OIG requested artifacts that document the current FTC IT governance structure. We assessed the current status of FTC IT Governance as deficient because there are no formalized governance structures with applicable policies and procedures. The FTC created a number of Boards, Councils, and Project Management Authorities in addition to FTC's mission-focused organization. Yet there currently is no artifact that clearly describes the roles and responsibilities of these entities and their interrelationships. For example, the two graphics (see Exhibits 8 and 9) the FTC provided to show the organizational entities with information security responsibilities and their location within the FTC organization are incomplete and inconsistent.

Exhibits 8 and 9 were provided by the FTC to show the FTC entities having specific information security responsibilities. Neither Exhibit 8 nor 9 provides a clear depiction of the current FTC information security or governance structure. For example, Exhibit 8 does not show the Security Operations Center (SOC) or the Boards that are identified in the IT Governance Charter; nor does it identify those entities that have mission or staff responsibilities or are only advisory.

Exhibit 8: FTC Entities with Information Security Responsibilities at November 9, 2017

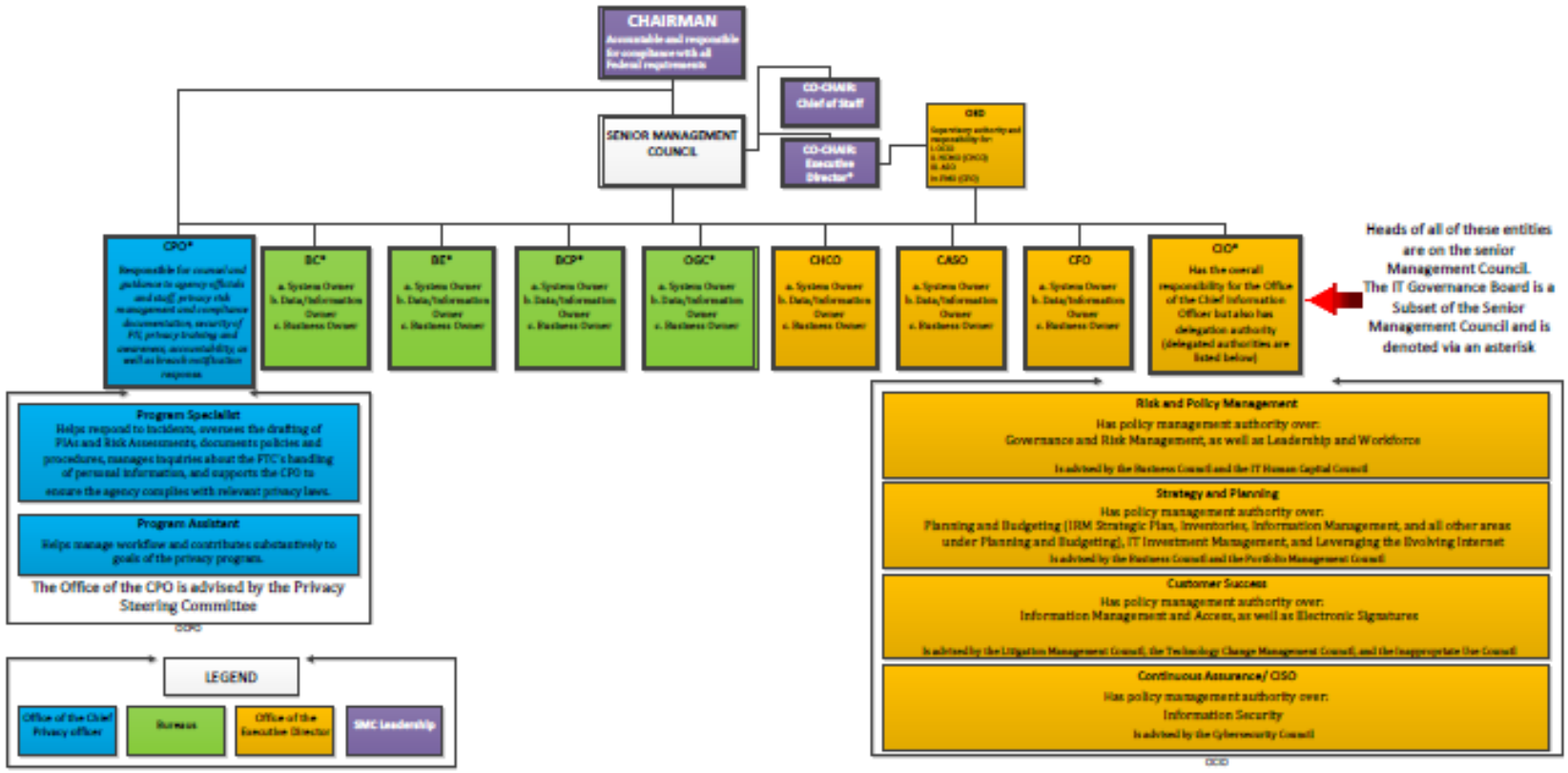
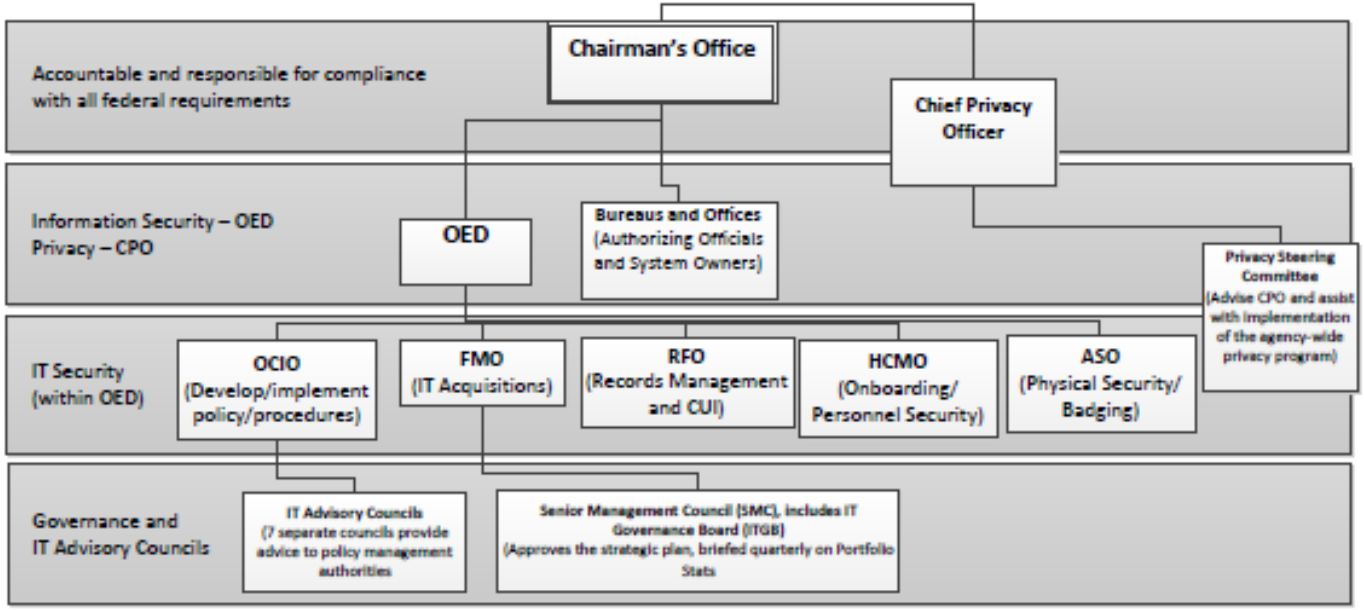


Exhibit 9: FTC Entities with Information Security Responsibilities at October 19, 2017



As of August 30, 2017, the FTC is preparing a new Information Technology Governance Administration Policy. The OIG reviewed this draft document. However, the Policy is early in its development and is not yet sufficient to determine whether it will provide the formal, organization, policies, and procedures FTC needs to support its governance structure.

The OIG previously addressed the FTC's lack of a defined organizational structure that supports governance of IT investments and management and oversight of its information security program in our FY 2015 FISMA evaluation. Our recommendation FY 2015 – 01: *Security Management and Governance Structure*, recommended that the FTC continue to improve its governance practices and associated policies and procedures. FTC management concurred with our recommendations for improvement and scheduled their mitigation for the Second Quarter of FY 2017. Our assessment shows that the deficiencies we identified in our FY 2015 recommendation were not addressed and we cannot determine from the information provided in FY 2017 the status of corrective actions.

During FY 2017, FTC reorganized its OCIO to align with its IT modernization objectives. FTC subsequently created additional organizational entities in response to specific incidents. These added entities detracted from management's progress in establishing an effective, formal governance structure. The FTC completed these actions without the documentation of organizational roles, responsibilities, and authorities that ensures assignment of responsibility and minimizes organizational conflicts. For example, the FTC delegated authorities to individuals, instead of roles, and described typical activities performed instead of clearly defining responsibilities that can be evaluated for conflicts and performance measured and monitored.

Development of clear organizational roles and responsibilities is also critical to ensure that the separation of federal employee and contractor responsibility is maintained. Contractors are not allowed to perform inherently governmental functions. The Federal Activities Inventory Reform (FAIR) Act of 1998, describes the "functions included" within its definition of inherently governmental function as functions that "require either the exercise of discretion in applying Federal Government authority or the making of value judgments in making decisions for the Federal Government, including judgments relating to monetary transactions and entitlements." As FTC continues its IT modernization initiative, it will need to ensure that contracts and contractor-shared responsibilities are properly segregated to ensure inherently governmental functions are identified and assigned.

Recommendation: FY 2017 – 03 - ID.GV– Replaces: FY 2015 – 01: Security Management and Governance Structure

To ensure the FTC has a formal IT governance process in compliance with NIST and OMB requirements, the FTC should revise its IT Governance practices.

FTC governance documentation should include a Charter that describes the scope and purpose of the governance program and the roles and responsibilities of those entities responsible for its execution and a graphic or other documentation that shows FTC entities with information governance responsibilities. The governance documentation should show how risk and information security requirements are identified and resolved. Governance artifacts should be subject to configuration management with change management and a formal process for rescinding and or replacing artifacts that are no longer in effect or are replaced.

Potential Impact: Moderate	Reference: OMB Circular A-130 Section 5.b Governance FAR Part 7 and Part 39 SP 800-53 PM-1 Information Security Program Plan, PM-7 Enterprise Architecture, PL-1 Security Planning Policy and Procedures Related Recommendation: FY 2015 – 01: Security Management and Governance Structure

3.1.3 Risk Assessment – Function: Identify Category: Risk Assessment

NIST information security guidance requires use of risk-based processes to support decision-making processes. NIST SP 800-30 describes risk assessments as follows:

> Risk assessment is one of the fundamental components of an organizational risk management process as described in NIST Special Publication 800-39. Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.
> …
> Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process – providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks.[18]

[18] See NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* (March 2011) for a discussion of the risk management hierarchy and its three tiers.

NIST guidelines allow agencies to use a variety of quantitative or qualitative risk assessment approaches based on their agency's risk management strategy and the maturity of its business processes and the scope, complexity, and criticality of the risk being evaluated. NIST also states that reproducibility and repeatability of results is enhanced by making explicit the risk model, the assessment approach, and the analysis approach employed, and requiring as part of the assessment process, a rationale for the assessed values of risk factors.[19]

In its *Strategy and Transition Plan* for IT modernization, the FTC states that it will "transition to a proactive risk-based, continuous prevention and monitoring posture verse inspecting for compliance." In response to our data calls, the FTC responded that:

> All IT modernization efforts are required to conduct risk assessments at multiple levels. OCIO is developing one overall Business Case Analysis (BCA) for all commodity IT products targeted to move to cloud-based services. Once a solution path is selected risk assessment is incorporated into the requirements for acquisition.
>
> Risks are also being captured in the OCIO FTC Issue and Risk Management (FIRM) site and are escalated by the Program Management Authorities (PMA) based on severity and potential impact.

The OIG evaluated information the FTC provided regarding risk assessments associated with the FTC IT modernization effort and assessed that it is not adequate. Even though the FTC stated that decisions were to be risk based and risk assessments are required at multiple levels, no risk evaluations were provided that are specific to the *Strategy and Transition Plan*.

In response to our request for risk assessments for the modernization effort, the FTC stated that risk assessments will be a requirement for awarded tasks (i.e., FTC stated that -- Once a solution path is selected a risk assessment is incorporated into the requirements for the acquisition). The OIG determined that this statement and BCA templates indicate that a risk assessment may be a requirement of pending acquisitions, but that no risk assessments were performed in the planning phases of the *Strategy and Transition plan*. Further, the FTC uses FIRM as "an agency-wide risk register that is used to document, rank, prioritize and manage IT risks" resulting from other processes (e.g., OIG audits and evaluations). FIRM is <u>not</u> used for risks being managed through REMEDY or CSAM. A FIRM risk may be closed when a risk is mitigated, escalated, or a Corrective Action Plan (CAP) is approved. Thus, its content cannot be treated as a consolidation of all risks or as a tool that memorializes the process the FTC uses for identifying, assessing, and mitigating risk. For example, we reviewed recommendations for corrective actions included in the FTC After-Action Report for the October 2016 data center outage and the email outage from August 2017. The FIRM reports did not allow us to track recommendations from identification,

[19] Reproducibility refers to the ability of different experts to produce the same results from the same data. Repeatability refers to the ability to repeat the assessment in the future in a manner that is consistent with and hence comparable to prior assessments—enabling the organization to identify trends.

through approval, to completion. The capability to track vulnerability mitigation in this manner is a primary function of a POA&M, demonstrating that the FIRM cannot serve as a POA&M replacement.

The FTC IT modernization effort is a complex undertaking with risks that must be known and mitigated if the effort is to be successful. Three key risks that the OIG determined were not adequately addressed are:

- Cloud-shared responsibility model

  The security of an information system is dependent on the identification of responsibility for secure component performance. Component responsibility in the central processing facility model remains with the system owner (e.g., the FTC). The system owner may explicitly shift performance responsibility through contract actions, creating a shared responsibility model.

  The cloud environment starts with a shared responsibility model. The cloud provider is responsible for performance of and activities within the cloud. The boundaries of the cloud are established by a contract between the cloud service provider and the contracting organization (e.g., the General Services Administration). The cloud service provider defines the services it will provide, and those services are memorialized in the services contract. The customer is responsible for providing the services not provided by a cloud provider. For example, a cloud service provider may provide backup for programs and data used in cloud operations, but backup of user programs and data remains the user's responsibility.

  Our assessment of the *IT Strategy and Transition* and associated documents determined that the FTC planning did not identify the risks associated with the cloud environment. The lack of an assessment of the risks associated with the cloud environment resulted in deficient planning for those risks. The *IT Strategy and Transition Plan* did not identify those capabilities that it expects to be inherent in basic cloud service and those capabilities it will retain. This differentiation is important as it is a significant consideration in evaluating overall risk and costs for a cloud-based solution.

- Enterprise Architecture (EA);

  As described in NIST guidance and OMB policies, agencies should adhere to a formal planning process where the in place structure of an IT environment (current state) is transitioned to a future state that is described in an enterprise architecture that includes an embedded security architecture. The OIG evaluated available documentation and determined that the FTC does not have an enterprise architecture nor an embedded security architecture. Instead, the FTC –

developed an inventory of systems and applications that support agency business processes. This inventory serves as the main artifact for the enterprise architecture. Each system/application is defined by its current state, functionality, and alignment to the FTC strategic plan through distinct capabilities based on agency mission and business practices. The agency capabilities are outlines (sic) in a business capability map. The current EA artifacts do not include an enterprise security architecture, although the inventory does track which systems/applications process PII and CUI, and align with the FTC's FISMA inventory.

This statement supports the OIG assessment that the FTC does not have an EA with an embedded security architecture to guide development of the planned architecture. Lack of an EA increases the risk that the total system will not perform as anticipated, especially when that system is being built as independent components. The risk associated with the lack of an EA is increased due to the deficiencies of the information systems inventory and the associated CSAM implementation, discussed in the previous section of this report.

- Acceptance of risks associated with legacy systems.

  In its FY 2017 Risk Management Assessment, the FTC accepted the risk of service disruptions associated with their legacy systems. The OIG reviewed the FTC risk acceptance and determined that, while management can exercise its prerogative to accept a risk, it is also responsible for ensuring that risk acceptance is appropriate and does not unduly compromise the agency's mission or information assets. Risk assessment is a tool that may be used to identify risks and available mitigation approaches and can provide the informed support for a decision to accept a risk and its associated consequences.

Modernizing the FTC's information technology support environment is a complex undertaking. There are a number of risks associated with the modernization initiative that management must identify and address if it is to successfully complete the modernization within planned costs and with minimum adverse mission impact. The FTC has the option to explicitly accept risk -- as it has done with the risks associated with its legacy systems -- or implicitly accept risks as it has done by not evaluating the risks associated with its planned (target) environment and the risks associated with the transition itself. The realization of even a small failure can have significant monetary and mission consequences to the FTC. For example, the FTC estimated that productivity loss for a two-day e-mail outage in August 2017 exceeded $400,000.[20]

Management should conduct risk assessments at multiple levels for its modernization, as stated in its response to our evaluation questions. It should also conduct risk assessments to evaluate the

[20] The FTC initially estimated lost productivity resulting from its e-mail outage at more than $600,000. Subsequently, the FTC revised the estimate to more than $400,000.

risks associated with its legacy systems and transition activities. These assessments will provide the FTC with the information it needs to mitigate or accept risk with an understanding of the potential impacts. At a minimum, the FTC should conduct an evaluation of:

- the target environment for the FTC information technology modernization so that the FTC's implicit acceptance of risk associated with the lack of an Enterprise Architecture is evaluated and risk components mitigated, transferred, or accepted, as supported by the analysis;

- the risks associated with consolidating all IT modernization acquisitions under a single BPA that has a five-year period of performance;

- the risks associated with the transition so that the FTC's implicit acceptance of associated risks can be evaluated and replaced with decisions to mitigate, transfer, or accept specific risks;

- the risks associated with FTC legacy systems may be evaluated to support decisions as to which risks are mitigated and which are accepted to replace the overall acceptance of risk associated with its legacy systems. Implementing targeted risk acceptance is critical for the FTC because its legacy systems contain vital information assets and actively support FTC missions. Thus, a disruption of its legacy systems will have an immediate mission impact as well as the potential for information compromise; and

- the risks associated with individual acquisitions conducted under the BPA.

In our FY 2016 FISMA evaluation, we identified deficiencies in the FTC IT modernization effort. In FY 2016, we stated:

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

Our assessment resulted in recommendation FY 2016 – 04 - ID.RA for the FTC to conduct risk assessments of its IT modernization effort and its components. Our recommendation FY 2016 – 03 - ID.GV, ID.RA, which recommends that the FTC implement a formal procedure for documenting risk-based decisions as part of the FTC risk management program is also related to our recommendation to conduct routine risk assessments. This recommendation, however, is

consolidated with FY 2017 – 05 - ID.RM, where we recommend that the FTC implement an overall risk management strategy as part of its risk management program.

Recommendation: FY 2017 – 04 - ID.RA – Replaces: FY 2016 - 04 – ID.RA

To ensure it has a thorough understanding of the risks associated with its IT modernization initiative, the FTC should evaluate the risks associated with its IT current (legacy) state, future state, and activities needed to transition from the current to future state.

The FTC should conduct risk analyses to identify the risks associated with its modernization initiative. These risk assessments should identify the risks associated with maintaining the legacy system until its retirement, the risks associated with the proposed cloud-based target environment, and the risks associated with the transition to the target environment. The assessments should be sufficiently documented to provide for an FTC decision to mitigate, transfer, or accept risk. Where a risk is accepted, the FTC should include in its documentation a description of the risk accepted and an estimate of the duration and potential impact of an event should the risk be realized.

Potential Impact: Moderate	Reference: NIST 80037; NIST 800-39; NIST 80053: PL-2, RA-1; NIST 800-30; CSF:ID.RA-1 – 6) Related Recommendation: FY 2016 - 04 – ID.RA, FY 2017 – 05 - ID.RM

3.1.4 Risk Management Strategy – Function: Identify Category: Risk Management Strategy

In its Program Management Policy OCIO 12-PM-100, Risk Management Strategy (PM-9) FTC policy requires that the FTC shall:

> Develop a comprehensive strategy to manage risk to operations and assets, individuals, and other organizations associated with the operation and use of information systems, and implement the risk management strategy consistently across the agency.

The OIG reviewed material describing the FTC's risk management practices implemented under OCIO 12-PM-100, PM-9. Based on our review, we determined that the FTC does not have a risk strategy that specifically addresses IT risks as described in NIST SP 800-39, *Managing Information Security Risk, Organization, Mission, and Information System View*, as required under SP 800-53 R4, PM-9.

FTC has an FTC *Enterprise Risk Management Implementation Plan* and an FTC *Enterprise Risk Management Guide* that operate under the authority of the FTC Senior Assessment Team (SAT). These documents describe an Enterprise Risk Management Plan (ERM) that focuses on objectives and requirements contained in Office of Management and Budget Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15,

2016). The risk management guidance contained in SP 800-39 is specific to IT risks and is complementary to and should be used as part of the more comprehensive Enterprise Risk Management (ERM) program described in OMB Circular A-123. For example, SP 800-39 guidance is based on –

- SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*
- SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*
- SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

The risk management guidance contained in SP 800-39 is essential to an appropriate understanding of the complexity and pervasiveness of IT risks and how they should be evaluated. For example, SP 800-39 guidance describes an Enterprise Architecture and how it promotes the concepts of segmentation, redundancy, and elimination of single points of failure—concepts that can help organizations more effectively manage risk; and identifies the three tiers of the information security hierarchy: system (Tier 3), mission/business process (Tier 2); and organizational risk (Tier 1). By contrast, Circular A-123 does not specifically address the concept of an enterprise architecture or the concept of a tiered information security hierarchy.

The guidelines contained in SP 800-39 are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C.§ 3542. The FTC needs to develop policies and procedures that comprise an information security risk management program, as described in SP 800-39. The FTC risk management program should provide guidance describing methodologies for making and supporting risk-based decisions at all three tiers of the information security hierarchy. The information security risk management program should be a complementary of FTC's ERM to facilitate consolidated agency risk management.

In our FY 2016 FISMA evaluation, we recognized that the FTC needs to include guidance in its risk management program for documenting its risk-based decisions as stated in our recommendation FY 2016 – 03 - ID.GV, ID.RA. Our recommendation for a formal documentation process for risk-based decisions should be included in an FTC risk management program.

Recommendation: FY 2017 – 05 - ID.RM – Replaces: FY 2016 - 03 – ID.GV

To ensure it has a comprehensive risk management strategy, the FTC should implement an information security risk management program. The information security risk management program should operate as a component of the FTC ERM.

The FTC should implement an information security risk management strategy that operates as a component of the FTC Enterprise Risk Management program and is applied to all FTC information systems operated by the FTC or under contract to support the FTC.

Potential Impact: Moderate Reference: NIST 800-39, OMB Circular A-130
Related Recommendation: FY 2016 - 03 – ID.GV

3.2 Protect

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

In our FY 2017 evaluation, the OIG determined that the FTC information security program continues to rely on legacy systems and manual controls to protect its information assets. The OIG assessed that the current state, legacy systems, while inefficient and subject to increasing risk as their components become obsolete, remained effective for FY 2017 in providing protection for FTC information assets. The FTC can expect that it will see increased system outages and costs as its legacy systems exceed their projected life span and the time and cost to repair increases. Exhibit 10 shows the tabulation of CyberScope metric responses for the Protect Function.

Exhibit 10: OIG CyberScope Metric Counts for the Protect Function

Maturity Level	Count
Ad-Hoc	0
Defined	5
Consistently Implemented	18
Managed and Measurable	0
Optimized	0
Total	23

The OIG identified three areas for improvement within the Protect Function: Information Protection Processes and Procedures and Configuration Management.

3.2.1 IT Strategy and Transition Plan – Function: Protect Category: Information Protection Processes and Procedures

The FTC recognized that its IT infrastructure needs to be modernized. On September 30, 2016, the FTC issued a *Strategy and Transition Plan* for modernization of the FTC IT environment. The *Strategy and Transition Plan* is the FTC guide for planning, acquiring, implementing, and

operating the IT capabilities that will form the foundation of the FTC IT processing and information security environment. To be successful, the Plan must provide a "roadmap" and structure that ensures FTC assets are adequately protected during the transition to the modernized environment as well as after the modernization is complete.

The OIG reviewed the *Strategy and Transition Plan* as part of our FY 2016 evaluation. We determined that the Plan provides reasonable objectives for the modernization effort. However, the Plan does not provide sufficient definitive information or risk analyses to demonstrate that the modernization can be successfully completed within the planned timeframe or cost. We concluded that the FTC modernization, as described, is a high-risk effort that requires heightened management attention supported by management tools (e.g., an Enterprise Architecture, security baselines, security performance metrics) and performance data to monitor modernization activities and ensure that successful performance is defined and measurable.

The FTC has not updated its *Strategy and Transition Plan* to reflect the status of modernization activities -- as required by the Plan itself. For example, proposed implementation schedules have not been changed to reflect multiple months of acquisition delays or the technical issues that may be encountered because of those delays.

In response to an update to the September 30, 2016 *Strategy and Transition Plan*, the FTC stated that the Plan is being replaced by the Information Resource Management (IRM) Strategic Plan required under OMB Circular A-130 (DRAFT IRM Strategic Plan FY2018-FY2022). The OIG assessed that the DRAFT IRM Strategic Plan is not a substitute for an updated version of the *Strategy and Transition Plan*. The *Strategy and Transition Plan* focused on modernizing the FTC facility-centric IT infrastructure with a modernized cloud architecture with improved reliability, performance, and resilience. OMB defined the IRM Strategic Plan as a component of planning and budgeting that consists of developing and maintaining a strategy for managing and maintaining agency information resources. The IRM Strategic Plan is to describe the agency's technology and information resources goals, including but not limited to processes described in the Circular. This is a substantially different scope and objective than the FTC's *Strategy and Transition Plan* for modernizing its IT infrastructure. An FTC IRM Plan that fully addresses Circular A-130 requirements will not provide the specific guidance and direction necessary for successful completion of the FTC modernization effort. Similarly, if the FTC maintains an IRM Strategic Plan that addresses the management needs of the modernization effort, it will not address the Circular A-130 requirements.

The OIG also assessed the DRAFT IRM Strategic Plan as inadequate to serve as the IRM Strategic Plan OMB intended. The primary OMB requirement is that –

> The IRM Strategic Plan shall demonstrate how the technology and information resources goals map to the agency's mission and organizational priorities. These goals shall be specific, verifiable, and measurable, so that progress against these goals can be tracked.

OIG assessed that the DRAFT FTC IRM Plan provides general goals and approaches as did the *Strategy and Transition Plan*. The DRAFT IRM Plan does not provide the specific goals and metrics OMB sought in Circular A-130. Further, the DRAFT IRM Plan does not address inventories of FTC information systems and information holdings, information management, and risk, which are specific topics that OMB required in the plan.

The FTC should reconsider its decision to use the IRM Strategic Plan to achieve two dissimilar and competing objectives. The FTC should separately address the two requirements: provide a document that supports management and monitoring of its modernization initiative; and develop and maintain a document that describes the FTC strategy for successfully addressing all the Circular A-130 information resources management topics.

The FTC should segment complex efforts like its modernization plan so that it may be effectively planned and monitored. The FTC should monitor the progress of its modernization effort using the September 2016 *Strategy and Transition Plan* as a baseline. This will allow FTC management to monitor and evaluate progress of the modernization effort. A document focused on the modernization effort will allow the FTC to focus on successful project completion and will increase the transparency and improve the quality of FTC budgeting for complex IT projects.

The FTC should develop its IRM Plan so that it aligns with the structure presented in OMB Circular A-130. Incorporating modernization project-related issues detracts from the strategy presentation and does not support development of objectives that are specific and measurable for the IRM Plan. If management does not do so, the FTC will not be in compliance with OMB policy and will have a high risk that its information assets (including its reputation) will not be adequately protected or managed.

Recommendation: FY 2017 – 06 - PR.IP – Replaces: FY 2016 - 05 – PR.IP

To ensure the FTC has the tools it needs to monitor its modernization plan, it should establish a routine process for evaluating cost and schedule performance using the September 2016 version as the baseline.

The FTC should collect metrics describing the status and progress of its modernization effort. These metrics should be used to routinely (at least every 6 months) report project cost, schedule and performance status using the September 2016 version as the baseline.

Potential Impact: Moderate Reference: NIST 800-39, OMB Circular A-130
Related Recommendation: FY 2016 - 05 – PR.IP

Recommendation: FY 2017 – 07 - PR.IP

To ensure that the FTC complies with OMB A-130 planning requirements, the FTC should prepare an IRM Strategy that comports with OMB requirements.

The FTC should develop an IRM Plan that addresses the topics OMB identified for inclusion. The FTC should incorporate metrics into its IRM Plan that allow the performance and cost to be monitored. The FTC should monitor IRM Plan status and costs at least on an annual basis.

Potential Impact: Moderate Reference: NIST 800-39, OMB Circular A-130
Related Recommendation: None

3.2.2 Configuration Management – Function: Protect Category: Configuration Management

Configuration Management is used to describe those processes that ensure that changes to information system components are orderly, tested, and documented.[21] Two key features of an effective configuration management program are the ability to identify the current status of all components of an information system at any point in time, and change management that applies to system documentation and security artifacts.

In prior FISMA evaluations the OIG determined that Configuration Management (CM) practices for individual systems were generally adequate, but there were ongoing issues regarding quality control (e.g., FTC did not have CM quality practices that ensure consistent levels of monitoring and change control across the agency). We also assessed that CM practices were not modified appropriately as systems scaled in complexity and scope (i.e., as systems got larger and more

[21] Configuration Management is a subcategory of the Protect Function identified as subcategories PR.IP-1 and PR.IP-3 in the NIST Cybersecurity Framework. (see https://www.nist.gov/document-3764) The CyberScope reports use term "Configuration Management" and do not provide the subcategory coding. This report uses the Configuration Management (CM) terminology to align with CyberScope reporting.

complex, the quality of and compliance with FTC CM implementations decreased). Further, the quality of CM implementations varied among FTC contractors. For example, some contractors applied CM practices to system documentation while other did not. Without reliable system documentation, information systems become increasingly difficult to maintain and to diagnose errors.

CM is a critical component of an agency's risk management strategy required under control PM-9 in NIST SP 800-53. The basic requirement for CM is contained in CM-1 in SP 800-53 which requires the –

- Development, documentation, and dissemination of a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

- Provides procedures to facilitate the implementation of the configuration management policy and associated configuration management controls across agency information systems.

In FY 2017, the FTC experienced two significant service disruptions: an e-mail system outage and an HVAC outage at the data center. The FTC concluded that lack of effective configuration management was a significant contributing factor to its ability to quickly identify and resolve the e-mail system outage. The OIG reviewed the artifacts for both incidents and determined that deficient configuration management practices was also a contributing factor in the earlier HVAC outage. The FTC estimated a productivity loss of more than $400,000 from the email outage. Combined, these two outages may have cost the FTC more than $600,000 in lost productivity and recovery costs.[22]

The FTC needs to improve its configuration management practices. This is especially important for the FTC modernization effort where the FTC will be replacing or reengineering most of its information systems. The IT infrastructure solutions are expected to be provided by multiple task order teams comprised of multiple companies and service providers. Thus, establishment of an organization-wide CM policy is critical to maintaining consistent CM quality across the agency.

The FTC should develop an agency-wide configuration management policy that establishes the configuration management requirements and processes that must be in place for all FTC information systems, regardless of service model (e.g., cloud, managed hosting, or application as a service). The policy should require that individual information systems have configuration management practices tailored to their specific configurations. FTC policies and procedures should require configuration/document management practices for all system documentation and

[22] The lost productivity estimate was based on an estimate generated by the OCIO for the email outage. The OIG used the FTC estimated downtime productivity loss for its two-day e-mail outage to estimate a productivity loss for the approximately 2.5-day data center outage from its HVAC outage. These combined estimates to result in an estimated productivity loss of more than $600,000 for both service outages.

security artifacts. At a minimum, document configuration management procedures should impose change control and positive identification of effective dates for all system documentation and security artifacts.

The OIG previously recommended that the FTC implement an enterprise-level Configuration Management Plan (Recommendation FY 2014 – 03: Infrastructure Documentation). The FTC provided several draft versions, but all the versions provided were at the individual system level and used the FTC HQ data center as the model system. As we explained to the OCIO, this approach does not address the need for an effective CM policy and practices that may be allied across the agency or for use with different technological solutions. The OIG is therefore reissuing recommendation FY 2014 – 03: Infrastructure Documentation as FY 2017-08-PR.CM to ensure it is addressed as part of FTC modernization and incident resolution activities.

Recommendation: FY 2017 – 08 - PR.CM – Replaces: FY 2014 – 03: Infrastructure Documentation
FY 2015-05: Configuration Management
FY 2016-08-RC.RP

To ensure that the FTC knows the authorized and actual component status of its information systems at any point it time, it should establish a policy that defines agency-wide configuration management requirements. The agency-wide policy should be augmented by system specific practices. FTC configuration practices should also be applied to system documentation and security artifacts.

The FTC should develop an agency-wide configuration management policy that applies to any information systems supporting the FTC. The policy should require development of procedures that are specific to individual systems. The FTC configuration management policy should also require configuration control for all system and information security artifacts.

Potential Impact: Moderate	Reference: OMB Circular A-130, NIST SP 800-53: CM-1 and CM-2 Related Recommendation: FY 2014 – 03: Infrastructure Documentation FY 2015-05: Configuration Management FY 2016-08-RC.RP

3.3 Detect

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

- The FTC developed an ISCM strategy and plan, but did not implement that plan. The FTC acquired tools that can be used to establish an ISCM. The FTC uses the tools in their native state, but did not develop a plan for combining these tools into an integrated system. The FTC also has not identified how continuous monitoring requirements are applied to individual system controls to monitor control effectiveness. [redacted]

- The FTC developed a Privacy Continuous Monitoring Strategy in FY 2017. The OIG assessed this plan as adequate, but dependent on the FTC information security plan. Deficiencies in the information security plan adversely impact the Privacy Continuous Monitoring Plan. The FTC should be able to identify and mitigate adverse impacts from the FTC information security program through Privacy Continuous Monitoring Strategy monitoring and reporting.

- The FTC modified its Plan of Action and Milestones (POA&M) process so that it is not the consolidated listing/tracking tool for vulnerabilities and mitigating actions intended by OMB. The FTC needs to revise its POA&M process so that it includes all the data elements required by OMB and aligns with associated FTC Corrective Action Plans and budgets. Management advised that it plans to have a compliant POA&M by the second quarter of FY 2018.

Based on the results of our FY 2017 evaluation, Exhibit 11 shows the tabulation of CyberScope metrics for the Detect Function:

Exhibit 11: OIG CyberScope Metric Counts for the Detect Function

Maturity Level	Count
Ad-Hoc	0
Defined	5
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Total	5

The OIG has no new recommendations for the Detect Function. The FTC must implement an [redacted] and a POA&M process. [redacted] Without a

POA&M, the FTC will not have the consolidated document needed to record and manage the mitigation and remediation of identified weaknesses and deficiencies.

3.4 Respond

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

The OIG reviewed the FTC incident response procedures such as:

- Computer Incident Response Team (CIRT) Procedure, OCIO 12-IR-001P, effective June 11, 2014
- OCIO-12-IR-100 - Incident Response Policy - 06/13/2016
- OCIO 12-IR-001P - Computer Incident Response Team Procedure - June 11, 2014
- Breach Notification Response Plan (BNRP) – November 2015

Of these procedures, the BNRP is the most focused and was recently tested by the FTC.

The OIG reviewed the OCIO contingency plans and determined that while they provide an incident response structure, testing is inadequate. The OCIO contingency plan was last tested in 2014 (NIST recommends at least annual testing). Thus, the OIG determined that the plan requires updating and, without testing, has a low success potential. Exhibit 12 shows the tabulation of CyberScope metrics for the Respond Function.

Exhibit 12: OIG CyberScope Metric Counts for the Respond Function

Maturity Level	Count
Ad-Hoc	0
Defined	6
Consistently Implemented	1
Managed and Measurable	0
Optimized	0
Total	7

As noted previously, in FT 2017, the FTC experienced two significant outages, one resulting in a multi-day outage of the Headquarters data center and the second resulting in a multiday outage of the FTC e-mail system. These incidents provide fresh illustrations of deficiencies in the FTC's incident response policies and procedure. Critically, the FTC did not execute any contingency plans in responding to either of these outages.[23] Our analysis of After Action Reports, staff communications, and contemporaneous documents showed that –

[23] The OIG issued a Management Advisory, [redacted]

- The FTC never considered executing a contingency plan, the incident response was ad hoc, and recovery was unnecessarily extended;

- The FTC did not notify US-CERT that an incident was in progress as required.[24] The FTC did not know the cause of the disruptions for several hours after FTC technical staff became aware of the service disruption. Thus, there was no viable rationale for a failure to report the events as availability disruptions of unknown cause;

- In both instances, response and recovery efforts were hampered by the absence of effective electronic communications. At the time of the HQ data center outage, all phone and e-mail communications were supported by the HQ data center. Failure of the FTC e-mail service also significantly hampered the FTC's capability to communicate in support of its mission-focused activities as well as efforts to identify and resolve the e-mail outage;

- In both instances the FTC did not maintain activity logs. This made analysis of the incident and FTC response actions difficult and resulted in errors in the activity timeline. For example, the FTC initially pursued an hypothesis that the e-mail outage was caused by an increase in SPAM, and reported the outage as a potential denial of service attack. FTC evaluated this potential and concluded that the outage was not the result of an attack, even though the e-mail system was still out of service and the cause was still unknown;

- In the data center outage, response was delayed because an HVAC problem alarm was sent via e-mail. This approach meant that the notification required an explicit action to retrieve the problem notification. Further, the notification was not repeated or sent to an alternate address even though the problem condition was not resolved;

- In both events, the root cause analysis was deficient. OCIO's root cause analysis identified the external threat source that instigated the disruption *instead of focusing on vulnerabilities that allowed the event to affect the FTC system and could have been*

[24] FISMA defines "incident" as "an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." [1] FISMA requires federal Executive Branch civilian agencies to notify and consult with US-CERT regarding information security incidents involving their information and information systems, whether managed by a federal agency, contractor, or other source. [2] This includes incidents involving control systems, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), programmable logic controllers (PLCs) and other types of industrial measurement and control systems.

The data center outage denied FTC availability of its information assets. The cause of that denial was unknown until several hours. Similarly, until FTC was able to perform an after-action analysis, the potential impact on confidentiality and integrity were also unknown. Thus, under US-CERT requirements, FTC should have initially reported the data center outage as a service disruption with an unknown cause.

avoided or discovered more quickly and mitigated by FTC action. For example, in the data center outage, the monitoring system sent a message to programmed contact points, but was not programmed to continue sending alerts and changing the contact points if no action was taken. Had an individual taken action when the alert was first sent just after midnight, corrective measures could have been taken before the data center overheated; and

- After Action reporting identified a number of actions that should be taken or could be taken, but did not explicitly state what mitigating actions were approved, who was responsible for tracking them, and what policies or procedures would be developed to reduce the likelihood or severity of similar incidents.[25]

Exhibit 13 provides a timeline for the October 7, 2016 HQ data center outage and Exhibit 14 provides a list of FTC recommended improvements. Management determined that the cause of the HQ data center outage was the failure of a pump in a component (chiller) of the data center air conditioning system. Further, the FTC analysis showed that the air conditioning monitoring system detected a problem and sent an alert, but due to the late hour, there was no response to the alert. In addition, the system programing contained an error that prevented automatic switch-over to a backup component. Technicians corrected the technical errors so the air conditioning system will operate backup devices correctly. The FTC assigned its contract guard service a responsibility to monitor a new temperature display at their guard desks and notify staff if they identify a temperature anomaly; and the FTC is reviewing the possibility of assigning the guard service a duty to set-up alternate cooling capabilities in an emergency situation.

The OIG reviewed the available information regarding the data center outage. Our analysis showed that there were three issues that need resolution:

- The FTC has a number of incident response plans. None of these plans was activated during the October 2016 outage. Thus, response to the data center outage was ad hoc, resulting in a failure to timely notify US-CERT of the service disruption event. The FTC is required to notify US-CERT of availability disruptions within one hour of identification of the disruption by a responsible FTC official. Per the outage chronology, the FTC Security Officer was informed of the data center by the Security Command Center at 3:47 am. Thus, the FTC was required to inform US-CERT of the service disruption by 4:47 am. The FTC must have procedures in place to activate its contingency plans to avoid missing mandatory incident reporting requirements;

[25] A vulnerability is a weakness in a system, system security procedure, internal controls, or implementation that could be exploited by a threat source. A threat source can be adversarial or non - adversarial. Adversarial threat sources are individuals, groups, organizations, or entities that seek to exploit an organization's dependence on cyber resources. Non-adversarial threat sources refer to natural disasters or erroneous actions taken by individuals in the course of executing their everyday responsibilities. NIST Special Publication 800-12 Revision 1, *An Introduction to Information Security* (June 2017).

- The data center monitoring system sent a problem alert to the facilities team, but no action was taken. The FTC should establish a policy that automated warnings are repeated, possibly with increasing frequency or alternate recipients, until there is a positive acknowledgement; and

- The FTC should enforce standard federal requirements that Government Furnished Equipment (GFE) is properly inventoried as part of contract turnover activities. These requirements ensure that the government is made aware of the serviceability and end-of-life considerations through independent reviews (GFE reviews are generally performed by both an existing and incoming contractor).

Exhibit 13: FTC HQ Data Center 10/7/2016 Timeline

Exhibit 14: FTC Recommended Corrective Actions for October 2017 Data Center Outage

The FTC Exchange e-Mail outage incident generated recommendations for improvement by both the OIG and the FTC. Our OIG evaluation of the Exchange e-mail outage of August 2, 2017 identified the failure to activate and use its incident response plan as a problem that resulted in failure to appropriately report the service disruption to US-CERT and maintain effective activity logs; and extended the resolution timeframe. For example, Exhibit 15 provides a chronology of the FTC e-Mail outage that we constructed from FTC provided summaries.

While our identified deficiencies focused on mitigation of vulnerabilities relevant to the current outage, the FTC used an expanded analysis that addressed a number of issues affecting data center Operation and Maintenance (O&M) practices. As shown in Exhibit 16, the FTC contractor identified not only the correction of the failed patch as the needed mitigation but also provided recommendations for operational improvements. Management's recommendations included configuration management issues, improved oversight of O&M activities, tailoring server monitoring tools, [redacted] and key staff workload allocations. The FTC proposed changes may be warranted, but including them in a [redacted] will not get the staff or management attention they deserve. The corrective actions would have better receptivity if [redacted] focused on those recommendations that address the immediate incident. Recommended improvements that had no direct impact on the e-Mail outage could then be reviewed, planned, and scheduled as part of normal technical refresh and update activities.

Exhibit 15: OIG Chronology of the FTC e-Mail Outage of August 3rd, 2017

[redacted]

Exhibit 16: Summary of FTC-Suggested Improvement to Address Issues Identified As Part of Exchange Outage Analysis

The lack of contingency planning is a continuing FTC deficiency. In FY 2014 and FY 2016, we recommended that the FTC implement a contingency planning capability. Our recommendation **FY 2014 – 06: Contingency Plans** focused on disaster recovery, and **FY 2016 – 08 – RC.RP** focused on contingency planning for the HQ data center and hosted applications. We are now consolidating FY 2014 – 06 and FY 2016 – 08 – RC.RP under FY 2017-09-RD.RP to facilitate FTC's development of contingency plan strategy and contingency plans that will accommodate the FTC HQ data center and all other IT support solutions. This strategy should include specific processes for ensuring that systems using cloud-support report system disruption within a timeframe that allows the FTC to meet its US-CERT reporting requirements.

Recommendation: FY 2017 – 09 - RS.RP – Replaces: FY 2014 – 06: Contingency Plans FY 2016 – 08 – RC.RP

To ensure that it has effective contingency planning, the FTC should revise its contingency plans. FTC incident response plans and information system contingency plans need to have tested approaches that are focused on incident response and recovery.

FTC should revise its incident response and information system contingency plans to ensure they provide viable procedures for responding to system outages potential sensitive information compromises. The revised plans should include consideration for US-CERT response, maintaining activity logs, communications with stakeholders, and After-Action reporting that includes root cause analyses, and timely reporting. Plans should be tested at least annually.

Potential Impact: Moderate Reference: OMB Circular A-130, NIST SP 800-34
Related Recommendation: FY 2014 – 06: Contingency Plans FY 2016 – 08 – RC.RP

3.5 Recover

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

The FTC uses a mix of contractor owned and operated systems and systems owned, operated, and hosted on its HQ data center. Contractor-hosted systems have in place offsite backup and tested contingency plans. The HQ data center has offsite data backup, but does not have disaster recovery or other contingency plans in place. Exhibit 17 shows the tabulation of the CyberScope metric counts for the Recover Function.

Exhibit 17: OIG CyberScope Metric Counts for Recover Function

Maturity Level	Count
Ad-Hoc	3
Defined	3
Consistently Implemented	1
Managed and Measurable	0
Optimized	0
Total	7

The FTC has not developed a disaster recovery plan and does not have an alternate processing site. The FTC anticipates that its modernization initiative will mitigate its disaster recovery requirements as the FTC shifts its processing to cloud services environments.

The OIG has no new recommendations for the Recover Function.

As stated in our prior recommendations (FY 2014 – 06 and FY 2016 – 08 – RC.RP), the FTC should develop and test contingency plans for the HQ data center and hosted applications. The need for tested contingency plans was highlighted by the data center and e-mail outages in FY 2017. Both of these incidents could have been addressed in a timely manner had the FTC executed tested contingency plans. Contingency planning will become more critical as the FTC transitions to cloud environments. The FTC will need to ensure that its contingency plans are coordinated among all its suppliers to ensure FTC missions are not adversely impacted by system outages.

4. Status of Prior Year Recommendations

The OIG closes and consolidates recommendations based on action plans and related information provided by FTC management. Recommendations are closed when the action plan for mitigating the identified vulnerability is completed as determined through artifacts provided. As is standard practice, recommendations from FISMA reports or other OIG reporting may be consolidated when management's action plan shows a single mitigation addresses multiple recommendations. Exhibit 18 provides a list of open recommendations for FY 2014 – 2015. Exhibits 19 and 20 provide a detailed listing of the status of FY 2016 and FY 2015 recommendations.

The recommendations in Exhibits 18 through 19 show that FTC's information security program is losing effectiveness in its ability to protect FTC information assets. The recommendations, from year to year, show continuing delay in implementing corrective actions we identified and to which FTC management concurred. Moreover, the nature of the recommendations shows a decline in the maintenance and use of the tools necessary to plan, manage, and monitor an effective security environment: specifically, its information inventory system needs improvement so that it is complete and provides an accurate, complete picture of FTC information system assets; it needs to establish an ISCM to improve the capability to monitor the health of its information security environment; and it needs a reliable capability to monitor and manage mitigation of vulnerabilities from identification to completion through a compliant POA&M. The lack of these management tools contributed to extending the IT service outages experienced by FTC in FY 2017, and to difficulty in tracking corrective actions identified in an After Action Reports to resolution. Further, the OIG assessed that the performance risk to FTC IT assets is increasing because its information security program does not demonstrate the resilience required to effectively transition to the complex cloud-based architecture of its planned IT modernization.

Exhibit 18: List of Open Recommendations for FY 2014-FY 2015

Reference	POAM Reference	OCIO Status	OIG Status[26]
FY 2014 - 03	156	Closed	Consolidated with FY 2017-08-PR.CM
FY 2014 - 04	157	Open	Consolidated with FY 2017-02
FY 2014 - 06	159	Open	Consolidated with FY 2017-09
FY 2015 - 01	233	Closed	Consolidated with FY 2017-03-ID.GV
FY 2015 – 02	210	Closed	Consolidated with FY 2017-02-ID.AM
FY 2015 - 03	212	Open	Open – Scheduled Completion – 9/30/2016 – Status In Progress
FY 2015 - 05	235	Closed	Consolidated with FY 2017-08-PR.CM
FY 2015 - 06	236	Closed	Closed
FY 2015 - 07	237	Open	Open – Scheduled Completion – 12/30/2017 – Status In Progress

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

Exhibit 19: FY 2016 OIG FISMA Recommendations

Reference	Recommendation Synopsis	Scheduled Due Date	Status at August 31, 2017
FY 2016 – 01 - ID.AM	The FTC should document its system inventory management system and validate the system, database, and management procedures, at least on an annual basis, as a trusted FTC ISCM component under configuration control.	FY18 Q4	OIG - Closed Consolidated with FY 2017-01-ID.AM
FY 2016 – 02 - ID.AM	The FTC should complete its evaluation of its system boundaries as it completes its CSAM implementation. FTC should eliminate use of the Minor Application designation and document leveraged/common controls in accordance with NIST RMA guidance and ensure that all FTC systems are covered by an FTC ATO.	FY 19 Q2 – Rev 1 FY18 Q4	OIG - Closed Consolidated with FY 2017-02-ID.AM
FY 2016 – 03 - ID.GV, ID.RA	The FTC should implement a formal procedure for documenting risk-based decisions as part of the FTC risk management program.	FY 18 Q1 – Rev 1 FY 18 Q2	OIG - Closed Consolidated with FY 2017-05-ID.RM
FY 2016 – 04 - ID.RA	The FTC should implement a formal risk management program that addresses the requirements of OMB Circulars A-123 and A-130 and the guidance contained in NIST Special Publications 800-30, 800-37, and 800-39. The FTC should conduct risk analyses for its IT Modernization Initiative.	FY 18 Q2	OIG - Closed Consolidated with FY 2017 – 04 - ID.RA
FY 2016 – 05 – PR.IP, PR.MA	The FTC should structure modernization activities for acquiring major IT investments as useful segments that can be independently planned, acquired, and monitored.	FY18 Q2 – Rev 1 FY18 Q1	OIG - Closed Consolidated with FY 2017 – 06 - PR.IP
FY 2016 – 06 – DE.CM	The FTC should implement a fully compliant ISCM as described in its ISCM Plan in FY 2013 and its ISCM Strategy, dated November 2014.	FY18 Q1 FY18 Q4	
FY 2016 – 07 – DE.CM	The FTC should revise its POA&M process and content to ensure it meets OMB information requirements.	FY 18 Q2	

Exhibit 19: FY 2016 OIG FISMA Recommendations

Reference	Recommendation Synopsis	Scheduled Due Date	Status at August 31, 2017
FY 2016 – 08 – RC.RP	The FTC should develop viable contingency plans for the HQ data center and hosted applications. Plans should be tested to ensure viability and ensure staff are trained to execute them.	FY 18 Q4	OIG - Closed Consolidated with FY 2017-08-RC.RP

Exhibit 20: Status of FY 2015 OIG Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[27]	OIG Assessment
FY 2015 – 01: Security Management and Governance Structure	6.1.1	Continue to evolve FTC Continuous Monitoring Management practices through improvements in governance practices and providing improved documentation and estimating guidance. Review governance policies and procedures to resolve potential organizational conflicts of interest and confusion in roles and responsibilities, and ensure that Boards are appropriately established and resourced and its processes sufficiently guided and documented to complete assigned responsibilities. (Also, see recommendation FY 2015-04 to elevate the CPO to voting membership on the ITGB)	Moderate	Management concurs and will continue to improve governance practices and documentation. Planned actions for FY16 include: • Analyze governance practices since the issuance of the August 2014 Governance Charter, conduct lessons learned discussions with IT Governance Board and IT Business Council members, and develop updated Governance Charter to improve governance effectiveness and efficiency. • Review and update IT Business Council and IT Governance Board roles and responsibilities to ensure clearly defined and differentiated governance oversight and operational management responsibilities. • Develop improved Governance Charter documentation, including supporting processes and procedures, and update the FTC Administrative Manual to provide a governance guidance framework for all FTC staff. Expected Completion Date: FY2017 Q2	Closed Consolidated with FY 2017-03.ID.GV Last Milestone is shown as Not Started and included the following comment: "Develop improved Governance Charter documentation, including supporting processes and procedures, and update the FTC Administrative Manual to provide a governance guidance framework for all FTC staff."
FY 2015 – 02: FTC Security Policy and	6.1.2	FTC should continue its review of Accreditation Boundaries for Minor	Moderate	Management concurs and has completed the installation of the Cyber Security Assessment and	Closed

[27] OCIO comments are presented as provided.

Exhibit 20: Status of FY 2015 OIG Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[27]	OIG Assessment
Procedures/System Accreditation Boundaries		Applications, re-designating those systems that are significant resource investments or have special security considerations as Major Applications.		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	Consolidated with FY 2017 – 02 - ID.AM Expected completion date shown as 12/30/2016 with the final task showing as Not Started.
FY 2015 – 03: Certification and Accreditation	6.1.3	To support FTC Approval to Operate/Authorization (ATO) decisions, FTC should provide staff applicable NIST guidance, including risk assessment criteria, for reviewing security artifacts provided by other federal organizations that are using the same software or services.	Moderate	Management concurs. Planned actions for FY16 include: • Develop risk assessment criteria using applicable NIST guidance to assist in review of security artifacts provided by other federal organizations in support of Approval to Operate/Authorization (ATO) decisions. • Review all existing ATOs that leverage security artifacts from other federal agencies using the new criteria. Expected Completion Date: FY2016 Q4	OPEN OIG requested a copy of the *Draft of risk assessment criteria applied to third party audits and ATO from other federal agencies* identified as completed on 6/16/2016 with a final scheduled for completion at 8/31/2016 but still noted as In Progress. The artifact provided in response to the OIG request was a "list of documents that provide NIST guidance for leveraging third party audits and ATO from other federal agencies" reported as completed on 3/28/2016.

Exhibit 20: Status of FY 2015 OIG Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[27]	OIG Assessment
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	Closed Consolidated with FY 2017-08-PR.CM Scheduled completion date shown as 4/21/2017 with last milestone shown as not started. No intermediate artifacts were shown as completed.
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	Completed Scheduled completion shown as 12/30/2017. Four of five milestones shown as Not Started. The OIG categorized FY 2015 – 06: Identity and Access Management / Remote Access Management as Completed based on PIV project status information broadcast through the FTC intranet to the FTC workforce.

Exhibit 20: Status of FY 2015 OIG Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[27]	OIG Assessment
				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 data center and determine whether the monitoring approach or similar approach should be expanded to other FTC systems.	Moderate	Management concurs, and the Infrastructure Performance Report has been updated to focus on user-facing services. Infrastructure components have been separated so that the Contractor can report on infrastructure outages as well as service outages. Infrastructure outages have a calculated effect on services and all outages can be leveled based on specific impact and are weighted based on user populations to provide a consistent evaluation of performance. The new format allows for ongoing adjustment as services and communities change over time. Planned actions for FY16 include: • Update configuration of the Cascade performance management systems in order to investigate poor	OPEN The development of user focused performance metrics is critical for development of an ISCM system. Metrics need to be aligned with the capabilities to monitor that are allowed under the various acquisition approaches. FTC is still seeking to improve its current tool or select an alternate tool or process to develop additional user performance metrics.

Exhibit 20: Status of FY 2015 OIG Recommendations

Reference	Paragraph	Recommendation	Potential Impact	OCIO Action Plan[27]	OIG Assessment
				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	

5. SUMMARY OF FY 2017 RECOMMENDATIONS

Section 5 provides a summary of the FY 2017 recommendations. Our recommendations address specific vulnerabilities or weaknesses we identified in FTC information security or privacy programs. The scope of the FY 2017 recommendations may overlap with prior recommendations. In that event, we anticipate that management may elect to consolidate corrective action for the FY 2017 recommendations and prior recommendations that have not yet been completed.

In consolidating our recommendations, the FTC should place priority attention on FY 2016 – 05 – PR.IP, PR.MA. This recommendation from FY 2016 addresses the complexities that result when acquisitions are so large and complex that the monitoring and management of the solicitation and the resultant contract become extremely difficult and error-prone. The principle of increasing project complexity is accompanied by increasing performance risk also applies to information security. Thus, management should address the recommendations with specific corrective actions instead of large, complex corrective action plans. For example, our FY 016 recommendation FY 2016 – 03 – ID.GV, ID.RA sought a procedure for documenting risk-based decisions that are transparent and can support an audit. The FTC identified the root cause of the documentation deficiency as "The IT governance charter is outdated and does not outline processes for risk management and procedures for conducting risk analysis, tracking risks, issues, and decisions." While the issue the FTC presented may be correct, the root cause for this recommendation is the lack of decision documentation that can show that the decision was risk based and supported by the analysis performed. The difference in root cause analysis resulted in a corrective action plan that required almost a year to complete and included:

- Implementation of a Tiered Governance & Advisory Councils; and
- Implementation of a Tiered Risk Management Framework Status.

The CAP also did not show that its completion would result in decision documents that demonstrate use of a risk-based decision – they very crux of the OIG recommendation.[28]

The OIG updates the status of recommendations as updating information is provided by the FTC. The primary document used to provide the status information is the POA&M, with supporting artifacts as necessary. As previously noted, FIRM reports do not have the information necessary to replace the POA&M as the principal tool for monitoring mitigation of information security vulnerabilities.

[28] The FTC revised the CAP in response to OIG comments and discussions to show an action plan that, properly implemented would provide documented, risk-based decisions. OCIO submitted artifacts for CAP closure that did not address the areas of concern; that decisions made should be documented such that they are transparent, auditable, and provide the risk-based supporting rationale. Instead, the artifacts provide a general discussion of a governance policy.

Exhibit 21: FY 2017 Recommendations

Reference	Recommendation Synopsis	Consolidated Prior Recommendations
FY 2017 – 01 - ID.AM Systems Inventory	*To ensure the FTC has an inventory that contains the information required to describe all its information systems and data holdings, the FTC should document its inventory practices and validate associated databases.* The FTC should document its system inventory management system and validate the system, database, and management procedures as a trusted FTC ISCM component under configuration control and that supports continuous monitoring. The FTC should also implement a capability to view its inventory as a single database even though it may be constructed as three separate components.	FY 2016-01- ID.AM
FY 2017 – 02 - ID.AM ATO Process	*To ensure the FTC has the artifacts required to support decisions to grant Approvals to Operate, the CSAM implementation should be documented, integrity controls implemented, and all artifacts be subject to 100 percent review until data integrity can be established.* The FTC should institute configuration management of its CSAM process; produce security artifacts that support effective analysis of CSAM security controls and granting of an FTC ATO; and validate the CSAM database.	FY 2016-02- ID.AM FY 2015-02: FTC Security Policies and Procedures/Systems FY 2014 – 04 Certification and Accreditation
FY 2017 – 03 - ID.GV IT Governance	*To ensure the FTC has a formal IT governance process in compliance with NIST and OMB requirements, the FTC should revise its IT Governance practices.* The FTC governance documentation should include a Charter that describes the scope and purpose of the governance program and the roles and responsibilities of those entities responsible for its execution and a graphic or other documentation that shows the FTC entities with information governance responsibilities. The governance documentation should show how risk and information security requirements are identified and resolved. Governance artifacts should be subject to configuration management with change management and a formal process for rescinding and or replacing artifacts that are no longer in effect or are replaced.	FY 2015-01: Security Management and Governance Structure

Exhibit 21: FY 2017 Recommendations

Reference	Recommendation Synopsis	Consolidated Prior Recommendations
FY 2017 – 04 - ID.RA Modernization Risk Assessments	*To ensure it has a thorough understanding of the risks associated with its IT modernization initiative, the FTC should evaluate the risks associated with its IT current (legacy) state, future state, and activities needed to transition from the current to future state.* The FTC should conduct risk analyses to identify the risks associated with its modernization initiative. These risk assessments should identify the risks associated with maintaining the legacy system until its retirement, the risks associated with the proposed cloud-based target environment, and the risks associated with the transition to the target environment. The assessments should be sufficiently documented to provide for an FTC decision to mitigate, transfer, or accept risk. Where a risk is accepted, the FTC should include in its documentation a description of the risk accepted and an estimate of the duration and potential impact of an event should the risk be realized.	FY 2016-04-ID.RA
FY 2017 – 05 - ID.RM IT Risk Management Strategy	*To ensure it has a comprehensive risk management strategy, the FTC should implement and follow an information security risk management program. The information security risk management program should operate as a component of the FTC ERM.* The FTC should implement an information security risk management strategy that operates as a component of the FTC Enterprise Risk Management program and is applied to all the FTC information systems operated by the FTC or under contract to support the FTC.	FY 2016-03-ID.GV
FY 2017 – 06 - PR.IP Modernization Performance Metrics	*To ensure FTC has the tools it needs to monitor its IT modernization plan, the FTC should establish and follow a routine process for evaluating cost and schedule performance using the September 2016 version of the Strategy and Transition Plan as the baseline.* FTC should collect metrics describing the status and progress of its modernization effort. These metrics should be used to routinely (at least every 6 months)	FY 2016-05-PR.IP

Exhibit 21: FY 2017 Recommendations

Reference	Recommendation Synopsis	Consolidated Prior Recommendations
	report project cost, schedule and performance status using the September 2016 version as the baseline.	
FY 2017 – 07 - PR.IP IRM Strategy	*To ensure that the FTC complies with OMB A-130 planning requirements, the FTC should prepare an IRM Strategy that comports with OMB requirements.* The FTC should develop an IRM Plan that addresses the topics OMB identified for inclusion. The FTC should incorporate metrics into its IRM Plan that allow the performance and cost to be monitored. The FTC should monitor IRM Plan status and costs at least on an annual basis.	
FY 2017 – 08 - PR.CM Configuration Management	*To ensure that the FTC knows the authorized and actual component status of its information systems at any point it time, it should establish a policy that defines agency-wide configuration management requirements. The agency-wide policy should be augmented by system specific practices. The FTC configuration practices should also be applied to system documentation and security artifacts.* The FTC should develop an agency-wide configuration management policy that applies to any information systems supporting the FTC. The policy should require development of procedures that are specific to individual systems. The FTC configuration management policy should also require configuration control for all system and information security artifacts.	FY 2014-03:Infrastructure Documentation FY 2015-05: Configuration Management FY 2016-08-RC.RP
FY 2017 – 09 - RS.RP Contingency Planning	*To ensure that it has effective contingency planning, the FTC should revise incident response plans and information system contingency plans to ensure that they have tested approaches that are focused on incident response and recovery.* The FTC should revise its incident response and information system contingency plans to ensure they provide viable procedures for responding to system outages and potential sensitive information compromises. The revised plans should include policies and protocols for US-CERT reporting, maintaining activity logs, communications with stakeholders, and	FY 2014-06: Contingency Planning FY 2016-08-RC.RP

Exhibit 21: FY 2017 Recommendations

Reference	Recommendation Synopsis	Consolidated Prior Recommendations
	After-Action reporting that includes root cause analyses, activity log analyses, and timely reporting. Plans should be tested at least annually.	

APPENDIX A - FTC OIG FY 2017 FISMA CYBERSCOPE RESPONSE

APPENDIX A – CONTAINS INFORMATION DESCRIBING FTC INTERNAL OPERATIONS AND IS REDACTED IN ITS ENTIRETY

APPENDIX B - MANAGEMENT'S RESPONSE TO THE OIG'S FY2017 EVALUATION OF THE FTC'S INFORMATION SECURITY PROGRAM AND PRACTICES

FTC Management concurred in the OIG's nine recommendations in our FY 2017 FISMA report and our consolidation of prior recommendations that addressed related vulnerabilities. Management committed to provide action plans to address our recommendations within 60 days of our March 1, 2018 submission of our final report. Management's response to our report is included in its entirety in this Appendix.

UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION

WASHINGTON, D.C. 20580

MEMORANDUM

DATE: February 23, 2018

FROM: David Robbins, Executive Director

TO: Roslyn Mazer, Inspector General

SUBJECT: Management's Response to the OIG's FY2017 Evaluation of the FTC's Information Security Program and Practices ("*Report*")

The Federal Trade Commission (FTC) appreciates the work performed by the Office of the Inspector General (OIG) during the evaluation of the FTC's Information Security Program and Practices as required by the Federal Information Security Management Act (FISMA). The agency takes information security very seriously and will use the OIG recommendations to strengthen its Information Security Program. The *FY2017 FISMA Report* recognizes that the Information Security Program of the Federal Trade Commission is effective, echoing its earlier finding noted by the Office of Management and Budget (OMB) in its 2017 Risk Management Assessment (RMA) for the FTC:

> *The OIG determined that the FTC currently provides effective protection for its information assets and that its information security and privacy programs comply with FISMA and related policies, standards, and guidelines of OMB, DHS, and NIST.*

During FY2017, the agency prioritized efforts to improve its Information Security Program by focusing on maturing those elements of its IT operations and risk management that the agency highlighted in its FY2016 Management Response. As a result of these efforts, the agency has successfully:

1. Closed all seven of OMB's action items, which included requiring use of the PIV card;
2. Enforced Domain-based Message Authentication, Reporting, and Conformance (DMARC) to combat spoofing and phishing threats;
3. Moved litigation review services – a critical mission function at the FTC – to a cloud service provider through GSA's FedRAMP process, thereby greatly reducing risk of loss of critical agency functions during a catastrophic event;
4. Replaced its legacy on-premise security services with MTIPS services for URL filtering, IDS, and email inspection, using GSA's Networx contract; and
5. Upgraded all of its government furnished endpoints to ensure the agency can continue to update endpoint security controls regularly reviewed by OMB.

The agency believes that these efforts have resulted in improvements to information security.

The Report contains nine recommendations to improve the agency's IT security maturity and modernization efforts and Management concurs with these recommendations. A number of

these recommendations reiterate past OIG recommendations that the agency update its processes and procedures. To that end, the agency appreciates the actions of the OIG to consolidate the recommendations in this Report with prior recommendations and previously agreed upon corrective action plans, preserving the work that the agency has taken to address OIG's prior recommendations. The OIG has expressed a commitment to develop recommendations that are specific and actionable, and the agency shares in the commitment to develop specific action plans that will close open recommendations. The FTC looks forward to working with the OIG to fully understand what specific measures the agency must take in addition to the previously agreed-upon corrective action plans to close the recommendations in this Report.

In this regard, the agency hopes the OIG will entertain its suggestion to adopt a more structured approach to the FISMA report that comports with the Council of Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation and clearly identifies the finding, condition, criteria, and facts for each recommendation. The agency is confident that such an approach will enable it to understand the OIG's findings and more quickly address and close the recommendations.

The FTC is committed to continually improving its Information Security and Privacy Program and has added significant resources to aid in that effort. The agency looks forward to working with the OIG on specific and actionable corrective measures that will address the OIG's open recommendations.

OIG Recommendation 1: FY2017 – 01 – ID.AM

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

The FTC should document its system inventory management system and validate the system, database, and management procedures as a trusted FTC ISCM component under configuration control and that supports continuous monitoring. The FTC should also implement a capability to view its inventory as a single database even though it may be constructed as three separate components.

Responsible Official: Raghav Vajjhala

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

Management recognizes that OIG Recommendation 1: FY2017 – 01 – ID.AM consolidates prior recommendation FY2016– 01– ID.AM and looks forward to working with the OIG to understand what in addition to the previously agreed upon actions plans must be done to resolve this recommendation.

OIG Recommendation 2: FY2017 – 02 – ID.AM

To ensure the FTC has the artifacts required to support decisions to grant Approvals to Operate, the CSAM implementation should be documented, integrity controls implemented, and all artifacts be subject to 100 percent review until data integrity can be established.

The FTC should institute configuration management of its CSAM process; produce security artifacts that support effective analysis of CSAM security controls and granting of an FTC ATO; and validate the CSAM database.

Responsible Official: Raghav Vajjhala

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

Management recognizes that OIG Recommendation 2: FY2017 – 02 – ID.AM consolidates prior recommendations FY2016– 02– ID.AM, FY2015– 02: FTC Security Policies and Procedures/Systems, and FY2014– 04: Certification and Accreditation and looks forward to working with the OIG to understand what in addition to the previously agreed upon actions plans must be done to resolve this recommendation.

OIG Recommendation 3: FY2017 – 03 – ID.GV

To ensure the FTC has a formal IT governance process in compliance with NIST and OMB requirements, the FTC should revise its IT Governance practices.

The FTC governance documentation should include a Charter that describes the scope and

purpose of the governance program and the roles and responsibilities of those entities responsible for its execution and a graphic or other documentation that shows the FTC entities with information governance responsibilities. The governance documentation should show how risk and information security requirements are identified and resolved. Governance artifacts should be subject to configuration management with change management and a formal process for rescinding and or replacing artifacts that are no longer in effect or are replaced.

Responsible Official: Raghav Vajjhala

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

Management recognizes that OIG Recommendation 2: FY2017 – 03 – ID.GV consolidates prior recommendation FY2015– 01: Security Management and Governance Structure and looks forward to working with the OIG to understand what in addition to the previously agreed upon actions plans must be done to resolve this recommendation.

OIG Recommendation 4: FY2017 – 04 – ID.RA

To ensure it has a thorough understanding of the risks associated with its IT modernization initiative, the FTC should evaluate the risks associated with its IT current (legacy) state, future state, and activities needed to transition from the current to future state.

The FTC should conduct risk analyses to identify the risks associated with its modernization initiative. These risk assessments should identify the risks associated with maintaining the legacy system until its retirement, the risks associated with the proposed cloud-based target environment, and the risks associated with the transition to the target environment. The assessments should be sufficiently documented to provide for an FTC decision to mitigate, transfer, or accept risk. Where a risk is accepted, the FTC should include in its documentation a description of the risk accepted and an estimate of the duration and potential impact of an event should the risk be realized.

Responsible Officials: Raghav Vajjhala and David Rebich

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

Management recognizes that OIG Recommendation 2: FY2017 – 04 – ID.RA consolidates prior recommendation FY2016– 04– ID.RA and looks forward to working with the OIG to understand what in addition to the previously agreed upon actions plans must be done to resolve this recommendation.

OIG Recommendation 5: FY2017 – 05 – ID.RM

To ensure it has a comprehensive risk management strategy, the FTC should implement and follow an information security risk management program. The information security risk management program should operate as a component of the FTC ERM.

The FTC should implement an information security risk management strategy that operates as a

component of the FTC Enterprise Risk Management program and is applied to all the FTC information systems operated by the FTC or under contract to support the FTC.

Responsible Official: Raghav Vajjhala and David Rebich

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

Management recognizes that OIG Recommendation 2: FY2017 – 05 – ID.RM consolidates prior recommendation FY2016– 03– ID.GV and looks forward to working with the OIG to understand what in addition to the previously agreed upon actions plans must be done to resolve this recommendation.

OIG Recommendation 6: FY2017 – 06 – PR.IP

To ensure the FTC has the tools it needs to monitor its IT modernization plan, the FTC should establish and follow a routine process for evaluating cost and schedule performance using the September 2016 version of the Strategy and Transition Plan as the baseline.

The FTC should collect metrics describing the status and progress of its modernization effort. These metrics should be used to routinely (at least every 6 months) report project cost, schedule, and performance status using the September 2016 version as the baseline.

Responsible Official: Raghav Vajjhala and David Rebich

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

Management recognizes that OIG Recommendation 2: FY2017 – 06 – PR.IP consolidates prior recommendation FY2016– 05– PR.IP and looks forward to working with the OIG to understand what in addition to the previously agreed upon actions plans must be done to resolve this recommendation.

OIG Recommendation 7: FY2017 – 07 – PR.IP

To ensure that the FTC complies with OMB A-130 planning requirements, the FTC should prepare and follow an IRM Strategy that comports with OMB requirements.

The FTC should develop an IRM Plan that addresses the topics OMB identified for inclusion. The FTC should incorporate metrics into its IRM Plan that allow the performance and cost to be monitored. The FTC should monitor IRM Plan status and costs at least on an annual basis.

Responsible Official: Raghav Vajjhala

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

Management recognizes that OIG Recommendation 2: FY2017 – 07 – PR.IP is a new recommendation and looks forward to working with the OIG to understand what must be done to resolve this recommendation.

OIG Recommendation 8: FY2017 – 08 – PR.CM

To ensure that the FTC knows the authorized and actual component status of its information systems at any point it time, it should establish a policy that defines agency- wide configuration management requirements. The agency-wide policy should be augmented by system specific practices. The FTC configuration practices should also be applied to system documentation and security artifacts.

The FTC should develop an agency-wide configuration management policy that applies to any information systems supporting the FTC. The policy should require development of procedures that are specific to individual systems. The FTC configuration management policy should also require configuration control for all system and information security artifacts.

Responsible Official: Raghav Vajjhala

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

Management recognizes that OIG Recommendation 2: FY2017 – 08 – PR.CM consolidates prior recommendations FY2016– 08– RC.RP, FY2015– 05 Configuration Management, and FY2014– 03 Infrastructure Documentation and looks forward to working with the OIG to understand what in addition to the previously agreed upon actions plans must be done to resolve this recommendation.

OIG Recommendation 9: FY2017 – 09 – RS.RP

To ensure that it has effective contingency planning, the FTC should revise its incident response plans and information system contingency plans to ensure that they have tested approaches that are focused on incident response and recovery.

The FTC should revise its incident response and information system contingency plans to ensure they provide viable procedures for responding to system outages and potential sensitive information compromises. The revised plans should include step-by-step protocols and policies for US-CERT reporting, maintaining auditable activity logs, communications with stakeholders, and After-Action reporting that includes root cause analysis, activity log analyses, and timely reporting. Plans should be tested at least annually.

Responsible Official: Raghav Vajjhala

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

Management recognizes that OIG Recommendation 2: FY2017 – 09 – RS.RP consolidates prior recommendations FY2016– 08– RC.RP and FY2014– 06: Contingency Planning and looks forward to working with the OIG to understand what in addition to the previously agreed upon actions plans must be done to resolve this recommendation. Management further notes that this recommendation is a continuation of the conditions cited in Recommendation FY2016– 08 from the FY 2016 FISMA report. Management also will continue to implement the corrective action plan agreed to with the OIG dated 09/29/2017.

Contact the OIG

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

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

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

Complaints may be made anonymously.

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

FINAL REPORT
REDACTED FOR PUBLIC RELEASE