Description of document: Federal Trade Commission (FTC) Information Technology Strategy and Transition Plan, Security and Technology Services FY 2016 - FY 2019, 2016

Requested date: 03-September-2017

Released date: 11-October-2017

Posted date: 28-May-2018

Source of document:
Freedom of Information Act Request
Office of General Counsel
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580
Fax: (202) 326-2477
Email: FOIA@FTC.GOV

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

OCT 11 2017

Re: FOIA-2017-01418
FTC IT Strategy and Transition Plan

This is in response to your request dated September 03, 2017, under the Freedom of Information Act seeking access to [enter request description here]. In accordance with the FOIA and agency policy, we have searched our records as of September 05, 2017, the date we received your request in our FOIA office.

We have located 34 pages of responsive records. I am granting partial access to the accessible records. Portions of these pages fall within one or more of the exemptions to the FOIA's disclosure requirements, as explained below.

Some responsive records contain staff analyses, opinions, and recommendations. Those portions are deliberative and pre-decisional and are an integral part of the agency's decision making process. They are exempt from the FOIA's disclosure requirements by FOIA Exemption 5, 5 U.S.C. § 552(b)(5). *See NLRB v. Sears, Roebuck & Co.,* 421 U.S. 132 (1975).

If you are not satisfied with this response to your request, you may appeal by writing to Freedom of Information Act Appeal, Office of the General Counsel, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580, within 90 days of the date of this letter. Please enclose a copy of your original request and a copy of this response.

You also may seek dispute resolution services from the FTC FOIA Public Liaison Richard Gold via telephone at 202-326-3355 or via e-mail at rgold@ftc.gov; or from the Office of Government Information Services via email at ogis@nara.gov, via fax at 202-741-5769, or via mail at Office of Government Information Services (OGIS), National Archives and Records Administration, 8601 Adelphi Road, College Park, MD 20740.

If you have any questions about the way we handled your request or about the FOIA regulations or procedures, please contact Chip Taylor at 202-326-3258.

Sincerely,

Dione J. Stearns
Assistant General Counsel

FEDERAL TRADE COMMISSION

INFORMATION TECHNOLOGY

Customer success through transparency and teamwork to
inspire trust in IT services across all Bureaus and Offices

Protect Consumers • Maintain Competition • Advance Organizational Performance

Strategy and Transition Plan

Security and Technology Services FY 2016 – FY 2019

September 30, 2016

Message from the Chief Information Officer

It is with pleasure that I present the Federal Trade Commission's Information Technology (IT) Strategy and Transition Plan – a roadmap that will guide significant changes for core operations that will lead to revitalized support for objectives, strategies, and goals identified in the FTC's Strategic Plan. This document represents the Federal Trade Commission's IT Strategy and Transition Plan for its IT Services. To achieve the long-term vision for FTC IT Services – customer success through transparency and teamwork to inspire trust in IT services across all Bureaus and Offices – the plan identifies a transition plan to target several key areas for improvement as follows:

- Section 1: Highlights the alignment of IT strategic initiatives to FTC's mission. Establishes priorities to refocus workforce efforts from maintenance of legacy services to continuous improvement and business aligned change. Establishes performance metrics in the areas of Customer Satisfaction, Stable and Secure Operating Environment, and Effective IT Resources.
- Section 2: Baselines current IT performance and practices
- Section 3: Discusses industry best practices and relevant federal guidance
- Section 4: Establishes IT performance guidance and practices to include focusing on the customer, increasing mobility, effective cybersecurity, highly available architecture, data driven decision culture, and realigns IT resources to better support the FTC mission.
- Section 5: Provides a high-level schedule and budget for key IT strategic initiatives that will transform FTC's IT environment from on premise custom hosting to secure leased services.

This document was written to be as actionable as possible, focusing on the next two years by fulfilling the immediate needs of an agency updating current infrastructure operation capabilities.

To ensure that the FTC properly assessed the future IT landscape to take advantage of emerging IT services, the plan reflects feedback and information from industry, other federal agencies and the entire FTC. Successful completion of the initiatives outlined in this plan will enable future updates to focus on innovation built with emerging capabilities – including those from secure cloud service providers. At the conclusion of efforts outlined in this plan, the FTC should experience significant improvement in:

- The ability to conduct its mission anywhere and anytime on any device with the same high quality experience
- Applying information resources beyond current roles focusing on system uptime to roles that focusing on measurable mission impact
- Measuring the impact of decisions against baselines for mission outcomes, security controls, and data protection.

We appreciate the support of all FTC stakeholders whose insight greatly contributed to this plan:

- IT Governance Board: Katherine Race Brin (Office of the Chairwoman), Marian Bruno (Bureau of Competition (BC)),Daniel Kaufman (Bureau of Consumer Protection (BCP)), David Rebich (Office of the Executive Director (OED)), David Robbins (OED), David C. Shonka (Office of the General Counsel (OGC)), and Michael G. Vita (Bureau of Economics (BE))
- IT Business Council: Katherine Race Brin (Office of the Chairwoman), Donald S. Clark (Office of the Secretary), Richard Custer (Office of Public Affairs), Laura DeMartino (BCP), Nathan Hawthorne (BC), Daniel S. Hosken (BE), Sarah D. Mackey (OGC), David Rebich (OED), David Robbins (OED), Jon M. Steiger (East Central Regional Office), and Fenice Wade (OED)

- IT Council: Binoy Agarwal (OED), Megan Baburek (OED), Janice Brown-Taylor (OED), Chloe Collins (OED), Jack F. Gabriel Jr. (OED), Meenu Gupta (OED), Bruce Jennings (OED), Jacalyn Johnson (OED), William Merkle (OED), Jeffrey M. Smith (OED), and Juanhui Xie (OED).

On behalf of the IT Governance Board, IT Business Council, and IT Council, we are pleased for this opportunity to lead the FTC through this modernization of its information technology work so we can continue to meet the expectations of Congress, consumers, businesses, law enforcement, and other stakeholders as we strive for excellence.

FTC Chief Information Officer

Raghav Vajjhala

Contents

Tables and Figures

1 Strategic Goals and Desired IT Performance

The Federal Trade Commission (FTC) is an independent federal agency with a unique mission to protect consumers by preventing anticompetitive, deceptive, and unfair business practices, enhancing informed consumer choice and public understanding of the competitive process, and accomplishing this without unduly burdening legitimate business activity. The FTC vision is a vibrant economy characterized by vigorous competition and consumer access to accurate information. These overarching principles will be the basis for the ongoing development and maintenance of an IT Strategic Plan that aligns IT services with FTC priorities.

FTC Strategic Goals

Strategic Goals	Objectives
Goal 1: Protect Consumers	• Identify and take actions to address deceptive or unfair practices that harm consumers • Provide the public with knowledge and tools to prevent harm to consumers • Collaborate with domestic and international partners to enhance consumer protection
Goal 2: Maintain Competition	• Identify and take actions to address anticompetitive mergers and practices that harm consumers • Engage in effective research and stakeholder outreach to promote competition, advance its understanding, and create awareness of its benefits to consumers
Goal 3: Advance Organizational Performance	• Optimize resource management and infrastructure • Cultivate a high-performing, diverse, and engaged workforce

The FTC's mission, vision, and strategic goals drive expectations of IT services that reflect the needs of its key employees, attorneys and economists. Per the *FY2017 Congressional Budget Justification*, the FTC requires highly available IT services to support an organization that operates as both a large law firm and a think tank specializing in financial analysis.

Strategic Performance Goal Objective 3.1.2

Measure	Description
Availability of information technology systems: 99.5%	This goal addresses the availability of 10 mission-critical IT systems, such as email, telecommunications, Internet access, and mobile devices. Network availability addresses the reliability of the FTC computer and communications systems.

Strategic Initiative Alignment

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

1.1 Ongoing Customer Success Priorities

The FTC has established enterprise-wide infrastructure priorities to promote consistent communication, analysis and decision-making.

- Document issues, risks, milestones, and analysis
- Stabilize network and security operations
- Reduce occurrence of critical or non-standard events across all logs
- Change business process and policies to reduce duplicative or minimally used services, eliminate customizations that prevent manufacturer upgrades, and increase business use of IT services
- Resolve remaining customer tickets of current services through immediate action or deferment to future Development, Modernization, and Enhancement (DME), and confirm customer communication on status
- Conduct only authorized DME activities
    - Prepare documentation beginning with business case analysis, TechStat research, business requirements gathering, and task order preparation that targets successful adoption of IT services, not merely product deployment
    - Measure success of deployments through Key Performance Indicators (KPIs) sufficient to inform evaluation of contractor, technology, and employee performance

1.2 IT Performance Measures

As the FTC works to stabilize and improve the IT operating environment, we will be developing KPIs to monitor our progress. The FTC is looking to establish metrics for both the regional offices and headquarters around the areas of user satisfaction, security, and effective use of IT resources. We will evaluate performance indicators, establish a baseline and create annual performance targets. Below are several KPIs under evaluation to measure performance during and after the transition:

- User satisfaction
    - % of users satisfied with IT support
    - Availability greater than 99.5% (24x7 less maintenance windows)
    - Time to first byte
    - Time to load
    - Mean time to repair
    - IT support performance
- Stable and Secure Operating Environment
    - % of IT systems under continuous authorization
    - % of IT systems patched within 30 days
    - % of IT systems with documented configurations
    - % of users using 2 Factor Authentication
    - Mean time between failures
- Effective IT Resources
    - % of IT Services hosted in the cloud versus internally
    - % of systems with SLAs
    - % OCIO FTEs trained in Clinger-Cohen competencies
    - IT governance boards review 100% of the annual IT budget

- % of current IT spend reinvested in business support
- % IT service utilization
- % IT budget/overall agency budget

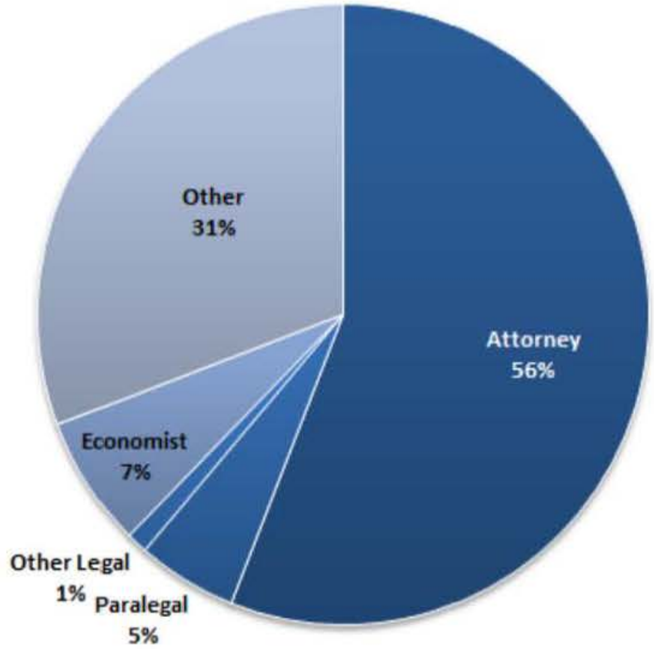
We acknowledge the lack of metrics that directly relate technology to the support of FTC's mission, and will work to develop metrics once transition plans are established. The appendix shows the list of service portfolios and categories, as well as proposed SLAs for each service portfolio.

2 Current IT Performance and Practices

2.1 Customer Base

The FTC user base is approximately 1,700 federal employees and contractors, with an estimated 100 additional temporary staff between May and September. Washington, DC based staff are located in the Headquarters building at 600 Pennsylvania Avenue NW and a satellite facility at 400 7th Street SW. FTC staff is also located throughout the country in eight regional offices: New York, New York; Atlanta, Georgia; Cleveland, Ohio; Chicago, Illinois; Dallas, Texas; Seattle, Washington; Los Angeles, California; and San Francisco, California.

Federal Workforce Distribution



Data from OPM Fedscope, March 2016 (http://www.fedscope.opm.gov/employment.asp)

2.2 Customer Experience

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 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. As noted in the *OIG FY 2015 Independent Evaluation of the Federal Trade Commission's Information Security Program and Practices*:

- The deployment of "smart phones" was undertaken in FY 2014 without the planning, user-based requirements, testing, and documentation required for an information system under FTC (e.g., OCIO Acquisition Strategy for Information Technology) and NIST requirements. Instead, FTC relied on lessons learned from other GSA smart phone implementations. This resulted in phones that did not operate within FTC facilities; phones that did not provide anticipated functionality, and phones deployed with known deficiencies.
- The e-Discovery Support System (eDSS), BCA approved November 2011, was acquired without the functional or performance baselines and tools necessary to quickly identify, resolve, and test

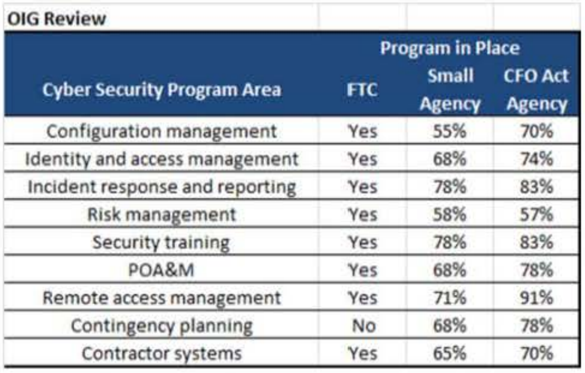
errors. FTC did conduct market research to identify suitable commercial software products. This effort, however, focused on functionality and did not collect the information to construct performance metrics or pricing practices to support an acquisition. This resulted in poor product performance (e.g., extended search times and inability to accommodate FTC workloads), the need to devote FTC resources to resolve product deficiencies, and a higher risk of unidentified errors than reasonable for a Commercial, Off-The-Shelf product. Poor product performance also delayed replacement of the legacy system, further increasing operations and maintenance costs.

2.3 Cybersecurity

In OMB's 2015 *Report to Congress on the Federal Information Security Modernization Act (FISMA)*, OMB published comparative data for all federal government agencies on their Cybersecurity practices. In addition, OIG made public its annual review of FTC cybersecurity practices in its *Independent Evaluation of the Federal Trade Commission's Information Security Program and Practices*.

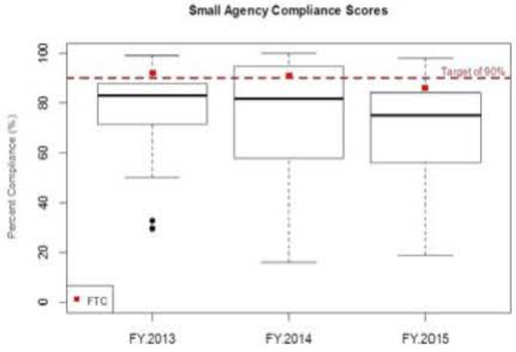
While the FTC scored above most small agencies, it fell short in several measures for Cross Agency Priority (CAP) goals, and the FTC fell short of an overall "Green" rating for its practices. Most significantly, the OIG rated the FTC's contingency planning in most need of improvement.

Comparison of FTC Security Compliance Scores

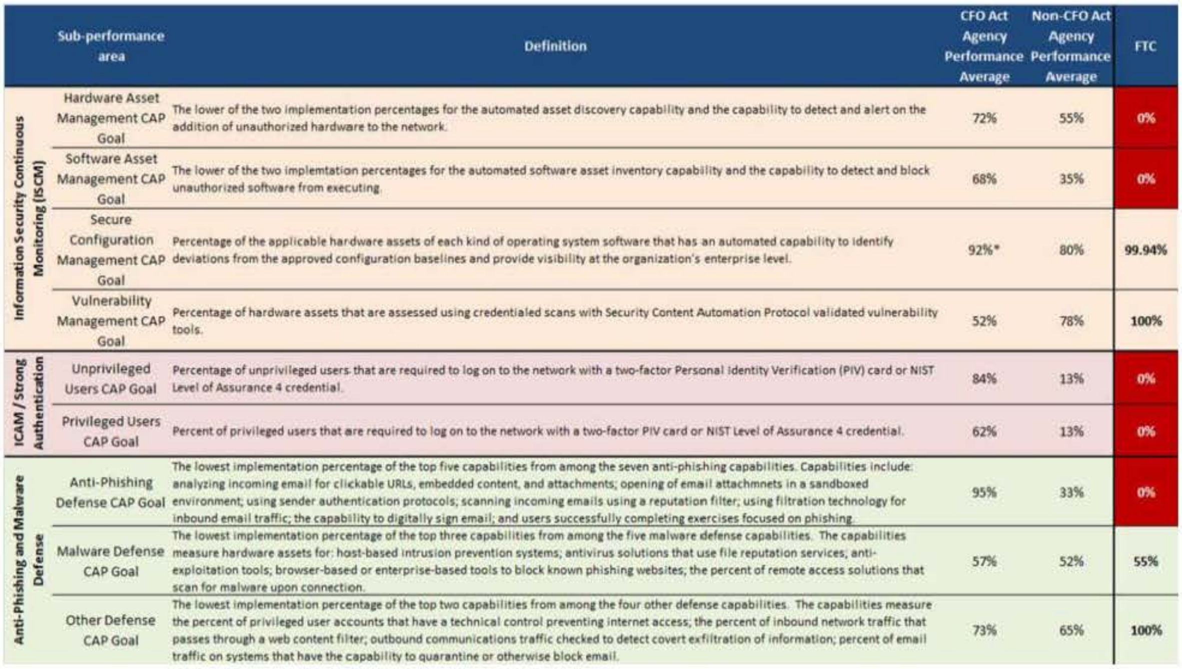


OIG Review

Cyber Security Program Area	Program in Place		
	FTC	Small Agency	CFO Act Agency
Configuration management	Yes	55%	70%
Identity and access management	Yes	68%	74%
Incident response and reporting	Yes	78%	83%
Risk management	Yes	58%	57%
Security training	Yes	78%	83%
POA&M	Yes	68%	78%
Remote access management	Yes	71%	91%
Contingency planning	No	68%	78%
Contractor systems	Yes	65%	70%



Comparison of FTC Responses on CAP Security Goals

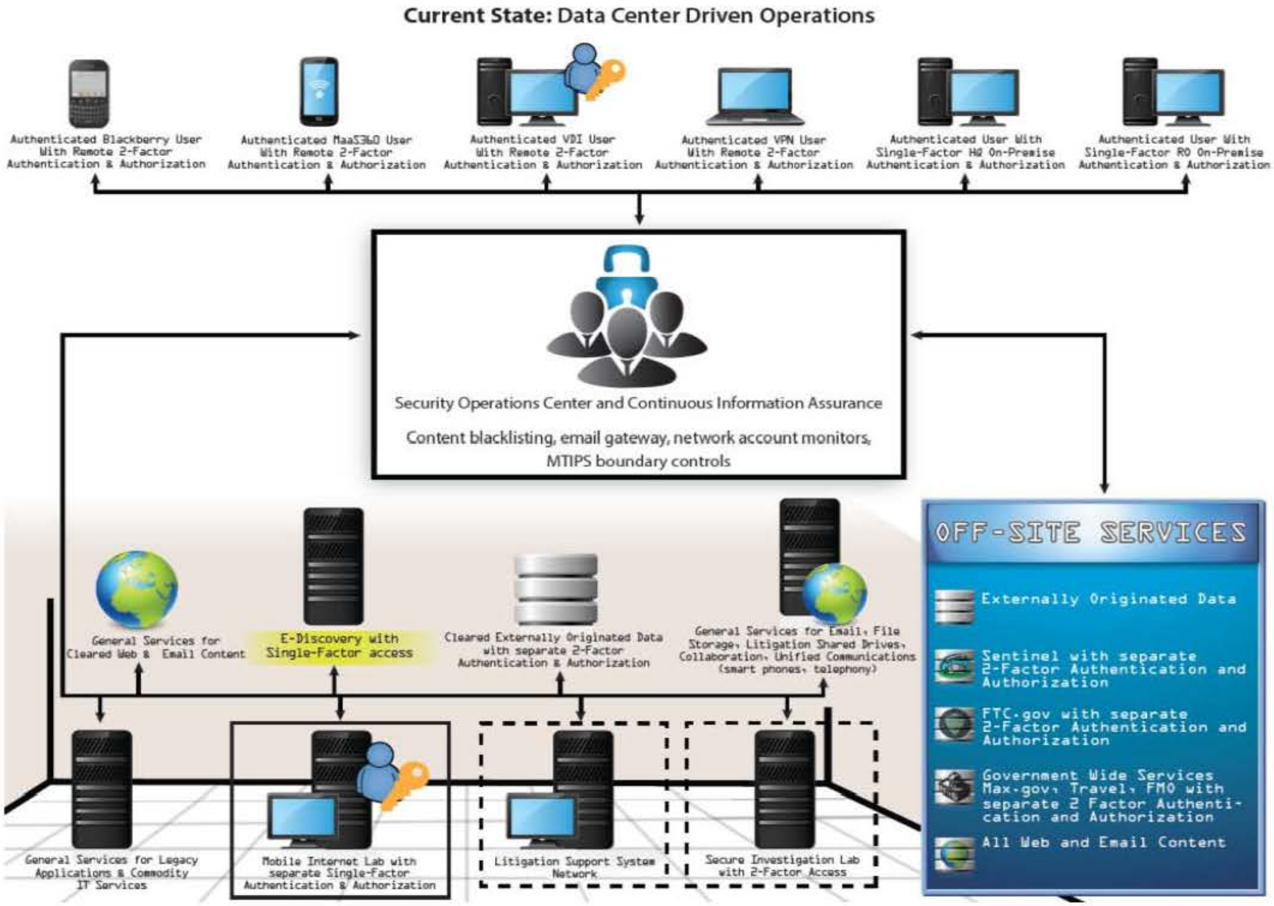


	Sub-performance area	Definition	CFO Act Agency Performance Average	Non-CFO Act Agency Performance Average	FTC
Information Security Continuous Monitoring (ISCM)	Hardware Asset Management CAP Goal	The lower of the two implementation percentages for the automated asset discovery capability and the capability to detect and alert on the addition of unauthorized hardware to the network.	72%	55%	0%
	Software Asset Management CAP Goal	The lower of the two implemtation percentages for the automated software asset inventory capability and the capability to detect and block unauthorized software from executing.	68%	35%	0%
	Secure Configuration Management CAP Goal	Percentage of the applicable hardware assets of each kind of operating system software that has an automated capability to identify deviations from the approved configuration baselines and provide visibility at the organization's enterprise level.	92%*	80%	99.94%
	Vulnerability Management CAP Goal	Percentage of hardware assets that are assessed using credentialed scans with Security Content Automation Protocol validated vulnerability tools.	52%	78%	100%
ICAM / Strong Authentication	Unprivileged Users CAP Goal	Percentage of unprivileged users that are required to log on to the network with a two-factor Personal Identity Verification (PIV) card or NIST Level of Assurance 4 credential.	84%	13%	0%
	Privileged Users CAP Goal	Percent of privileged users that are required to log on to the network with a two-factor PIV card or NIST Level of Assurance 4 credential.	62%	13%	0%
Anti-Phishing and Malware Defense	Anti-Phishing Defense CAP Goal	The lowest implementation percentage of the top five capabilities from among the seven anti-phishing capabilities. Capabilities include: analyzing incoming email for clickable URLs, embedded content, and attachments; opening of email attachmnets in a sandboxed environment; using sender authentication protocols; scanning incoming emails using a reputation filter; using filtration technology for inbound email traffic; the capability to digitally sign email; and users successfully completing exercises focused on phishing.	95%	33%	0%
	Malware Defense CAP Goal	The lowest implementation percentage of the top three capabilities from among the five malware defense capabilities. The capabilities measure hardware assets for: host-based intrusion prevention systems; antivirus solutions that use file reputation services; anti-exploitation tools; browser-based or enterprise-based tools to block known phishing websites; the percent of remote access solutions that scan for malware upon connection.	57%	52%	55%
	Other Defense CAP Goal	The lowest implementation percentage of the top two capabilities from among the four other defense capabilities. The capabilities measure the percent of privileged user accounts that have a technical control preventing internet access; the percent of inbound network traffic that passes through a web content filter; outbound communications traffic checked to detect covert exfiltration of information; percent of email traffic on systems that have the capability to quarantine or otherwise block email.	73%	65%	100%

2.4 Current State Architecture

The Headquarters data center has space for 39 racks, with current network equipment and security devices occupying 12 racks. The Constitution Center data center has 24 racks, with current network equipment and security devices occupying five racks. Storage devices and servers are limited to the remaining rack space, constricting our current environment.

Current State: Data Center Driven Operations


Current State: Data Center Driven Operations
Authenticated Blackberry User With Remote 2-Factor Authentication & Authorization
Authenticated MaaS360 User With Remote 2-Factor Authentication & Authorization
Authenticated VDI User With Remote 2-Factor Authentication & Authorization
Authenticated VPN User With Remote 2-Factor Authentication & Authorization
Authenticated User With Single-Factor HQ On-Premise Authentication & Authorization
Authenticated User With Single-Factor RO On-Premise Authentication & Authorization
Security Operations Center and Continuous Information Assurance
Content blacklisting, email gateway, network account monitors, MTIPS boundary controls
General Services for Cleared Web & Email Content
E-Discovery with Single-Factor access
Cleared Externally Originated Data with separate 2-Factor Authentication & Authorization
General Services for Email, File Storage, Litigation Shared Drives, Collaboration, Unified Communications (smart phones, telephony)
General Services for Legacy Applications & Commodity IT Services
Mobile Internet Lab with separate Single-Factor Authentication & Authorization
Litigation Support System Network
Secure Investigation Lab with 2-Factor Access
OFF-SITE SERVICES
Externally Originated Data
Sentinel with separate 2-Factor Authentication and Authorization
FTC.gov with separate 2-Factor Authentication and Authorization
Government Wide Services Max.gov, Travel, FMO with separate 2 Factor Authentication and Authorization
All Web and Email Content

The current state reflects numerous add-ons to legacy services established in the FTC data center. Add-ons include mobile services, telework access, and secure labs for mission support.

Pros

By retaining services in its data center, the FTC can exercise direct control over access to its services from RO, HQ, and mobile users.

Cons

Monitoring of internal services relies on numerous technologies across various network access paths. RO traffic must connect through HQ. Additionally, fail-over ready disaster recovery requires high-cost, fully redundant services at an alternate data center.

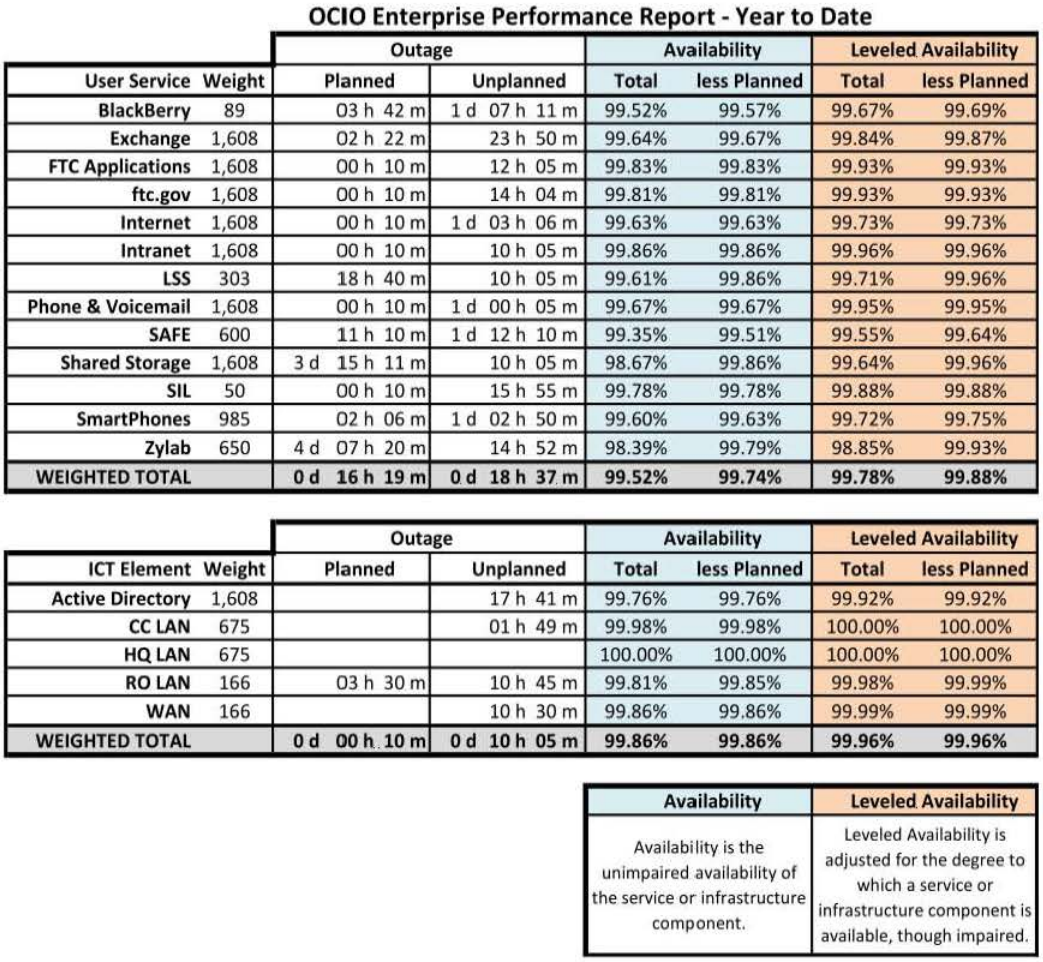
2.5 Service Availability

When compared to cloud vendor targets listed in their respective service level agreements, the FTC target of 99.5% falls short of industry targets.

Cloud Services Targets for Availability

Company	Cloud Services	Availability Target
Microsoft	Microsoft 365 Services including email, Skype, OneDrive, SharePoint, and Office	99.9%
Google	Google Apps including Gmail, Calendar, Talk, Docs and Drive, Groups, Sites and Apps Vault	99.9%
Amazon	Amazon Web Services for Storage (S3)	99.9%

Service Availability from Week of August 1, 2016



OCIO Enterprise Performance Report - Year to Date

		Outage		Availability		Leveled Availability	
User Service	**Weight**	**Planned**	**Unplanned**	**Total**	**less Planned**	**Total**	**less Planned**
BlackBerry	89	03 h 42 m	1 d 07 h 11 m	99.52%	99.57%	99.67%	99.69%
Exchange	1,608	02 h 22 m	23 h 50 m	99.64%	99.67%	99.84%	99.87%
FTC Applications	1,608	00 h 10 m	12 h 05 m	99.83%	99.83%	99.93%	99.93%
ftc.gov	1,608	00 h 10 m	14 h 04 m	99.81%	99.81%	99.93%	99.93%
Internet	1,608	00 h 10 m	1 d 03 h 06 m	99.63%	99.63%	99.73%	99.73%
Intranet	1,608	00 h 10 m	10 h 05 m	99.86%	99.86%	99.96%	99.96%
LSS	303	18 h 40 m	10 h 05 m	99.61%	99.86%	99.71%	99.96%
Phone & Voicemail	1,608	00 h 10 m	1 d 00 h 05 m	99.67%	99.67%	99.95%	99.95%
SAFE	600	11 h 10 m	1 d 12 h 10 m	99.35%	99.51%	99.55%	99.64%
Shared Storage	1,608	3 d 15 h 11 m	10 h 05 m	98.67%	99.86%	99.64%	99.96%
SIL	50	00 h 10 m	15 h 55 m	99.78%	99.78%	99.88%	99.88%
SmartPhones	985	02 h 06 m	1 d 02 h 50 m	99.60%	99.63%	99.72%	99.75%
Zylab	650	4 d 07 h 20 m	14 h 52 m	98.39%	99.79%	98.85%	99.93%
WEIGHTED TOTAL		**0 d 16 h 19 m**	**0 d 18 h 37 m**	**99.52%**	**99.74%**	**99.78%**	**99.88%**

		Outage		Availability		Leveled Availability	
ICT Element	**Weight**	**Planned**	**Unplanned**	**Total**	**less Planned**	**Total**	**less Planned**
Active Directory	1,608		17 h 41 m	99.76%	99.76%	99.92%	99.92%
CC LAN	675		01 h 49 m	99.98%	99.98%	100.00%	100.00%
HQ LAN	675			100.00%	100.00%	100.00%	100.00%
RO LAN	166	03 h 30 m	10 h 45 m	99.81%	99.85%	99.98%	99.99%
WAN	166		10 h 30 m	99.86%	99.86%	99.99%	99.99%
WEIGHTED TOTAL		**0 d 00 h 10 m**	**0 d 10 h 05 m**	**99.86%**	**99.86%**	**99.96%**	**99.96%**

Availability	Leveled Availability
Availability is the unimpaired availability of the service or infrastructure component.	Leveled Availability is adjusted for the degree to which a service or infrastructure component is available, though impaired.

Current help desk service hours are lower than 24x7 cloud environments, with more limited hours on holidays and weekends.

(b)(5)

(b)(5)

3 Guidance for Target IT Performance and Practices

3.1 Research and Directives

In order to improve the quality of IT services and meet the demands of the agency's strategic goals, the FTC must stay abreast of emerging practices across government and industry.. These include but are not limited to:

- OIG Recommendations: OCIO must improve its management and security practices, especially those most recently identified and agreed to with the OIG in 2016
    - OIG FY 2015 Independent Evaluation of the Federal Trade Commission's Information Security Program and Practices
    - Evaluation of the FTC Office of the Chief Information Officer
- Strong Authentication: The Office of Management and Budget (OMB) directed federal agencies to use strong authentication since 2005 with the issuance of OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive-12*. In light of recent breaches, in June 2015, OMB launched a 30-day cybersecurity sprint to assess and improve the health of all Federal IT assets and networks. As part of the sprint, OMB directed agencies to accelerate the use of Personal Identity Verification (PIV) cards or an alternative form of strong authentication for accessing networks and systems.
- Elimination of Expiring Passwords: Research documented by Zhang, Monrose, and Reiter (2010) in *The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis* and by Chiasson and van Oorschot (2015) in *Quantifying the Security Advantage of Password Expiration Policies* details the limited value of strong authentication practices based on expiring passwords and PINs.
- Cloud First: In 2011 OMB released the *Federal Cloud Computing Strategy* requiring CFO Act agencies to evaluate safe, secure cloud computing options before making any new investments. OMB followed with the 2011 Memorandum for CIOs *Security Authorization of Information Systems in Cloud Computing* announcing the Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
- Government-Wide Acquisition Contracts (GWAC): In 2014, the Office of Federal Procurement Policy released a Memorandum, *Transforming the Marketplace: Simplifying Federal Procurement to Improve Performance, Drive Innovation, and Increase Savings*, implementing the use of category management for federal procurements. In 2015 OMB Memorandum M-16-02, *Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops* was issued, the first in a series of policies directing agencies to take new steps to improve the acquisition and management of common IT goods and services.
- Federal Strategic Sourcing Initiative (FSSI): In May 2005, OMB and the Office of Federal Procurement Policy issued a Memorandum, *Implementing Strategic Sourcing*, requiring federal agencies to identify commodities that the government could efficiently purchase through strategic sourcing. In November 2005, FSSI was launched as a partnership between GSA and the Department of the Treasury. In 2012 OMB Memorandum M-13-02, *Improving Acquisition through Strategic Sourcing* was issued, building on past efforts and established a broad strategic sourcing initiative; putting additional responsibilities for designing and implementing government-wide strategic sourcing solutions on large agencies.

- Electronic Records: In accordance with the President's November 2011 Memorandum, *Managing Government Records*, OMB and the National Archives and Records Administration (NARA) issued a joint *Managing Government Records Directive* in 2012, which mandated that agencies eliminate paper and use electronic record keeping. The directive requires that federal agencies manage both permanent and temporary email records in an electronically accessible format by December 31, 2016; and requires that federal agencies manage all permanent records in an electronic format by December 31, 2019. In September 2014, OMB and NARA released M-14-16, *Guidance on Managing Email*, to assist agencies in meeting these goals and the Federal records management requirements. In September 2015, NARA Bulletin 2015-04 released guidance on the transfer of permanent electronic records.

3.2 Reliability Measures

To ensure that efforts are undertaken in support of the above, the FTC must ensure the completeness of methods used to measure the quality of IT services in support of IT strategic goals. Current measures for availability reflect a lack of underlying measures that would indicate the potential for adverse customer impacts and do not take into account the differences in quality of service experienced by customers in regional offices.

To ensure completeness of data and insight into overall service reliability, reliability measures should account for all aspects of IT security from NIST's *Standards for Security Categorization of Federal Information and Information Systems*:

NIST Security Categories and Description

Security Category	Description
Confidentiality	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information.
Integrity	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information.
Availability	"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542] A loss of availability is the disruption of access to or use of information or an information system.

3.3 Emerging Customer Facing Services

Similarly, the FTC must invest in IT services that will most likely lead to an improved customer experience. On review of industry research and past budget requests, OCIO will seek an improved customer experience and availability through the expansion of IT services in the following categories (all language below is culled from Gartner service category definitions or related market research). Unless otherwise specified, expansion through software or platforms as a cloud service offers the best opportunity for improved availability when compared to current IT performance and practices.

- E-Discovery software facilitates the identification, collection, preservation, processing, review, analysis and production of electronically stored information to meet the mandates imposed by common-law requirements for discovery. These demands may be due to civil or criminal litigation, regulatory oversight or administrative proceedings. E-Discovery requirements tend to generate heterogeneous solutions that must consider both cloud and on premise hosting arrangements.
- Cloud Office Suites refer to integrated packages for unified communications (telephony, messaging, video-conferencing, email) and office productivity tools (word processing, spreadsheets, presentations).
- Enterprise Content Management (ECM) is used to create, store, distribute, discover, archive and manage unstructured content (such as scanned documents, email, reports, images and office documents), and ultimately analyze usage to enable organizations to deliver relevant content to users where and when they need it.
    - To meet government requirements, any vendor providing this service must cover all FTC needs to ensure compliance with NARA and OMB Memorandum M-12-18 Managing Government Records Directive
    - This includes the requirement that by December 31, 2016 Federal agencies will manage both permanent and temporary email records in an accessible electronic format
- Enterprise File Synchronization and Sharing (EFSS) refers to a range of on-premises or cloud-based capabilities that enables individuals to synchronize and share documents, photos, videos and files across mobile devices, such as smartphones, tablets and PCs. Sharing can happen between people (for example, partners and customers) within or outside the organization, or on a mobile device, as data sharing among apps. Access to files in enterprise repositories (such as file servers and content platforms) from mobile devices or remote PCs extends user productivity and collaboration. Security and collaboration support are critical aspects for enterprises to implement EFSS.
    - To meet government requirements, any vendor providing this service must cover all FTC needs to ensure compliance with NARA and OMB Memorandum M-12-18 Managing Government Records Directive
- Application Platform as a Service (aPaaS) is a cloud service that offers development and deployment environments for application services. An aPaaS that is designed to support the enterprise style of applications and application projects (high availability, disaster recovery, security and technical support) is an enterprise aPaaS. This may replace all internally developed and hosted applications, i.e., Oracle applications.
- Web Content Management (WCM) is the process of controlling the content to be consumed over multiple digital channels using specific management tools based on a core repository. This service may be procured as part of commercial products, open-source tools or hosted service offerings.
- Infrastructure as a Service (IaaS) offers the capability to deliver virtual machines, along with the basic storage and networking capabilities associated with those computing resources. For the purposes of the FTC, IaaS represents scalable access to services that include, but are not limited to, support of E-Discovery and advanced economic analytics.

- Identity and access management as a Service (IDaaS) delivers a predominantly cloud-based service in a multitenant or dedicated and hosted delivery model that brokers core identity governance and administration, access and intelligence functions to target systems on customers' premises and in the cloud.
  - To meet government requirements, any vendor providing this service must also show the capability to implement a mobile derived PIV credential as part of a complete solution for NIST 800-157 and HSPD-12.
  - The business process for granting credentials must align with government practices for background checks, ensuring human capital and security management needs are met.
- Enterprise Data Loss Prevention (DLP) solutions incorporate sophisticated detection techniques to help organizations address their most critical data protection requirements. Leading characteristics of enterprise DLP solutions include a centralized management console, support for advanced policy definition and event management workflow. Integrated DLP is a limited DLP feature set that is integrated within other data security products, including, but not limited to: secure web gateways, secure email gateways, email encryption products, ECM platforms, data classification tools, data discovery tools and cloud access security brokers.
- IT Service Support Management (ITSSM) tools help infrastructure and operations organizations manage the consumption of IT services, the infrastructure that supports the IT services and the IT organization's responsibility in supporting these services. IT service desks and IT service delivery functions most heavily use these.
  - Any ITSSM solution must be able to satisfy all FTC needs; enabling a common customer service platform across OED

A Business Process Re-engineering (BPR) review will need to occur to assess current mission needs and evaluate technology solutions to meet future needs. For example, current premerger filings are paper based; the FTC automating premerger filings improves data accuracy, response time, customer support and lowers costs. BPR that includes leveraging technology enables the FTC to gain efficiencies agency-wide.

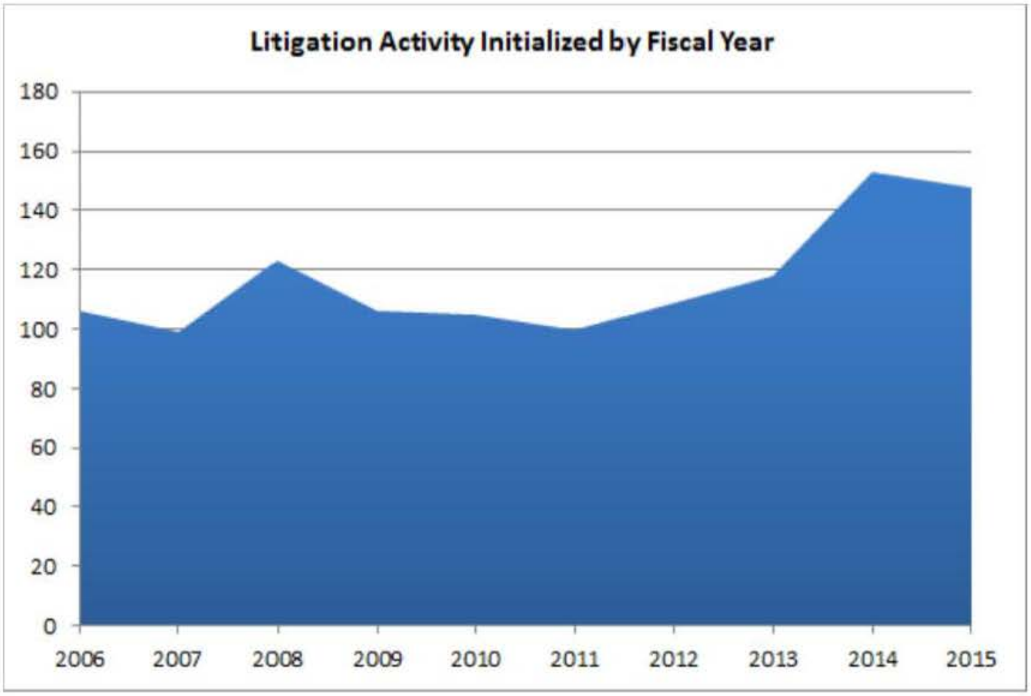
4 Target IT Performance and Practices

4.1 Mission Critical Customer Focus

FTC staff rely on the agency's IT systems to manage the high volume of information gathered as part of the agency's law enforcement, research, and consumer education initiatives, and to comply with mandates concerning the preservation and handling of agency records. The FTC will continue to leverage technology to help staff effectively search, categorize, collect, review, analyze and produce records in litigation and to meet disclosure obligations under the Freedom of Information Act and other records laws.

Per recent history, the FTC should anticipate a continuance or increase in the amount of litigation activity and corresponding education of the public to maintain competition and protect consumers. Even if current demand holds steady, the FTC should prepare to process increasing amounts of data and conduct more economic analysis with each litigation activity. Accordingly, IT resources shall prioritize the delivery of litigation related services and communication of FTC points of view through events and multi-media communications. The FTC will ensure its systems allow the agency to effectively manage increasing volumes of data while meeting regulatory obligations.

FTC Mission Activity by Fiscal Year



4.2 Mobile Always Customer Experience

The standard experience for delivery of IT services will assume a mobile user, whether through a smartphone or Wi-Fi enabled device; standalone devices, such as workstations, shall continue. However, they will accommodate standard configurations as necessary for delivery of mobile and remote access. For example, even when using workstations within FTC offices, customers will login using 2-Factor Authentication (i.e. PIV card or username/password/RSA token). Application delivery teams shall modify testing to ensure customers can readily access and view IT services across mobile devices whether connected via VPN, Wi-Fi, or WAN/LAN.

To further specify the devices and methods of access to FTC Data, OCIO shall share recommendations through TechStats on standard equipment:

- Smartphones – The FTC must select a smartphone/carrier combination that allows users the convenience to securely download and use mobile applications in a way that prevents exfiltration of FTC data. To do so in a way that both provides security and a seamless customer experience, the FTC must decide:
    - Should the FTC operate and maintain two types of smart phones– with selection of multiple standards coming at a cost of increasing complexity for customer service?
    - Should the FTC route all internet access from those devices through a VPN – which comes at a cost of increased latency the farther staff are from the FTC data center?
- Workstation – The FTC must select a standard approach to workstation issuance that addresses needs for mobility and remote access. Ideally, the FTC can issue each person a Wi-Fi enabled 2-in-1 device that can serve as both a tablet and PC light enough for travel and remote access. To ensure the optimum level of resource support for issued equipment, the FTC must decide:
    - Should the FTC continue to support remote access from personal devices – which comes at a cost of staff addressing issues related to non-FTC equipment?
    - Should the FTC re-purpose existing equipment to build "zero-clients" for FTC staff to use at home – which comes at a cost of staff supporting an additional equipment standard?

4.3 Effective and Measurable Cybersecurity

Per its mission and per federal IT statutes and guidelines, the FTC must regularly assess its cybersecurity practices to ensure that they comply with federal directives and reflect the latest reputable research. FTC will transition to a proactive risk-based, continuous prevention and monitoring posture verse inspecting for compliance. Accordingly, the table below lists three practices critical to driving cybersecurity related policy and configurations at the FTC.

Cybersecurity Practices

Practice	Description
Confidentiality **Simplify Strong Authentication**	Engineer multi-factor authentication mechanisms that eliminate: • attack vectors capitalizing on single-factor authentication • expiring PINs and passwords
Integrity **Always Assume Breach**	Minimize the impact of an adversary gaining control of a user's credentials by engineering controls for data loss prevention that limit the adversary's access to data, monitoring outbound traffic for signs of exfiltration, and blocking inbound traffic from untrusted sources
Availability **Pursue Pragmatic Configurations**	Review and modify as needed FTC configurations and education so that the FTC workforce can adopt highly valued features – such as faster performance and ease of use – of information technology without increasing risk of security incidents

In accordance with these practices, configurations must reflect well thought out approaches such that the FTC can validate expected behavior. For example, in addition to using multi-factor authentication the FTC must also establish internal policies and procedures that emphasize use of industry recognized widely accepted protocols. The FTC must ensure that these are properly and continuously implemented, and consistent with existing NIST, GSA, and other applicable Federal guidance. Additionally, the FTC must establish standard operational parameters for use of those protocols through regularly reported availability measures as strategic security configurations.

As an example of the impact of the above practices on customers, the FTC can more pragmatically assess use of smartphones and accommodate the secure use of mobile applications by its workforce.

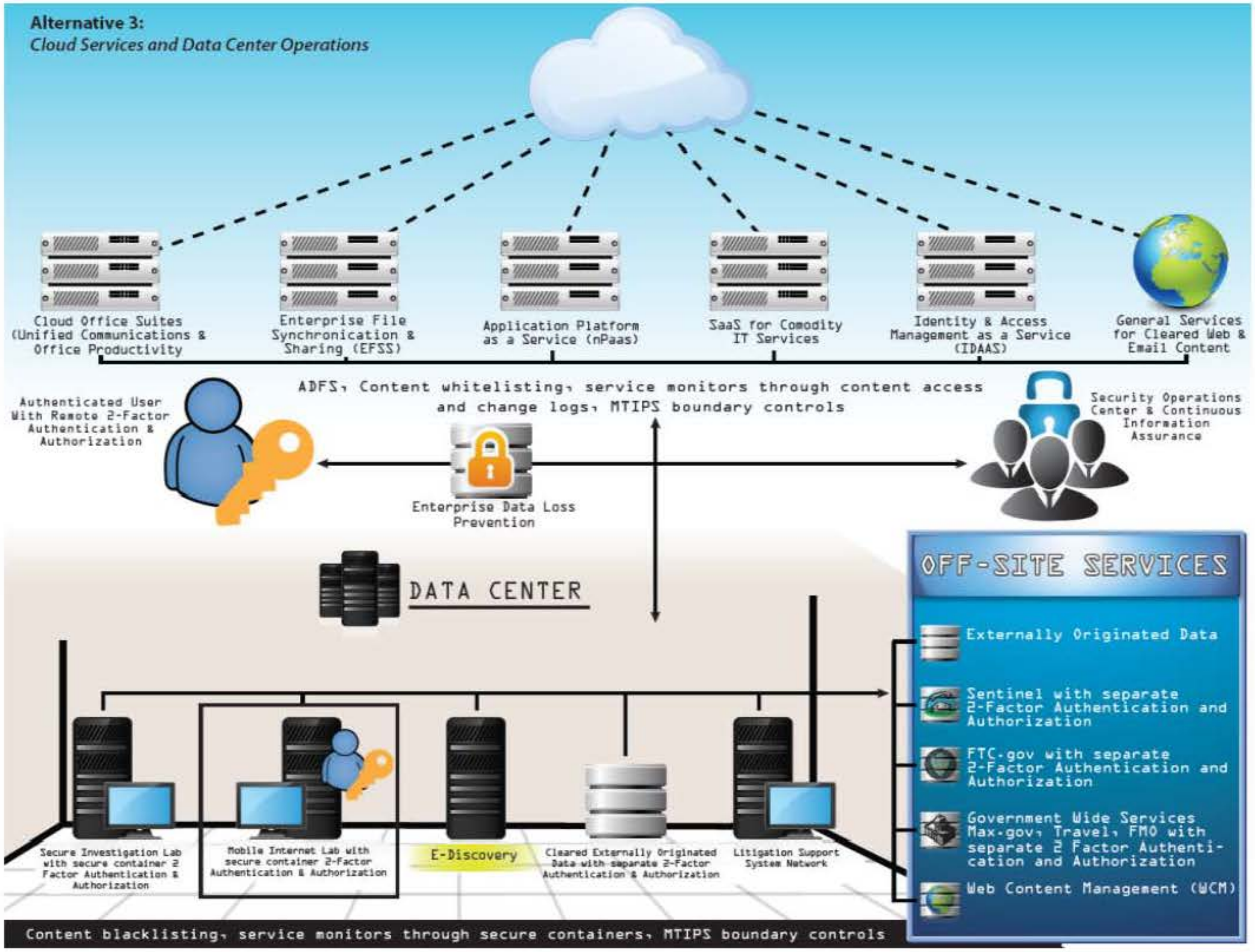
- Travel, navigation, food and drink, weather-related apps: FTC staff travel frequently, both locally and outside their duty area making applications such as Uber and Kayak very useful
- Social media and news-related apps: FTC staff often attend conferences where the audience provides real-time feedback through social media posts. Similarly, FTC staff would benefit from access to the latest news and information prior to court appearances.
- Other categories (e.g., gaming, health, photo/video, music): The Commission has made the privacy and security of apps a priority. Just as FTC staff benefited from minimally restricted internet access to gain a better understanding of the online marketplace, they will similarly benefit from minimal restrictions on mobile applications in order to better understand the mobile marketplace.

Once two-factor authentication is fully deployed, an additional impact of the above security practices would be the removal of the requirement to change passwords.

4.4 Highly Available Target Architecture

As depicted below, the target architecture uses FedRAMPed or government ATOed cloud services to increase availability of most office productivity services across all devices (smartphones, tablets, PCs) while continuing to host mission critical services in FTC data centers.

Baseline Alternative: Cloud Services and Targeted Data Center Operations


Alternative 3:
Cloud Services and Data Center Operations
Cloud Office Suites (Unified Communications & Office Productivity
Enterprise File Synchronication & Sharing (EFSS)
Application Platform as a Service (nPaas)
SaaS for Comodity IT Services
Identity & Access Management as a Service (IDAAS)
General Services for Cleared Web & Email Content
ADFS, Content whitelisting, service monitors through content access and change logs, MTIPS boundary controls
Authenticated User With Remote 2-Factor Authentication & Authorization
Enterprise Data Loss Prevention
Security Operations Center & Continuous Information Assurance
DATA CENTER
OFF-SITE SERVICES
Externally Originated Data
Sentinel with separate 2-Factor Authentication and Authorization
FTC.gov with separate 2-Factor Authentication and Authorization
Government Wide Services Max.gov, Travel, FMO with separate 2 Factor Authentication and Authorization
Web Content Management (WCM)
Secure Investigation Lab with secure container 2 Factor Authentication & Authorization
Mobile Internet Lab with secure container 2-Factor Authentication & Authorization
E-Discovery
Cleared Externally Originated Data with separate 2-Factor Authentication & Authorization
Litigation Support System Network
Content blacklisting, service monitors through secure containers, MTIPS boundary controls

Pros

Use of FedRAMPed commodity services allows re-allocation of current resources towards expansion of internally hosted litigation services as well as more efficiently addresses disaster recovery and failover for commodity IT.

Cons

Use of internally hosted litigation services likely requires use of failover ready disaster recover at an alternate data center with associated costs.

To further specify the allocation of services between the cloud and the FTC data center, OCIO shall share recommendations on the items below:

- Network Management and Monitoring – The FTC must select a combination of network management and monitoring that ensure the optimum access to available bandwidth from every authenticated and authorized endpoint (thin clients, workstations, smartphones, Wi-Fi connections, LTE connections).
    - Should the FTC, concurrent with moving all commodity IT services to FedRAMPed cloud services and enforcing use of secure access services in the FTC data center, adopt broadband access at all offices – which comes at a cost of monitoring each endpoint whenever connected to the internet as part of data loss prevention?
    - Should the FTC, concurrent with upgrading the network connectivity to support cloud services deploy a Virtual Private LAN Service (VPLS)?
- BIA/DR (Business Impact Assessment/Disaster Recovery) – The FTC must align its recovery services with its customer expectations for time to recovery.
    - Should the FTC, concurrent with moving all commodity IT services to FedRAMPed cloud services, state that FTC staff should expect to work from home to support continuity of operations – which comes at a cost of ensuring FTC staff have adequate resources to work from home?
    - Should the FTC, concurrent with upgrades to E-Discovery software, consider alternate hosting of E-Discovery software utilizing a cloud provider or a service provided by another agency – which comes at a cost of storing data at another site?
- E-Discovery software – The FTC must assess E-Discovery in the desired approach for BIA/DR and network management.
    - Should the FTC, if choosing to host E-Discovery software at the FTC data center, always have available failover for E-Discovery technology software – which comes at a cost of data storage at another facility?

4.5 Granular Reliability Measurement

The FTC will establish strategic configurations and measurements and review them as part of every regularly scheduled IT operations meeting. The configurations shall allow for:

- Communication of existing security posture based on recurring testing and security tool logs
- Measurement of IT service reliability across multiple devices and from any region
- Review of procurement related measurements to inform award of performance incentives for continuous improvement such as:
    - Service Level Agreements targeting 99.9% availability with avenues of recourse for sub-optimal performance
    - Logon monitoring that identifies failed authentication to alert technicians to down services ahead of customer calls to the help desk
    - Usage monitoring that identifies services for replacement or elimination
    - Minimal and granularly measurable network latency such as no more than 200ms time to first byte for any transaction from any office

4.6 Empowered Federal Workforce

FTC's Office of the Chief Information Officer (OCIO) holds the responsibility to provide the FTC with infrastructure, connectivity, and computing capabilities necessary for FTC staff and mission partners to access, share, and act on needed information. To ensure all staff, internal and external to OCIO, understand and acknowledge resource assignments, OCIO will organize its resources based on:

- Customer success supporting the needs of the business for innovation, flexibility, reliability, or engagement
- Improved oversight in support of generally acknowledged Clinger-Cohen management competencies

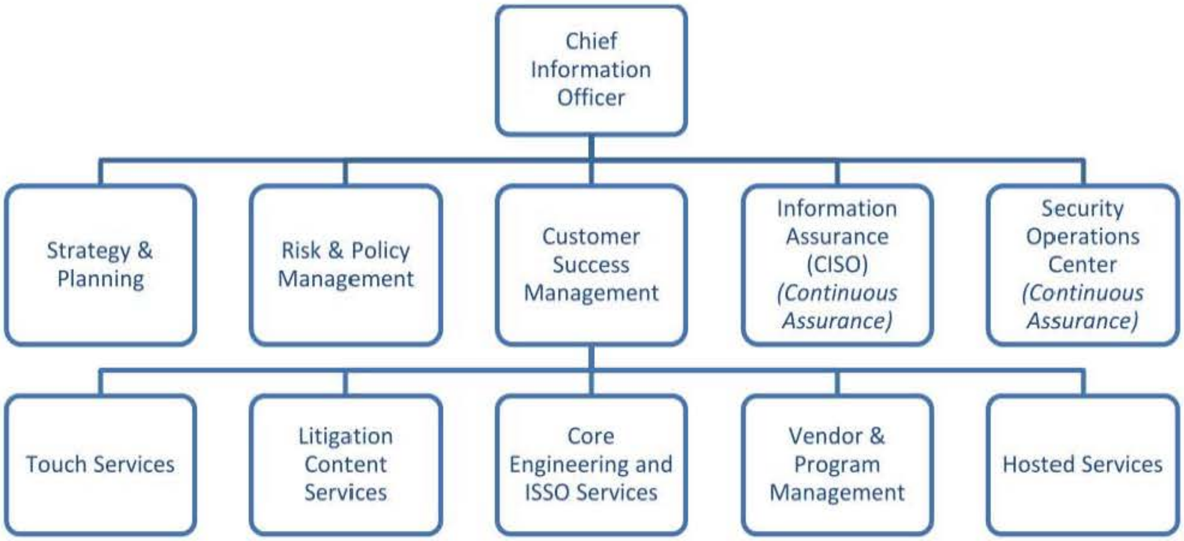
Across all staff, managers will ensure consistent adherence to the core competencies below to ensure measurable approaches to customer success and improved oversight:

- Partnership Core Competency: Customer, Stakeholder, and Peer Focused Communication, Team Building, and Knowledge Sharing
- Fact and Data-Driven Analysis Core Competency: Performance Measurement and Subject Matter Expertise

OCIO managers will support employees as they exercise opportunities for regular training across all Clinger-Cohen competencies with a strong emphasis on project, contract, and performance management. Managers will make sure progress is documented in employee IDPs.

OCIO's new focus on service delivery, project management, contract oversight, and continuous monitoring and authorization, requires a shift in the organization's hiring, training and management plans. With Clinger-Cohen competencies identified as the required knowledge skills and abilities, recruitment priorities shifted from hiring engineers and developers to IT program managers, business analysts, and information security analysts. The FY 2016 hiring priorities included recruitment efforts for the following positions: IT program managers, IT service leads, and program analysts.

Organization Structure


Chief Information Officer
Strategy & Planning
Risk & Policy Management
Customer Success Management
Information Assurance (CISO) *(Continuous Assurance)*
Security Operations Center *(Continuous Assurance)*
Touch Services
Litigation Content Services
Core Engineering and ISSO Services
Vendor & Program Management
Hosted Services

Team Duties and Desired Results

Organization	Team Duties	Desired Results
Chief Information Security Officer **Continuous Assurance**	• FISMA categorizations, control implementation, authorizations and assessments • POA&M management • Government-wide security reporting • Annual security training • Change management process	• Risk properly documented and reported to the commission • Commission risk tolerance defined • Continuous authorization of FISMA systems • ISSO design controls based on risk tolerance • SOC monitors ongoing threat status and suggests mitigations • Monitor progress on CAP security goals
Security Operations Center **Continuous Assurance**	• CIRT incidents • Internal investigations • Threat management • Security policies • US CERT Reporting	• Compliance with technical and security standards • Alert management on deviations from optimal technical and security operations • Continuous monitoring • Continuous authorization
Risk & Policy Management **Conducts continuous review and analysis of business practices, with the goal of improving decision making**	• Governance processes and procedures • Governance meeting management • Ensure IT decisions are made in partnership with business stakeholders	• Increased transparency agency-wide of performance gains, challenges, and actions underway to correct deficiencies • Policies and procedures are assessed for effectiveness and impact on the budget, performance, and operations services

Organization	Team Duties	Desired Results
Strategy & Planning **Ensures information technology investments make meaningful and measurable impacts on the FTC mission**	• Budget and financial management • Strategic planning • Data and performance analysis • Discover new technologies and monitor IT trends • Overall enterprise architecture accountability and central artifact repository	• IT strategy and transition plan aligns with FTC mission and strategic plan, and drive creation and management of IT budgets • Acquisition strategy and HR recruitment aligned with skills required to execute IT strategy and transition plan • Representation of FTC services and performance reflects industry best practices to inform evaluation of FTC capabilities • Customers welcome changes prescribed in the IT Strategy
Core Engineering & ISSO Services **Provides the foundation required to deliver robust, scalable, and integrated IT services**	• Maintenance and management of data centers • Server environment management • Network management • Configuration management • Manage test lab environment • Desktop engineering • Patch management • Storage management • Remote access management • PIV implementation • DR procedures • Technical architecture development	• Proactively provision systems and services which align with agency needs and client expectations • Balance availability, security, functionality and ease of use to provide cost effective services • Creation of an architecture library to contain baseline configurations, as well as justifications for deviations
Litigation Content Services **Focuses on customer needs related to Litigation processing**	• Maintenance and management of enterprise litigation applications • Technical consultant and system owner for Litigation Support System environment	• Become a valued litigation solution provider for the customer • Prioritize and resolve issues • Understand the work being performed and customer needs • Find litigation support products that meet customer needs (in-house or in the cloud)

Organization	Team Duties	Desired Results
Touch Services **Focuses on putting the "human touch" at the core of IT service delivery, shifting the way we communicate, deliver and support IT services**	• Helpdesk management • Asset management • Intranet web page development and maintenance • Remote litigation team support • Enterprise content management • Event planning • Audio, video, and photo support • Graphic support • Print services • Web applications • SES support • Calling card program	• Improved communication with customers • Improved level of customer service and personalized support • Tailor services to better meet the needs of the customer • Increased customer satisfaction
Hosted Services **Determines appropriate service offering to meet current and future customer needs**	• Application management • Secure environment support • Technical POC for externally hosted agency systems • COTS application support • Database support • Ticket escalation/Desktop support • Enterprise software management	• Delivers modern, scalable, and secure environments to the FTC • Services that do not need to be hosted inside the FTC can be moved to an external provider for recognized cost savings, added reliability, enhanced security, or with greater methods of access to the data
Vendor & Program Management **Enables the organization to improve performance through increased value from vendors**	• Contract management • Contract renewals • Invoicing • Project management office • 508 compliance	• IT resources and work efforts are transparent, integrated, and traceable to clear business outcomes and user benefits • Establish clear and effective service levels for all contracted services • Vendors actively contribute ideas to improve efficiency and accelerate innovation (b)(5)

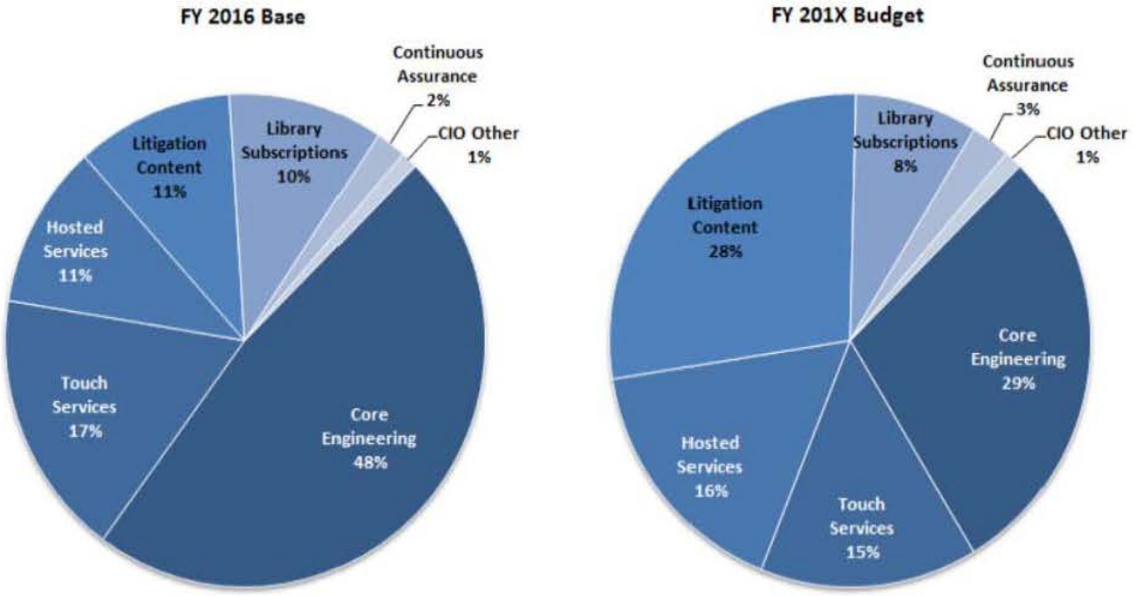
(b)(5)

(b)(5)

4.8 Zero-Based Spending

Reallocation of existing funds through the adoption of emerging services, and additions to base starting in FY2016, can improve support for litigation and economic services. OCIO shall manage detailed breakdowns by purchase item level that identify line items subject to replacement by emerging services, such as Documentum by ECM or EFSS, or render line items as non-essential, such as the current spending on development and test environments for commodity services.

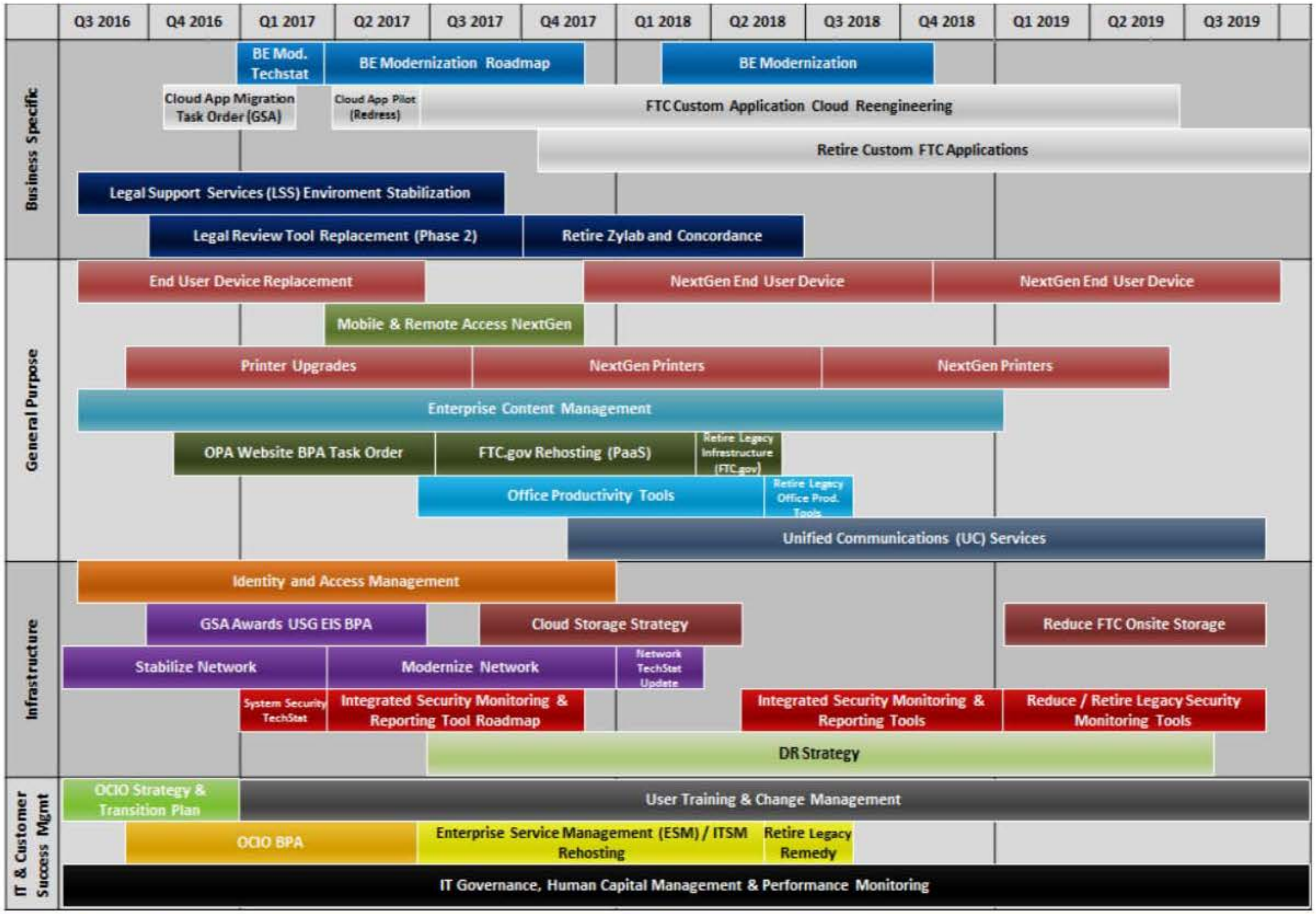
Summary of Current and Future Budgets



5 Transition Plan Estimates

Below is the high-level transition schedule and cost estimate. The current priority of FTC resources is on the BPA, and the network stabilization and optimization project. The initial transition projects will move the suite of office productivity tools and the enterprise service management tool to the cloud.

Transition Schedule



The above transition schedule assumes that there will be multiple projects aligned to each strategic initiative; these projects will cover both new features and decommission legacy technology. Additionally, each strategic initiative outlined above will align to a service plan.

(b)(5)

6 References

- Chiasson, S., & van Oorschot, P.C. (2015). Quantifying the Security Advantage of Password Expiration Policies. *Designs Codes and Cryptography, 77*(2), 401-408.
- Zhang, Y., Monrose, F., & Reiter, M. (2010). The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis. In Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10), 176-186.

7 Appendix: Service Categories

Service Portfolio	Service Categories	Proposed SLAs
Business Specific **Software used to support primary business specific functions**	• Acquisition and Financial Management • Business Administration Management • Consumer Protection Support • Economic Analysis • Human Resources • Litigation Support • Maintaining Competition	• User satisfaction composite >85% • Operating environment composite >85%
General Purpose **Processes, software and hardware/equipment used to support general day to day work related activities across the enterprise**	• End User Device – Fixed • End User Device – Mobile • Enterprise Collaboration, Productivity, and Communication • Enterprise Content Management • Management Tools • Media/Event Support • Web Presence	• User satisfaction composite >85% • Operating environment composite >85%
Infrastructure **Access points**	• Remote Access • Secure Authentication • Identity and Access Management • Infrastructure and Network Management • Monitoring Tools • Operating Systems/Email • Security Management Services • Storage Management	• Operating environment composite >85%
IT & Customer Success Management **Services that enable IT Customers to make better use of IT Services**	• Services Quality • Services Management	• Effective IT resources composite >85%

The makeups of the proposed SLA composites are under evaluation.