OIG EVALUATION

of the Federal Trade Commission's Office of the Chief Information Officer

Report No. ER 16-02 // December 2015

Executive Summary

The Federal Trade Commission (FTC) is an independent law enforcement agency founded in 1914 with the passage of the Federal Trade Commission Act. The mission of the FTC is to protect consumers by preventing anticompetitive, deceptive, and unfair business practices, enhancing consumer choice and public understanding of the competitive process, and accomplishing this without unduly burdening legitimate business activity. To execute its broad mandate, the FTC employs a variety of tools, including law enforcement, rulemaking, advocacy, research and studies on marketplace trends, and consumer and business outreach and education.

The Chief Information Officer (CIO) occupies a critical position within the FTC and with external stakeholders, whose sensitive information is housed in FTC's databases and repositories. The Chief Information Officer's role is defined in several statutes and directives, including the Clinger-Cohen Act of 1996, the Federal Information Security Management Act (FISMA) of 2002, the Federal Information Technology Acquisition Reform Act (FITARA), and directives issued by the Office of Management and Budget (OMB). At the FTC, the CIO heads the Office of the Chief Information Officer (OCIO), which executes and manages the agency's information technology and information security responsibilities. The FTC's stewardship of its IT investments and the safeguarding of its sensitive nonpublic holdings are uniquely important, given the FTC's leading role in monitoring merger and acquisition activities, advocating for protection of consumer information and consumer privacy, and hosting a national repository of consumer complaints.

In the FTC, the CIO reports to the Executive Director who, in turn, reports directly to the Chairwoman. The Office of the Executive Director (OED) manages the agency's five customer support entities, including the OCIO, the Administrative Services Office, the Records and Filings Office, the Financial Management Office, and the Human Capital Management Office. The Executive Director also chairs the FTC's IT Governance Board, the highest tier of the FTC's IT investment governance structure.

The FTC Office of Inspector General (OIG) performed this evaluation to determine whether the OCIO has the authority, resources, structure, and organizational support needed to accomplish its current priorities and to assist the agency in realizing its mission. The OIG assessed the state of the OCIO's planning efforts in defining and documenting its mission, vision, objectives, and priorities. In conducting this evaluation the OIG reviewed key statutes and documents governing OCIO's operations, conducted 30 interviews of supervisory and non-supervisory personnel in the OCIO and other agency stakeholders, and performed an analysis of other federal agencies' IT units to identify similar challenges, solutions for overcoming obstacles, and potential best practices.

In this evaluation we found that:

A disconnect between authority and responsibility diminishes the CIO position. The current agency organizational and IT governance body structures limit the CIO's ability to reject a customer request for immediate assistance or to stop or modify an IT investment. Positioning the OCIO under a customer-service entity such as the OED often thwarts the OCIO's ability to reject a customer request or push back on a proposed mission need. Furthermore, while the CIO is represented – and plays an important role – on all three IT governance bodies, the CIO is a non-voting, ex-officio member of the highest two bodies – the IT Governance Board (ITGB) and the IT Business Council (ITBC). Another vital position in the agency's information security leadership – the Chief Information Security Officer (CISO) – is not a member of either body. The CIO's subordinate role on the FTC's IT governance boards diminishes

the CIO's ability to advance the CIO's authority and hampers the ability of the CIO to execute the agency's information security and IT mission. As the FTC moves to incorporate the principles of enterprise risk management for managing IT investments and establish a common structure for project management, the CIO should be empowered to help the FTC realize strategic IT priorities for the agency and fulfill the CIO's information security responsibilities.

High turnover in the CIO position hampers short-term and long-term planning efforts. Since 2000, the FTC has had five permanent CIOs who served an average tenure of 2.8 years or 34 months, and seven acting CIOs. Consequentially, OCIO employees have lacked consistent direction and clear focus, with each CIO having his own agenda and approach. Adapting to a challenge experienced across the federal government, OCIO personnel and agency stakeholders have had to adjust to each new permanent and acting CIO's policy and procedural approach. While previous CIOs undertook formal planning and modernization efforts, the strategic planning process has been hampered by leadership turnover, leaving the emphasis on "putting out fires." When combined with insufficient resources, the absence of strategic focus means that the OCIO's priorities and objectives do not align with the agency's enterprise-level priorities, but rather with maintaining and enhancing existing infrastructure. While long-term IT planning is difficult when an IT unit's base budget cannot fund its current operations and must rely on unfunded requirements (UFRs) for new, multi-year investments, the absence of enterprise-level strategic IT planning leaves the FTC more vulnerable to increased costs, outdated technologies, duplication of effort, poor or degraded performance of its IT systems, and potential data breaches and cyberattacks. To mitigate these risks and help the agency accommodate future leadership transitions, the FTC should develop and implement an IT strategic plan and provide increased transparency through communication of IT project priorities and status to OCIO staff, customers, and stakeholders. Other essential priorities for the OCIO's new leadership are measures to ensure the OCIO staff is right-sized and right-skilled, strengthen the OCIO's mid-level leadership, and provide training for IT planning and modernization efforts.

Lack of clear delineation and understanding of OCIO employees' roles and responsibilities creates confusion and limits accountability. Our review identified confusion among both OCIO employees and customers as to what responsibilities OCIO employees and branches execute, and a general lack of communication and transparency about projects. Lack of role clarity stems from 1) unclear, outdated, and frequent discrepancies in OCIO employee position descriptions; 2) lack of skilled personnel in key positions, resulting in high-performing OCIO employees gravitating to complete work outside their branch's area of responsibility; and 3) an antiquated organizational structure that does not promote matrixed management. Without clear delineation of duties, employee accountability is difficult to enforce and poor performers are not disciplined, thereby diminishing the higher performers' contributions and lowering morale. The current OCIO organizational structure also lacks a central planning unit or individual tasked with coordinating all planning endeavors, along with research and development capability, leaving the agency behind the curve in optimizing its information security and IT infrastructure. The agency's relatively immature governance process for IT acquisitions does not ensure full stakeholder participation in IT planning or development of user-focused metrics to measure the OCIO's contribution to the agency's mission. As the agency's IT governance structure matures, the OCIO will be better equipped to evaluate its performance and improve customer relations by developing, collecting, and reporting user-focused metrics.

Poor contract management compromises the OCIO's mission. Agency stakeholders reported adverse ramifications from poor requirements gathering, drafting, and oversight of IT contracts by OCIO personnel. Specifically, the OIG found that 1) some OCIO employees who serve as Contracting Officer's Representatives (COR) lack project and contract management skills even though they serve as CORs on as many as 15 separate contracts; 2) OCIO does not correctly capture end user requirements in initial contract solicitations; 3) end users' initial needs sometimes expand beyond the initially defined contract boundaries; and 4) IT contracts do not specify proper performance metrics or define the process for measuring objectives. As we identify in our Final Report Assessing the Federal Trade Commission's Compliance with the Federal Information Security Management Act for Fiscal Year 2014, contractor performance and user-centric system monitoring measures are essential for the successful evolution of the FTC information assurance and privacy programs. Taken together, we found these shortfalls increase the agency's risk for poorly performing contractors and vendors, undelivered or delayed capabilities and functionality, protracted litigation, and, ultimately, challenges for mission success. As FTC management continues to implement OIG FISMA recommendations to improve contract management and adopt acquisition best practices, there are opportunities for FTC leadership to accelerate these efforts.

To address these findings, we recommend that the FTC:

1. Extend voting rights to the Chief Information Officer on the FTC IT Governance Board and the IT Business Council.
2. Identify the current OCIO core competencies and determine how they align with stakeholder needs, and identify performance shortfalls and gaps and their root causes (e.g., personnel, policy, business processes, resources, or technology).
3. Using the data developed through the core competency assessment, the FTC's Quadrennial Strategic Plan, and other agency priorities and initiatives, develop an IT Strategic Plan. The IT Strategic Plan should establish goals and objectives to serve both a) internal customers (operations and infrastructure) and b) external stakeholders (including federal partners, litigants, contractors, and consumers) that incorporate principles of enterprise risk management, performance-based metrics, and change management.
4. Assign ongoing responsibility to staff for conducting a) strategic planning, b) enterprise architecture planning that accommodates the Federal Enterprise Architecture relevant to the FTC mission, c) prototypes of emerging technology activities, and d) agency IT acquisition strategy to help anticipate and plan for the agency's future IT and information security requirements.
5. Update all OCIO employees' position descriptions to delineate current job descriptions, correct grade and promotion potential, and supervisory status; ensure position descriptions for OCIO managers include review of Contracting Officer's Representative (COR) performance in collecting and drafting contract requirements and monitoring contractor performance.
6. Using established Office of Management and Budget, Federal Acquisition Regulation, Federal Acquisition Institute, and other guidance, and in coordination with the development of the IT Strategic Plan, develop an acquisition strategy that reduces the complexity of current procurements and increases stakeholder visibility into contractor performance.

7. Publish IT services that align with stakeholder requirements and the Quadrennial FTC Strategic Plan, service levels, and corresponding levels of resources required to provide these service levels, and post this data on the FTC Intranet.
8. Using the core competency assessment and published IT services, and in coordination with the development of the IT Strategic Plan, develop a recruitment, hiring, and training plan to acquire and sustain personnel needed for improved contract management, program management, and oversight within OCIO and in the FTC's Bureaus and Offices, and for IT service delivery across the FTC.

In response to a draft of this report, FTC management concurred or partially concurred with our recommendations and proposed corrective actions to improve the OCIO and the FTC's information security and information technology mission. We consider management's planned actions responsive and will close the recommendations upon verification that the agency has completed them.

Management's response is reprinted in Appendix B.

Table of Contents

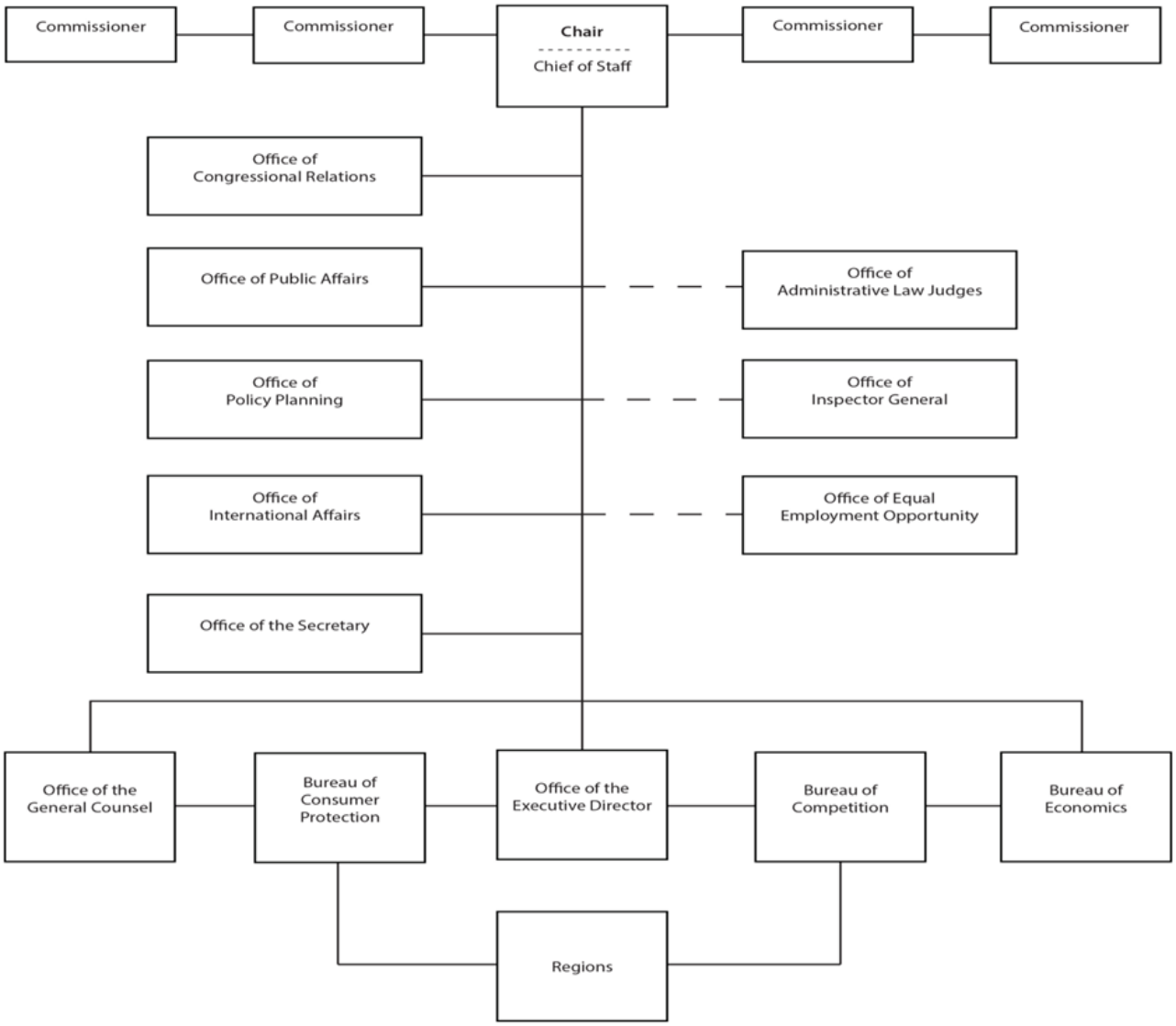
List of Figures

Background

The Federal Trade Commission (FTC) is an independent law enforcement agency, founded in 1914 with the passage of the Federal Trade Commission Act. The mission of the FTC is 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. In this endeavor, the FTC administers and enforces over 70 laws and regulations, including the Federal Trade Commission Act, Fair Credit Reporting Act, the Clayton Act, the Business Opportunity Rule, and the Telemarketing Sales Rule.

The FTC is led by a Commission of five members, each of whom is nominated by the President, approved by the Senate, and serves for a period of seven years. The President chooses one commissioner to act as Chair. No more than three members may be from the same political party. The organizational structure of the FTC is illustrated in Figure 1, shown below.

Figure 1: Federal Trade Commission (FTC) - Organizational Chart



Why We Did This Review

1. Legislation and Directives

Over the last 40 years, Congress has enacted various laws to improve the government's management of both information and technology. The Clinger-Cohen Act of 1996 attempts to strengthen Information Technology leadership by requiring agency heads to designate Chief Information Officers (CIOs) with sufficient authority to provide accountability. These CIOs are responsible for:

- Implementing and enforcing applicable government-wide and agency information technology (IT) management policies, principles, standards, and guidelines;
- Assuming responsibility and accountability for IT investments;
- Assuming responsibility for maximizing the value and assessing and managing the risks of IT acquisitions through a process that, among other things, is integrated with budget, financial, and program management decisions, and provides for the selection, management, and evaluation of IT investments;
- Establishing goals for improving the efficiency and effectiveness of IT operations through the effective use of IT;
- Developing, maintaining, and facilitating the implementation of a sound, secure, and integrated IT architecture; and
- Monitoring the performance of IT programs and systems and advising the agency head whether to continue, modify, or terminate such programs and systems.[1]

Likewise, the Federal Information Security Management Act (FISMA) of 2002 recognizes the importance of information security and created a framework for securing the federal government's IT systems. Agency officials play a vital role in conducting and/or participating in annual reviews of the agency's information security and privacy programs. The Federal Information Technology Acquisition Reform Act (FITARA) of 2014 further strengthens the role and authority of the CIO position by requiring heads of certain agencies to ensure their CIOs have a significant role in IT decision-making, including annual and multi-year planning, programming, budgeting, execution, reporting, management, governance, and oversight functions.[2]

The Office of Management and Budget (OMB) has paralleled these congressional actions with policy memoranda, circulars, and bulletins assigning areas of focus, roles and responsibilities, and reporting obligations for federal CIOs. OMB Circular A-130 provides policy guidance on managing information resources within federal agencies. In accordance with FISMA, OMB mandates that CIOs have the lead role over the agency's IT governance, commodity information technology, program management, and information security.[3] In its FITARA implementation guidance, OMB established a common baseline for roles, responsibilities, and authorities of the agency CIO and other applicable senior agency officials

[1] Public Law 104-106, Clinger-Cohen Act of 1996.
[2] While FISMA applies to all federal agencies, FITARA only applies to those agencies covered by the Chief Financial Officers (CFO) Act, though all executive branch agencies are encouraged to apply its principles. The FTC is not covered by the CFO Act.
[3] OMB M-11-29, *Chief Information Officer Authorities* 1-2 (August 8, 2011).

in IT management, together with guidance on strengthening the CIO's accountability for the agency's IT cost, schedule, performance, and security.[4]

2. FTC Information Technology and Security

CIOs at federal government agencies oversee the management of significant IT investments – totaling nearly $70 billion in FY 2014 – along with the employees and contractors who administer them.[5] In FY 2014, the FTC earmarked approximately one-fifth (18.5%) or $55.7 million of the agency's annual $298 million budget for IT expenditures.[6] The FTC CIO is responsible for overseeing that these funds are allocated to deliver, maintain, and secure the information security and IT needs of the agency's approximately 1,164 employees in furtherance of the agency's mission.

The FTC's stewardship of its IT investments and the safeguarding of its sensitive nonpublic holdings are uniquely important, given the FTC's role in monitoring merger and acquisition activities, advocating for protection of consumer information and consumer privacy, and hosting a national repository of consumer complaints. The FTC urges private entities to incorporate reasonable security measures that are commensurate with the sensitivity and volume of consumer information they hold and the cost of available tools that can improve security and reduce vulnerabilities.[7] Likewise, the FTC brings enforcement actions in federal courts against companies it believes fail to adequately protect consumers' private data, including Social Security numbers, birthdates, and credit card and report information.[8] The FTC also maintains the federal government's central repository for consumer fraud and identity theft complaints and administers the National Do Not Call Registry, a service that enables consumers to avoid unwanted telemarketing calls.

Confidentiality and information security are also integral to the FTC's competition mission. Investigations of potential corporate mergers begin when companies submit premerger notification filings to the FTC and the Department of Justice. The FTC maintains and assesses premerger filings on a confidential basis pursuant to the Hart-Scott-Rodino Act of 1976, and stresses to its workforce the obligation to maintain strict confidentiality of these holdings.[9] As the FTC stated in 2014 in assessing its information security progress:

> Maintaining the confidentiality of nonpublic agency information is critical because obtaining sensitive, nonpublic information from businesses and consumers is the lifeblood of agency law enforcement investigations, and those sources would be reluctant to share such information in the absence of effective confidentiality safeguards.[10]

---

[4] OMB M-15-14, *Management and Oversight of Federal Information Technology* (June 10, 2015).
[5] "Federal IT Spending Decreasing by Billions," *Computerworld* (October 15, 2013). http://www.computerworld.com/article/2486120/government-it/federal-it-spending-decreasing-by-billions.html.
[6] Figures provided by OCIO to the OIG on July 20, 2015.
[7] Jessica Rich, "Data Security: Why It's Important, What the FTC is Doing About it" (March 24, 2014), *available at* https://www.ftc.gov/system/files/documents/public_statements/295751/140324nclremarks.pdf, at page 4.
Prepared Statement of the Federal Trade Commission on Protecting Consumer Information: Can Data Breaches Be Prevented before the Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade, United States House of Representatives (February 5, 2014), *available at* https://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-consumer-information-can-data-breaches-be/140205databreaches.pdf.
[8] Prepared Statement of The Federal Trade Commission on Data Security and Breach Notification Act of 2015 before the Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade, United States House of Representatives (March 18, 2014), *available at* https://www.ftc.gov/system/files/documents/public_statements/630961/150318datasecurity.pdf.
[9] FTC's *Premerger Notification Program*, available at https://www.ftc.gov/enforcement/premerger-notification-program.
[10] FTC Office of Inspector General, *FY 2014 Management Priorities and Challenges*, 22-26, *available at* https://www.ftc.gov/system/files/documents/reports/ftc-fy-2014-summary-performance-financial-information/150218fy14spfi.pdf.

For these reasons, and to leverage the previous work of the FTC's Office of Inspector General (OIG) and reports by the U.S. Government Accountability Office (described below), we undertook this evaluation of the FTC OCIO. The objective of this evaluation was to assess whether the FTC OCIO has the authority, resources, structure, and organizational support it needs to accomplish its current priorities and assist the FTC in realizing its mission, and to make recommendations to advance those objectives.

3. Related OIG Reports

This evaluation follows several previous OIG reports that identify ongoing challenges with information security, management of IT investments and the performance of the OCIO. Most recently, in our FY 2014 FISMA evaluation report, we made six recommendations that come under the purview of the OCIO:

- The FTC should continue to evolve IT governance practices and expand the use of capital planning and investment control (CPIC) and investment analysis processes to document investment decisions. Ensure that risk-based decisions are appropriately documented for input to Information Security Continuous Monitoring (ISCM) reporting;

- The FTC should accelerate its implementation of NIST SP 800-39 compliant risk-based governance and IT investment processes. These processes should be applied to the FTC IT modernization effort and its associated activities;

- The FTC should take appropriate action to ensure completion of an appropriate Configuration Management (CM) plan and ensure that it is effectively applied to the FTC and across all FTC systems;

- The FTC should revise its process for determining Minor Applications and documenting security controls. Minor Applications should be differentiated from system services/functions and should be documented in a format that supports the ability to assess the security impact of a Minor Application as well as its impact on the associated General Support System (GSS). System Security Plans (SSPs) should adequately document control environments so that they can serve as an implementation guideline, a security baseline for testing, and a reference for individuals assessing the level of control compliance;

- The FTC should apply its revised governance process to PIV implementation so that compliance is not subject to continuing delay; and

- The FTC should develop a disaster recovery strategy and implementation plan.

In conducting its annual reviews of the FTC's most serious management and performance challenges, the OIG identified securing the FTC's information systems and networks from destruction, data loss, or compromise as a top management challenge in the last four fiscal years (FY 2012, FY 2013, FY 2014, and FY 2015). The ability to protect information assets is a complex challenge for the FTC, especially as the agency tries to integrate new technologies (e.g., cloud and mobile computing) into its IT infrastructure and as new and pervasive risks and actors threaten to disrupt or compromise operations. Senior management turnover (at the chief experience officer or CXO level, including the CIO) within

the last two years poses further challenges to improving information security and privacy programs at the FTC.

4. GAO Reports on CIOs and IT Management

The Government Accountability Office (GAO) has conducted numerous studies on ways to strengthen the role of the CIO, IT, and information management leadership and accountability in federal agencies. In its September 2011 report, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management*, GAO polled 30 federal agencies to assess the effectiveness of various CIO reporting structures. GAO concluded that a variety of reporting relationships between an agency and CIO can be effective so long as the CIO has direct interaction with the agency head and with senior executives across the agency.

In its March 2015 report on the state of the IT mission at the Library of Congress, GAO identified six essential and overlapping areas that provide a sound foundation for IT management: IT investment management, systems acquisition and development, information security and privacy, service management, IT leadership, and strategic planning. GAO concluded that effective strategic planning should include an IT strategic plan and enterprise architecture that outline the IT goals, performance metrics, timelines, and a parallel human capital plan to ensure that the IT workforce has the necessary skills to accomplish IT functions as well as support the agency's overall mission.[11]

Because the policy, technical, and human capital challenges facing the FTC are similar to those encountered by other federal agencies, we considered the themes and findings from the OIG's body of work, GAO guidance, and other federal OIG reporting in developing our recommendations.

[11] GAO Report 15-315, *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses* (March 2015).

Purpose, Scope, and Methodology

1. Purpose

Over the past few years, the OCIO has experienced significant leadership and operational changes. Given the flux in the CIO position as well as other factors, this review evaluated the state of the OCIO's planning efforts in defining and documenting their mission, vision, objectives, and priorities. Additionally, we assessed whether the OCIO has the authority, resources, structure, and organizational support needed to accomplish its current priorities and help the agency realize its mission.

2. Scope

This evaluation focused on answering the following questions:

- How has the OCIO's responsibilities evolved over the past five years and does it have the necessary resources and structure to meet those responsibilities?
    - What knowledge, skills, and abilities should OCIO staff possess to perform their jobs effectively?
    - What workforce changes, if any, would help the OCIO meet their objectives?
    - What obstacles and/or challenges does the OCIO encounter when introducing changes that affect its immediate workforce?
    - Is the OCIO's organizational structure conducive to mission needs?
- What authorities does the OCIO possess?
    - What challenges, if any, does the OCIO experience when exercising its authorities? What obstacles and/or challenges does the OCIO encounter when interacting with colleagues throughout the agency on technical, system, or application matters?
    - Does the OCIO have the agency support it needs to accomplish its mission?
- What are the OCIO's key initiatives and what are the status, challenges, and constraints surrounding these initiatives?

3. Methodology

This evaluation was conducted in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency in January 2012.

To inform this assessment, the OIG employed the following tools:

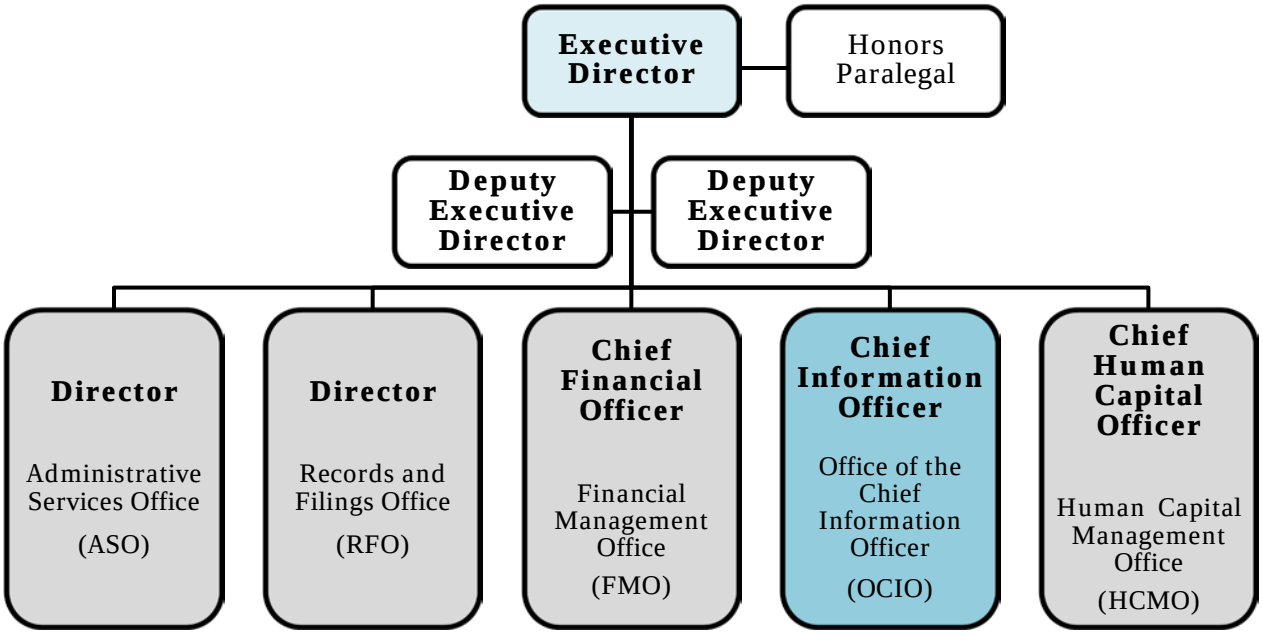
- **Document Review** – The OIG reviewed documents that provided historical, current, and/or future information about OCIO programs, priorities, and its workforce. The types of documents reviewed during this evaluation included:
  - Strategic, risk management, and contingency planning documents;
  - Functional responsibility statements for each OCIO branch;
  - Current and proposed OCIO organizational charts;
  - Prior organizational assessments and audits conducted on the OCIO; and
  - Key statutes, directives, and guidelines that govern OCIO operations.
- **Interviews** – The OIG conducted interviews with thirty current or former FTC employees. We interviewed both supervisory and non-supervisory employees from the OCIO, Bureau of Competition (BC), Bureau of Consumer Protection (BCP), Bureau of Economics (BE), Office of the Executive Director (OED), the Human Capital Management Office (HCMO), and the Office of the Chairwoman.
- **Benchmarking** – The OIG performed an analysis of other federal agencies' IT units to identify potential best practices, the types of IT challenges other organizations face, and how they are addressed. We selected agencies with a law enforcement or regulatory mission and, in some instances, a comparable employee count. The OIG selected three agency IT units to benchmark:
  - The Equal Employment Opportunity Commission (EEOC), Office of Information Technology (OIT);
  - The Federal Deposit Insurance Corporation (FDIC), Division of Information Technology (DIT); and
  - The Securities and Exchange Commission (SEC), Office of Information Technology (OIT).

OCIO Organizational Structure, Mission, and Priority Projects

1. The OCIO Organizational Structure

Headed by a Chief Information Officer (CIO), the OCIO is a centralized unit that services the FTC's offices and three bureaus – the Bureaus of Consumer Protection (BCP), Competition (BC), and Economics (BE) – from its position under the Office of the Executive Director (OED) (Figure 2, shown below).

Figure 2: Office of the Executive Director (OED) - Organizational Chart



The OCIO employs a mix of full-time equivalent (FTE) employees and contractors to fulfill the agency's IT needs. Generally, FTE provide technical guidance and direction for the contractors who perform the bulk of IT activities. Currently, the OCIO is comprised of 41 FTE and 162 contractors; the majority of FTE (35 FTE, 85%) are Information Technology Specialists. The remaining six FTE employees are Management and Program Analysts (3 FTE), Librarians (2 FTE), and a Program Assistant. OCIO's FTE staffing level is at 89% authorized capacity; when fully staffed, OCIO would have 46 FTE. The FTC announced the hiring of a new CIO on July 7, 2015 – the fifth permanent (non-acting) CIO in 10 years.

The majority of OCIO staff is organized into seven branches based on the type of support they provide and functions they fulfill. An Assistant Director or Technical Director (GS-15) leads each branch:

- **Enterprise Architecture Branch** (1 FTE): Maintains the FTC's IT governance framework, manages enterprise data warehouse and business intelligence applications, and develops enterprise architecture and its related policies and standards.

- **Production Branch** (6 FTE): Provides video and media services as well as web content management and graphic design services for the Intranet and multiple external FTC websites.

- **Operations Assurance Branch** (6 FTE): Ensures the confidentiality, integrity, and availability of systems, networks, and data by establishing and maintaining the agency's Information Assurance Auditing and Monitoring Program and the Development and Acceptance Test Laboratories.

- **Infrastructure Branch** (10 FTE): Manages IT operational services and ensures the availability of the FTC's information assets and communication facilities.

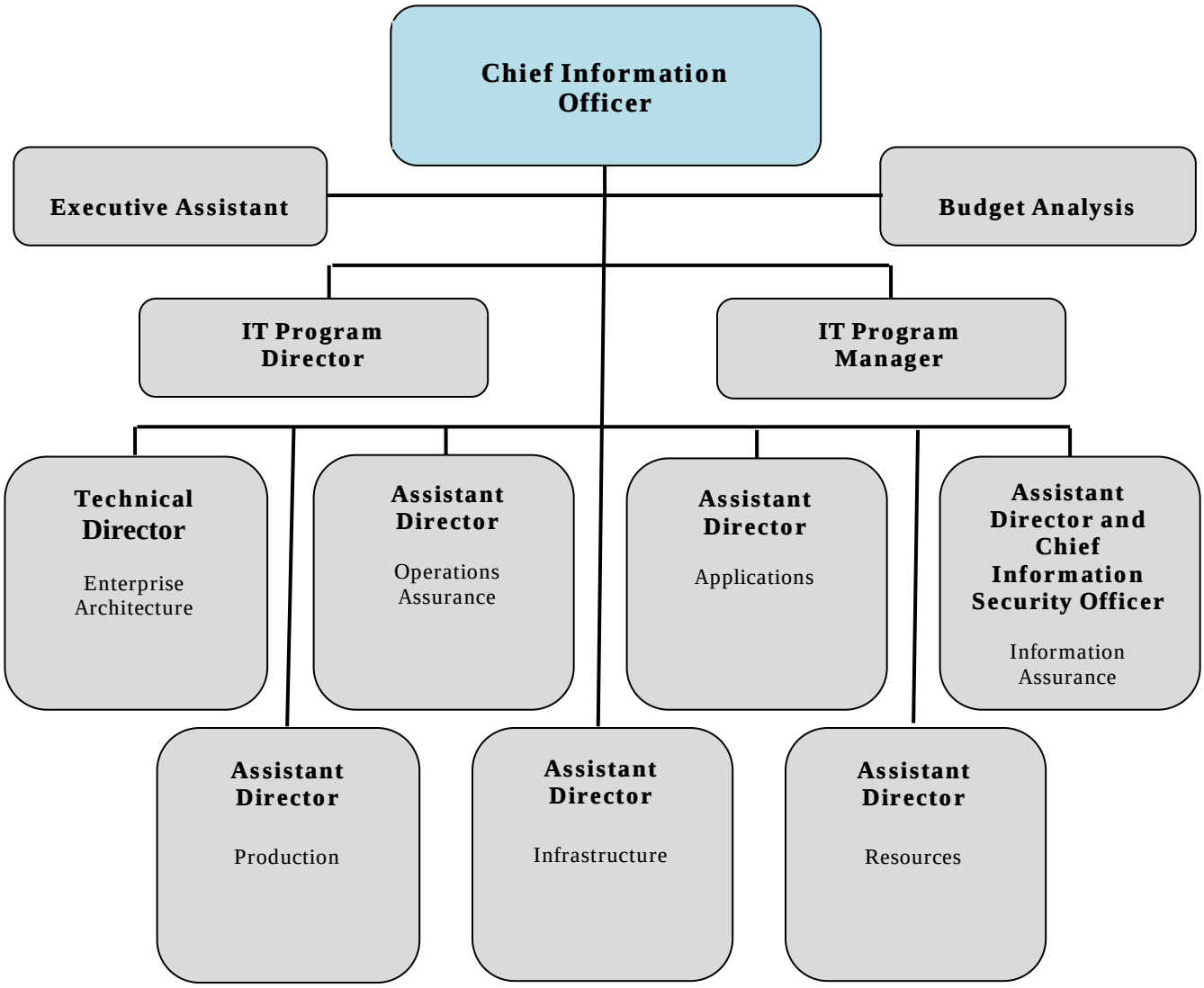
- **Applications Branch** (6 FTE): Plans/designs FTC applications or software-based solutions and requirements and ensures the integration of system components.

- **Resources Branch** (6 FTE): Manages OCIO's asset management program and manages and maintains the availability of FTC's library services including interlibrary loans, research requests, and research engine training.

- **Information Assurance Branch** (4 FTE): Manages the FTC's Federal Information Security Management Act (FISMA) process that protects the availability, confidentiality, and integrity of the FTC's information and information assets. The current Assistant Director of the Information Assurance Branch also serves as the FTC's Chief Information Security Officer (CISO).

In addition to the seven Technical or Assistant Directors, four other employees report directly to the CIO, including the IT Program Director, the IT Program Manager, the Management and Program Analyst who performs budget analysis, and the CIO's Executive Assistant. Figure 3, on the next page, shows the OCIO's organizational structure.

Figure 3: Office of the Chief Information Officer (OCIO) - Organizational Chart



2. The OCIO Mission and Key Stakeholders

The OCIO is responsible for "identifying and providing a host of critical high quality, low-risk IT services that are agile enough to meet Commission business needs."[12] The office is responsible for "providing the FTC with a robust, reliable, scalable, and interoperable infrastructure" and delivering services for both internal and external stakeholders.[13] The FTC's competition and consumer protection missions rely heavily on databases managed by the OCIO and its infrastructure, and on the agility and effectiveness of its IT investments.

[12] *Federal Trade Commission Strategic Plan 2014 to 2018*,16, *available at* https://www.ftc.gov/reports/2014-2018-strategic-plan.
[13] Federal Trade Commission, Congressional Budget Justification Book for FY 2015, 125, *available at* https://www.ftc.gov/system/files/documents/reports/fy-2015-congressional-budget-justification/2015-cbj.pdf.

Internally, the OCIO plays an important role in ensuring databases such as Concordance, Zylab, and the Hart-Scott-Rodino Premerger Notification System (PRS) are working effectively. All databases are essential to the FTC's mission: private entities use the PRS database to file information when seeking approval of mergers and acquisitions, whereas Concordance and Zylab enable FTC attorneys in the Consumer Protection and Competition Bureaus to store and manage large amounts of case data. The OCIO also is responsible for ensuring that FTC staff and external stakeholders can access other essential databases, some of which private contractors operate. Additionally, the OCIO aids FTC staff and external stakeholders in managing and analyzing external databases acquired in litigation.

3. The OCIO's Major Projects

The OCIO supports a diverse portfolio of projects and initiatives. The IT Governance Board (ITGB) tracks phases of select development modernization enhancement (DME) projects that have a five-year lifecycle cost exceeding $1 million, a high-impact on business processes, or a high risk of not completing execution or delivery. The IT Business Council (ITBC) reviews all DME projects, including those less than $1 million. (Operations and maintenance (O&M) or "steady state" projects are not reviewed or approved by any of the IT governance bodies.) In July 2015, the IT governance boards approved and/or tracked approximately 15 DME projects ranging in cost from approximately $57,000 to $8.8 million. The OCIO serves as the business and system owner for IT projects that support the FTC's internal processes. FTC Bureaus and Offices serve as the business owners for mission-focused IT projects. The OCIO may or may not serve as the system owner for mission-focused projects, but does serve as a technical consultant and monitors all IT projects to ensure compliance with information assurance, privacy, and IT acquisition requirements.

According to OCIO senior management, the OCIO's current priority projects include:

- **Secure Access for Employees (SAFE)** – SAFE is a remote access application that enables employees to access the agency's systems through a secure web-based portal. The OCIO is in the process of upgrading to SAFE2, which will offer employees a virtual desktop experience similar to their current office computer configuration and will improve functionality for MAC users. Additionally, the upgrades will lay the foundation for employees to access FTC's computing resources on mobile devices.

- **Network Stabilization** – The OCIO is upgrading the cabling and infrastructure supporting computer connectivity to provide employees with a more stable infrastructure and greater access to the Internet. Additionally, engineers are assessing traffic patterns to reduce the overall bandwidth consumption by identifying unwanted traffic and blocking it at the ISP.

- **Mobile Device Management (MDM)** – The OCIO has implemented a new mobile device platform, issued Smartphones to replace Blackberry devices, and provided additional options for Smartphone connectivity in areas where the carrier signal is weak or unavailable.

- **Zylab Implementation** – Zylab is a litigation support application that enables the Bureau of Competition (BC) and the Bureau of Consumer Protection (BCP) to store, process, and review millions of merger and other case documents. The OCIO is working to resolve functionality and processing (speed) issues associated with concurrent access by multiple users. The OCIO also is working to resolve performance delays associated with the legal review process, streamlining the validation process for upgrades, and revising the application architecture to ensure the application is available to meet user processing requirements.

- **Secure Investigations Lab (SIL) Process Automation** – The Bureau of Economics (BE) uses a discrete computing environment called SIL – which is separate from the FTC's production, development, and test environments – to house large volumes of personally identifiable information (PII) and sensitive health information (SHI). The BE analyzes this sensitive information to support FTC investigations, litigation, and studies. The OCIO is automating the process by which BE requests the movement of data from its production environment to the SIL. The OCIO also is investigating options for reducing the time required to conduct econometric analysis and help BE address "Big Data" challenges.

- **Identity Management** – The OCIO is implementing a solution to automate the network login process using two-factor authentication. The goal is to establish a standard authentication method that will be leveraged for all applications developed or upgraded in the future.

- **Patch Management** – The OCIO is evaluating risk mitigation strategies for installing security patches and upgrades to applications.

- **Service Management Improvement** – Remedy is the application the OCIO uses to assess service delivery by tracking client requests, problems, and assets. With the Remedy upgrade, the OCIO is implementing performance metrics, additional reporting, a configuration management system, and enhancing the Helpdesk services to facilitate a personalized user experience.

- **Audio Visual Modernization** – The OCIO is modernizing audiovisual equipment in the Constitution Center Conference Room, the Chairwoman's meeting room, and the Administrative Law Judge's Courtroom.

Results of the Review

1. A disconnect between authority and responsibility diminishes the CIO position

The Clinger-Cohen Act designates the CIO as the highest-ranking IT official within an organization and requires that the CIO report to the agency head on the progress made in improving information resources management capability.[14] Under the Clinger-Cohen Act, the CIO is responsible for 1) providing advice to the agency head and senior management on the acquisition and management of IT resources; 2) developing, maintaining, and facilitating implementation of sound and integrated IT architecture; and 3) promoting the effective and efficient design and operation of all major information resources management processes. In some federal agencies, the CIO reports directly to the agency head, while in other agencies, the CIO reports to the Deputy Secretary for Administration, the Chief Operating Officer, or an equivalent senior position.

Regardless of whether the CIO reports directly to the agency head or to another senior official, a major objective of the Clinger-Cohen Act is to ensure the CIO has a "seat at the table" with senior management and therefore is in a position to help drive overall strategy and align resources and priorities for the agency's information and IT investments. The current reporting structure at the FTC has the three Bureau heads and the Executive Director reporting directly to the Chairwoman, with the CIO reporting to the Executive Director. While the CIO has access to the Chairwoman and briefs her on IT security and strategic IT changes -- such as the risk management and modernization roadmap development processes -- the CIO reports to the Executive Director on all operational and infrastructure-related matters. As described below, when considered with the CIO's subordinate role on the FTC's IT Governance Boards, this reporting model diminishes the CIO's ability to advance the CIO's authority and hampers the ability of the CIO to execute the agency's information security and IT mission.

As figure 2 (pg. 8) illustrates, the OCIO is one of five offices managed by the Office of the Executive Director (OED). Like the OCIO, the other four offices – the Administrative Services Office, the Records and Filings Office, the Financial Management Office, and the Human Capital Management Office – provide services to all agency employees. Having the OED oversee customer support entities is logical, considering that the current Executive Director and Deputy Executive Directors possess deep institutional knowledge of FTC operations and customer expectations (with two of the three executives having worked in the Bureau of Consumer Protection (BCP) prior to their tenure in OED). Additionally, the Executive Director and both Deputy Executive Directors have acquired extensive knowledge of IT and operations, in the FTC, other federal agencies, and the private sector. While all offices under the OED's purview have mission-focused (information security) responsibilities as outlined under FISMA, the CIO is responsible for overseeing IT security and acquisitions for all FTC Bureaus and Offices. Securing the FTC's information and information systems poses many IT and management challenges and requires constant coordination and communication between the CIO and all agency stakeholders to ensure minimal disruption to operations, adequate protection for information resources and assets, and uncompromised mission success.

[14] 40 U.S.C. § 11315 (C)(3)(D).

The disconnect between the OCIO's authority and responsibility is also reflected in the CIO's subordinate role on the IT governance bodies. Established in FY 2011 and modified in FY 2014, the FTC's information technology governance program consists of three bodies that review and manage all agency IT investments for the duration of their lifecycle. The IT Council (ITC), chaired by the CIO, is comprised of Associate/Technical Directors in the OCIO, including the Chief Information Security Officer (CISO). The ITC serves as the point of contact with Bureaus/Offices on all proposed IT investments. ITC members work closely with each Bureau/Office to develop, support, conduct market research, assemble proposed IT portfolios and strategic modernization plans, and complete business cases for any high risk, high impact, or high dollar ($1 million or more) IT development, modernization, or enhancement projects for other governance bodies to review.

The IT Business Council (ITBC) is the "recommending body" to the IT Governance Board (ITGB). The ITBC conducts in-depth reviews of strategic plans and business cases for existing and proposed IT investment portfolios and makes recommendations to the ITGB. Reviews and oversight of each investment is commensurate with the investment's impact, complexity, and associated risks. The ITGB serves as the top-tier component of the FTC's IT governance structure. In that capacity, the ITGB provides high-level guidance on overall IT objectives and strategic priorities, approves the agency-wide IT portfolio, and reviews and makes significant IT investment selection and control decisions.

Figure 4, on the next page, lists the membership composition for both the ITBC and ITGB. The Executive Director chairs the ITGB, and the CIO co-chairs the ITBC. (The other ITBC co-chair serves in an 18-month rotating position.) While the CIO participates on the ITGB and the ITBC, and develops meeting agendas, the CIO does not have voting rights on either body. The CISO, who assesses and mitigates information security risk for the agency, is a member of IT Council. As such, the CISO performs risk analysis of potential investments and gives the other governance bodies risk explanations and alternative options to weigh in their discussions.

The CISO is not a permanent member of either the ITBC or the ITGB. However, the CISO does attend select meetings of both governing bodies when needed or requested. Voting decisions on both boards are based on a simple majority.

Figure 4: Composition of the IT Governance Board and the IT Business Council

IT GOVERNANCE BOARD (ITGB)	IT BUSINESS COUNCIL (ITBC)
Voting Members	***Voting Members***
Executive Director, Office of the Executive Director (Chair)	Bureau of Consumer Protection
Deputy Director, Bureau of Consumer Protection	Bureau of Competition
Deputy Director, Bureau of Competition	Bureau of Economics
Deputy Director, Bureau of Economics	Office of the Executive Director
Principal Deputy, Office of the General Counsel	Office of the General Counsel
	Office of Public Affairs
	Office of the Secretary
	Regional Offices
Non-Voting, Ex-Officio Members	***Non-Voting, Ex-Officio Members***
Chief Information Officer	Chief Information Officer (Co-Chair)
Chief Financial Officer	
Chief Privacy Officer	
IT Business Council's Chair	

With the establishment of the IT governance structure and bodies, the FTC is moving toward the principle of Enterprise Risk Management (ERM), a model adapted from an internal controls framework developed for the private sector in the early 1990s. ERM lifts the identification, assessment, and mitigation of financial internal controls and other risks to senior managers, who are looking across the entire enterprise, or in this case, the entire agency.[15] The responsibility for the security and use of information technology is decentralized among the FTC Bureaus and Offices. The governance boards are intended to provide a common structure for managing IT investments to minimize enterprise risks, improve sharing of best practices throughout the FTC, and provide improved, consistent monitoring of project performance. At present, however, a lack of voting rights for the CIO on the governance boards, together with the relatively subordinate position of the CIO within the agency, poses the risk that the CIO may not "have a seat at the table."

As explained to us in interviews with FTC staff, select FTC staff believe that the daily demands of the Bureaus for IT support and resources limit the CIO's ability to realize the agency's strategic IT priorities. Seeing itself as primarily a customer service organization, the OED takes customers' concerns and needs very seriously. Customers, particularly in the Bureaus, contact the Executive Director occasionally when the OCIO rejects a customer request or pushes back on a stated mission

[15] In June 2015, OMB provided initial ERM guidance to federal agencies about the first revision in ten years of OMB Circular A-123, *Management's Responsibility for Risk Management and Internal Control*. ERM principles are detailed in the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and 800-39, *Managing Information Security Risk.*

need, often creating an internal dynamic that yields to the influential Bureaus. OCIO employees commented that OED often supports the Bureaus' IT requests to the overall detriment of the agency and the consternation of OCIO employees. For example, an OCIO employee stated that a litigation support application's costs were escalating quickly. A TechStat -- an OMB accountability review tool designed to be applied to troubled IT investments -- was performed in July 2014 to address project concerns. The IT Governance Board (ITGB) Meeting Minutes for February 24, 2015 show that the ITGB was advised of the performance problems. The Executive Director (serving as ITGB Chair) directed presentation of a subsequent TechStat, which is now scheduled for October 2015. However, the ITGB continued to approve increased funding before completion of the requested TechStat because the project is a high priority for the Bureaus. Similarly, in our FY 2014 FISMA evaluation, the OIG reported that the OCIO does not provide specific direction or guidance regarding the development of cost estimates for IT investments, but instead relies on cost estimates for similar investments and staff judgment. The lack of estimating guidance leads to unreliable estimates with limited value in controlling project costs.

By not having adequate authority within the FTC organizational structure, the CIO is not sufficiently empowered to weigh a Bureau's request against other mission or cost considerations or to stop or modify an IT investment. OCIO employees told us they have adapted to this dynamic in three ways. First, to counter the Bureaus' stated needs, they leverage the position and influence of the Chief Privacy Officer (CPO), who reports directly to the Chairwoman. Second, OCIO employees sometimes limit the amount of information they share with OED management to avoid negative repercussions. Third, OCIO employees tend to "overpromise" the Bureaus and other customers, adding more projects to their portfolio, fearing that resisting or delaying their requests is not an option. OCIO employees acknowledge, however, that by yielding to the Bureaus or other customers and then not delivering on their promises, they damage the OCIO's credibility and reputation – and risk falling short of meeting expectations for the mission.

Exacerbating this dynamic, the OCIO often finds itself unable to deliver on projects as quickly as customers would like because it is under-resourced. OCIO employees and agency stakeholders told us that the OCIO is understaffed and does not have the skilled FTE with the necessary project management and communication skills to properly oversee contractors and effectively collaborate with the work force. However, other interviewees stated that many OCIO employees underperform, leaving a select and small group of OCIO employees to perform the majority of work – even work outside their branch's assigned area of responsibility. In the absence of a current core competency and skills assessment, the new CIO cannot be sure his staff is right-sized and right-skilled to execute the OCIO's core mission.

By not having the authority to push back, set boundaries, or help the FTC realize strategic IT priorities for the agency, the FTC risks having the CIO serve as a de facto Director of IT Operations, a position that lacks the authority envisioned for CIOs in the Clinger-Cohen Act. As a consequence, the CIO is not adequately and strategically weighing the costs and risks associated with IT investments on an enterprise level. We provided specific examples of this in our Fiscal Year 2014 FISMA evaluation, which reported that the FTC is not producing full life cycle cost estimates associated with IT investments.[16]

[16] FTC OIG FISMA 2014 Summary Report, *available at* https://www.ftc.gov/system/files/documents/reports/fisma-2014-summary-report/150526fismareport.pdf. The GAO has recognized this phenomenon in a recent report where it found that the Library of Congress lacked strong leadership to address its IT weaknesses because its "CIO does not have adequate responsibility for the agency's IT – in particular, authority over commodity IT and oversight of investments in mission-specific systems made by other service units." GAO Report 15-315, *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses* 94-

The prominence and importance of the leading information security position at the FTC – the Chief Information Security Officer (CISO) – also is not reflected in the OCIO organizational structure. Tasked with ensuring the FTC's compliance with FISMA and guaranteeing the security of systems internal and external to the agency, the CISO is one of eleven OCIO employees who report directly to the CIO. With so many employees reporting directly to the CIO, we found that the importance of the CISO position is not in line with best practices in the federal government, which is to elevate the CISO above that of IT branch chiefs.

To inform our study, we reviewed how other federal agencies position and empower their CIOs and position their CISOs. The Federal Deposit Insurance Corporation (FDIC) elevated its CIO position in 2013, when the IT unit underwent a re-organization. The main restructuring changes included separating the roles of the CIO and the Director of IT. The CIO, who formerly reported to the FDIC's Chief Financial Officer, now reports to the agency head. The CIO meets with the agency head biweekly to discuss business items and meets more routinely to discuss such matters as system development projects and security issues. The FDIC CIO co-chairs, and possesses voting rights on, the FDIC's Capital Investment Review Committee (CIRC), which reviews and oversees all major IT and non-IT capital investments with life-cycle cost estimates exceeding $3 million. The Director of IT and the Chief Information Security Officer (CISO) now directly report to the CIO. The CISO position was elevated during the restructure to make the position two levels down from the agency head. The CISO's role is more significant and demanding, with the high volume of data digitization in recent years, and therefore, the FDIC thought it important to reflect its prominence in its reporting structure.

The CIO at the Securities and Exchange Commission (SEC) reports directly to the agency head on IT strategic alignment with agency-wide mission-related goals and privacy breaches; cybersecurity; and rulemaking impacts. The CIO reports to the Chief Operating Officer (COO) for IT budget, personnel decisions, and day-to-day operations. The SEC CIO told us that the CIO should be a business partner who addresses high-level business strategy with the other agency heads and therefore cannot be "an operations person." At the SEC, the CISO reports directly to the CIO. The SEC CIO remarked that it vital to elevate the CISO position above most IT management since the CISO's job is to tell employees they cannot do something.

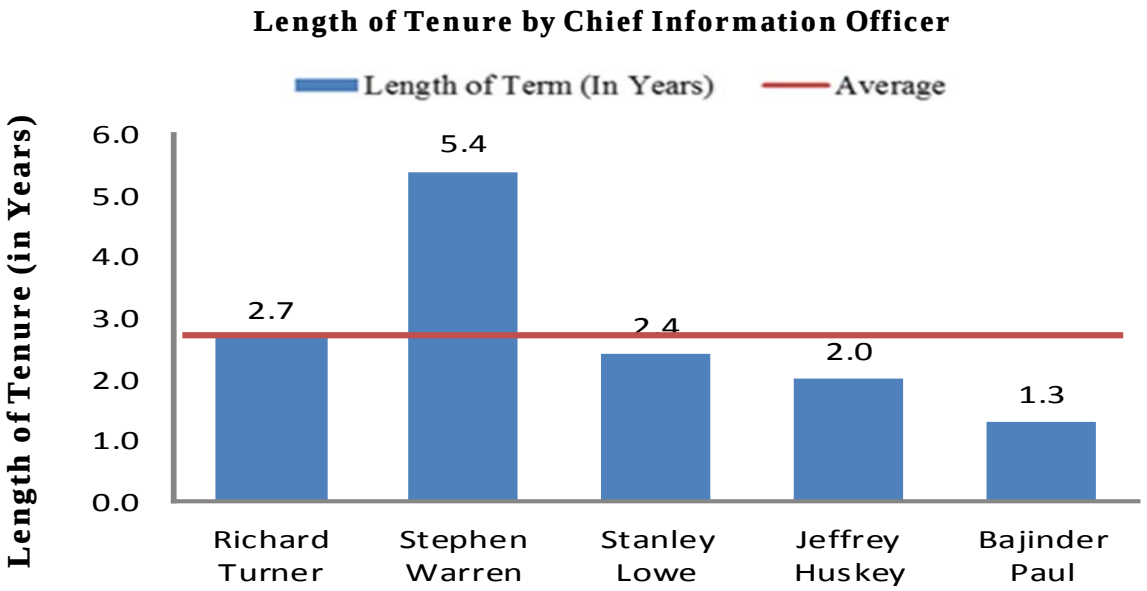
2. High turnover in the CIO position hampers short-term and long-term planning efforts

In a September 2011 report, GAO stated that major IT initiatives in both the public and private sectors may take 5 to 7 years to achieve buy-in and fully implement.[17] Since 2000, the FTC has had five permanent CIOs who served an average tenure of 2.8 years or 34 months (Figure 5, on the next page). For the periods of transition in between sitting CIOs, seven FTC employees have served as temporary Acting CIO, for a combined average total of 2.86 years. While the average tenure of permanent CIOs at the FTC is slightly greater than the median tenure of 25 months for CIOs across the federal government, the FTC needs to address and overcome this challenge in order to have effective long-range IT success.

95 (March 2015). As noted above, the Clinger-Cohen Act authorizes CIOs to be accountable for IT investments, including IT acquisitions, monitoring the performance of IT programs, and advising the agency head whether to continue, modify, or terminate such programs.

[17] GAO Report 11-634, *Opportunities Exist to Improve Role in Information Technology Management* 27 (September 2011).

Figure 5: Tenure of FTC Chief Information Officers, 2000-Present



For the past decade, OCIO employees have lacked consistent direction and clear focus, with each CIO having his own agenda. Planning and modernization efforts have been sidelined, and both OCIO personnel and stakeholders have had to adjust to each new permanent and temporary CIO instituting new policy and procedural changes for many aspects of IT management. Agency officials told us that the OCIO's lack of stable leadership generates more work for their respective Bureaus, particularly when it comes to learning and adapting to the changes each new CIO introduces. The OCIO needs to mature its IT governance structure, create an IT strategic plan, and incorporate other measures to compensate for the short tenure of CIOs. The OCIO, and the agency at large, will be better positioned to accommodate such turnovers if, in addition to those improvements: 1) action is taken to ensure that OCIO is right-sized and properly skilled; 2) leadership immediately below the CIO is strengthened; and 3) staff is properly trained and held accountable for accurately assessing the resources and time to implement new technology.

Strategic Planning

While agency-wide strategic planning efforts are in line with prescribed legislation and other mandates, the OCIO has not performed IT strategic planning in recent years that incorporates recommended guideposts. The Government Performance and Results Act (GPRA) of 1993 and the GPRA Modernization Act (GPRAMA) of 2010 mandate that federal agencies issue and publish agency-wide strategic plans with specific parameters, including concrete timeframes, timelines, and other components. Likewise, OMB Circular A-11 provides requirements for agency strategic plans and details how federal agencies and agency components can use and align their agency-wide strategic plan

to their human capital resources and information technologies to achieve cost-effectiveness and better outcomes.[18]

OMB Circular A-130 establishes the overarching policy for managing federal information resources, including both security and privacy. Circular A-130 reiterates that information resource strategic plans should support the agency strategic plan described in Circular A-11, as well as provide a description of how information resources will assist agency stakeholders in accomplishing and furthering the agency's mission. Circular A-130 stresses the importance of integrating and aligning information resources with all aspects of agency-wide planning efforts, including budgeting, acquisition and procurement, financial and resource management, and program decisions.

In two recent reports, the GAO highlighted the importance of an IT strategic plan in serving as an agency's IT vision and road map and aligning an agency's information resources with its business strategies and investment decisions.[19] Key elements of the IT strategic planning process include creating an IT strategic plan and an enterprise architecture, as well as sound human capital planning to equip IT employees with the necessary skills to accomplish IT priorities and agency goals.[20] According to the GAO, the necessary components of an IT strategic plan include:

- Alignment with the agency-wide strategic plan;
- Results-oriented goals and performance measures that stakeholders can use to assess and gauge success;
- Strategies the IT unit will use to achieve desirable or intended outcomes; and
- Descriptions of interdependencies within and across projects.

The OCIO participated in the FTC's most recent strategic planning process that culminated in the Quadrennial Strategic Plan for FY 2014 to FY 2018. Information technology and security, like most key management areas at the FTC, aligns with the FTC Strategic Plan under Goal 3, "Advance Organizational Performance." Specifically, the OCIO aligns to the FTC Strategic Plan under Objective 3.1, "Optimize Resource Management and Infrastructure." The OCIO is responsible for reporting to the Financial Management Office monthly progress towards accomplishing performance measure 3.1.2, "Availability of Information Technology Systems."

While the FTC has a Quadrennial Strategic Plan, the OCIO's most current strategic planning effort is reflected in a DRAFT IT Strategic Plan for FY 2012 to FY 2014. The former CIO and the OCIO staff attempted to create a high-level modernization roadmap that would allow the OCIO to better understand the FTC's Bureaus and Offices needs and to schedule and manage IT projects in partnership with them. The OCIO briefed the modernization roadmap development process to the Chairwoman and conducted interviews with agency stakeholders to solicit their requirements. However, due to personnel changes and other factors, the modernization process was curtailed before an official roadmap or strategy was produced. Consequentially, the OCIO's priorities and objectives do not align to the agency's enterprise-level priorities but rather to the goal of maintaining and enhancing the existing infrastructure.

[18] OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*, § 230-2 (June 2015).
[19] GAO Report 12-495, *Social Security Administration: Improved Planning and Performance Measures Are Needed to Help Ensure Successful Technology Modernization* 37-38 (April 2012).
[20] GAO Report 15-315, *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses* 21 (March 2015).

We note that at the FTC (and other federal agencies), enterprise-level strategic planning is made more challenging because, for the last several years, the OCIO has depended upon unfunded requirements (UFRs) to fund base operations. Long-term IT planning is difficult but required for normal FTC operations. When an IT unit's base budget cannot fund its current/normal operations and must rely on unfunded requirements (UFRs), funds must be transferred from other projects. The absence of enterprise-level strategic planning aligned with business priorities and IT investment planning leaves the FTC more vulnerable to increased costs, risks associated with continued use of outdated technologies, duplication of effort, poor or degraded performance of its IT systems, and potential data breaches and cyberattacks.

In the absence of an IT strategic plan, the CIO and OCIO managers communicate projects and priorities to OCIO staff during informal discussions and staff meetings. Also, OCIO dashboards list priority OCIO projects and track their completion status, variances, and risks. However, Bureau officials told us that while they know what the agency's big IT projects are, they do not know the order of project prioritization or project status. Interviewees also commented that IT planning efforts – including strategic planning, modernization, enterprise architecture, and contingency planning – are impeded due to high turnover in the CIO position, constantly having to "put out fires," and not having the resources or the necessary agency endorsement. In terms of resources, the OCIO has two positions – the Technical Director of Enterprise Architecture and the IT Program Manager – whose focus is to perform IT enterprise and strategic/modernization planning, respectively. Since neither of these individuals has support staff, and each assists with execution of many of the OCIO's ongoing projects, they devote little time or resources to IT strategic planning.

Benchmarked agencies perform strategic planning and involve their agency's business units to varying degrees. Like the OCIO, the Securities and Exchange Commission's Office of Information Technology (SEC/OIT) does not have a current IT strategic plan, but is in the process of building a one- to two-year technology roadmap. The Equal Employment Opportunity Commission's Office of Information Technology (EEOC/OIT) is in the process of creating a five-year IT strategic plan that is very business driven, with focus on both the EEOC/OIT's enforcement and litigation visions.

The Federal Deposit Insurance Corporation's Division of Information Technology (FDIC/DIT) has an Enterprise Technology Branch devoted to continuously performing strategic planning. FDIC/DIT periodically issues planning documents, including a strategic plan, every three to five years. According to FDIC/DIT leadership, the extent of strategic planning performed depends on the maturity of an organization. When creating its last IT strategic plan, FDIC/DIT separated its IT work by competency and asked its employees and customers to rate and describe each competency's level of service. FDIC/DIT then analyzed the responses to identify whether problems stemmed from people, business processes, or technology, and worked on resolving the root causes of the problems. FDIC/DIT personnel asked its customers where they saw their divisions heading in the next three to five years, and how they saw FDIC/DIT helping them achieve those goals.

Agency Participation in IT Planning

Bureau interviewees told us that they would like to be more heavily involved in the IT planning process on a more regular basis. Some acknowledged that their role in planning might expand with the maturation of the OCIO's IT governance boards. Specifically, Bureaus would like the OCIO to solicit agency input before the OCIO embarks on significant or long-term planning effort or before they deploy final products. Involving stakeholders in planning processes and listening to their suggestions will help ensure systems fit the culture and mission needs of the FTC and its respective Bureaus/Offices.

Numerous interviewees told us that their Bureaus appreciated the OCIO involving them in the mobile phone pilot program in the fall of 2014. However, while the OCIO solicited input about the pilot program from participants, it did not address or fix the concerns participants raised prior to the full-scale deployment of smartphones. Had they done so, problems that the pilot participants experienced could have been avoided but, instead, were aggravated by agency-wide deployment. For example, agency stakeholders said they were unable to access Wi-Fi networks at work or at home or to access shared network drives on their mobile phones because of security certificate issues.[21] Consequentially, agency employees were not able to fully work remotely (e.g., share documents with one another, cut and paste documents in emails) using solely their mobile phones. As a result, emails agency employees sent to one another using their mobile phones were often delayed in both sending and receiving, or not received sequentially, causing confusion and miscommunication. The OCIO is still resolving these and other issues surrounding the $1.15 million mobile device management/replacement initiative.

Bureau employees also observed that it would be helpful if the Bureaus periodically reviewed and discussed their future needs with the OCIO, along with internal factors that affect their Bureaus, to ensure the OCIO develops a more useful and sustainable solution or product. Bureau employees also voiced interest in helping the OCIO conduct contingency planning to mitigate problems or obstacles that may occur. Minutes from the February 2015 and March 2015 ITGB meetings show that the governance boards are beginning to integrate basic risk planning and risk management principles into their allocation decisions. With the expected evolution of the IT governance bodies, risk planning should become more comprehensive and routine, leading to more effective integration of Bureau and agency-wide needs over time.

3. Lack of clear delineation and understanding of OCIO employees' roles and responsibilities creates confusion and limits accountability

Confusion over Position Clarity and Position Descriptions

As the OCIO's current organizational structure illustrates, 11 positions report directly to the CIO, including the seven Technical/Assistant Directors, the IT Program Manager, the IT Program Director, the Management and Program Analyst performing Budget Analysis, and the Executive Assistant. While functional responsibility statements outline the functions that each of the seven OCIO branches perform, our review identified confusion among both OCIO employees and agency officials as to what responsibilities select OCIO employees and branches are assigned and why. Part of this uncertainty

[21] The FTC used a certificate-based security approach to restrict phone access. Using this approach, digital certificates are installed on each phone for each network where access is allowed. Network access is prohibited if the certificate is not present or does not correspond to the network certificate.

stems from what interviewees called a "lack of resources" such that OCIO is "stretched so thin their roles morph" and consequently OCIO employees do not have time to do their assigned (full-time) jobs and cannot provide the customer with the "full or ultimate experience."

We found that this uncertainty stems in part from a lack of positional clarity. Agency stakeholders said they were unsure what roles the IT Program Director and the IT Program Manager have within the OCIO, and the differences in roles and responsibility associated with these two positions. Other interviewees expressed confusion as to where one branch's responsibilities end (e.g., Infrastructure Branch) and another branch's (e.g., Application Branch) responsibilities begin. For instance, the Operations Assurance Branch, which is responsible for ensuring data systems' integrity and availability, oversaw the mobile device management initiative, a project heavily dependent on infrastructure. OCIO customers noted that blurring roles of OCIO employees and branches often leaves them wondering whom they should call in the OCIO when they need a particular issue resolved or assistance with a specific matter.

Complicating this problem, OCIO employees' official position descriptions (PDs) fail to provide clarity as to the nature of work performed by each employee. In addition, we identified numerous discrepancies in the position descriptions for current OCIO employees, including:

- The Assistant Directors of Operations Assurance and Infrastructure both had the title of "Deputy CIO for Management" in their PDs;
- The Assistant Director of Resources had the title "Assistant CIO for the Project Management Office" on her PD;
- The Technical Director of Enterprise Architecture was listed as having a non-supervisory position on her PD even though the employee was required to rate two subordinates;
- Two GS-13 OCIO employees had their grade levels listed as GS-14 on their PDs;
- The Human Resource Specialist signed and dated approximately one dozen employee PDs years before the employee matriculated into either OCIO or the FTC; and
- Someone had handwritten OCIO employees' names on more than a dozen PDs.

Without clear delineation of duties, employee accountability is difficult to enforce. Indeed, OCIO employees and agency stakeholders noted a perception that poorly performing OCIO employees are not disciplined, diminishing the higher performers' contributions and lowering morale. These interviewees noted that management rewards – or burdens – the higher-performing, "technically-minded" OCIO staff with more work sometimes outside the purview of their branch's responsibilities.

While OED periodically conducts a survey to collect feedback from agency stakeholders regarding the performance of the five offices under its purview, no survey questions addressed employee accountability or morale.[22]

[22] OED periodically conducts and distributes surveys to FTC Offices and Bureaus to assess the performance of the five customer service offices under its purview. However, OED's survey does not address accountability and morale challenges. Additionally, although the Office of Personnel Management (OPM) conducts an annual Federal Employee Viewpoint Survey (EVS), survey responses submitted by OCIO employees are not available for 2014 or preceding years because OED results were not disaggregated by its five customer service offices.

Current Organizational Structure

Lack of role clarity also stems from the OCIO operating under an antiquated organizational structure. As numerous OCIO employees noted, the current organizational structure encourages silos and does not promote matrixed management or collaboration between branches. For example, interviewees told us that the Technical/Assistant Directors do not communicate effectively with one another and their respective branches, often withholding critical information necessary to perform their duties. During the mobile device deployment in 2014, for example, OCIO employees told us that the Constitution Center, which houses many Bureau staff, had wireless "dead zones" (i.e., no wireless signal in select areas), but this information was not shared with the team tasked with deploying the full-scale deployment of new mobile phones. As a result, employees who worked in wireless dead zones were unable to regularly send or receive work emails or access the Intranet or Internet on their mobile phones. This example not only illustrates the failure of individuals within OCIO to communicate, but also shows a failure of organizational processes to capture and share performance-based requirements and IT acquisition best practices.

The OCIO's current organizational structure also fails to meet a host of other organizational and agency needs. First, the OCIO currently lacks a central planning unit or individual responsible for coordinating all planning endeavors. (The IT Program Manager position holds broad planning responsibilities, but the position is currently vacant.) Though the IT Governance Board should, with maturation, make planning decisions when it approves proposed IT investments for the agency, the OCIO needs to assign responsibility for performing strategic IT planning for the entire agency.

Second, the OCIO lacks a research and development capability. The Securities and Exchange Commission's Office of Information Technology (SEC/OIT) and the Federal Deposit Insurance Corporation's Division of Technology (FDIC/DIT) have separate research and development branches tasked with this purpose. The FDIC/DIT's Enterprise Technology Branch focuses on the short-term and long-term goals of FDIC's business units and the technology needed to achieve their goals, and analyzes technology and industry trends to identify opportunities for technological innovation and program improvements. Likewise, the SEC/OIT's Business Solutions Engineering Branch serves as the organization's primary research and development group that is singularly focused on researching and prototyping new and emerging technologies in support of SEC's business and IT needs and requirements.

To fulfill the FTC's strategic plan, the OCIO must keep abreast of the rapid pace of technological development to learn how emerging technology can support the agency's changing needs. While the FTC may not have the resources to support an in-house research and development unit or dedicated staff member, it can and should identify and adapt the best practices of comparable organizations to assign responsibility to support the CIO's strategic planning and vision.

Third, numerous interviewees identified opportunities to improve the OCIO's marketing and outreach activities to better understand the Bureaus' and Offices' business needs and to include them in the front end of gathering requirements for projects. While OCIO employees interact regularly with Bureaus and Offices on major IT projects, stakeholders wish to have their input solicited on smaller-scale projects as well, including such efforts as the agency's printer replacement selection.

As the governance process matures at the FTC, agency stakeholders should experience greater participation in all IT-related planning processes. In so doing, the OCIO can better measure and evaluate its performance and improve customer relations by developing, collecting, and reporting user-

focused metrics. User-focused metrics demonstrate OCIO performance that non-technical customers can readily understand and appreciate (e.g., time to resolve a reported problem and number of support requests resolved on the first call). Establishing and tracking such metrics will provide the agency with objective criteria to evaluate the OCIO's contribution to the agency's mission.[23] The CIO is leading this promising effort.

4. Poor contract management compromises the OCIO's mission

Based on interviews of OCIO managers, agency stakeholders, and the results of other OIG reviews, a top OCIO challenge is contract management. Many agency stakeholders told us that they had personally experienced adverse ramifications from poor requirements gathering, drafting, and oversight of IT contracts by OCIO personnel.

At the FTC, OCIO personnel collect requirements and also draft and oversee contracts involving IT products (e.g., mobile phones) and services (infrastructure operations and maintenance, external hosting of websites) provided by third party vendors. Depending on the dollar amount and scope of the contract, at least one OCIO employee serves as the Contracting Officer's Representative (COR), and other OCIO employees or employees from the end user's Bureau or Office may serve as Assistant COR(s) (ACOR). Prior to contract solicitation, the OCIO COR works with the end user and a contracting officer (CO) from the FTC Acquisition Branch to capture requirements and then monitor terms of the contract to ensure contractor compliance. The COR also works closely with Acquisition Branch staff to modify terms of the contract, if warranted.

Performance-based acquisition is the preferred method for acquiring services within the Federal government (Public Law 106-398, section 821). Federal contract administration is governed by the Federal Acquisition Regulations (FAR). FAR Subpart 37.6 provides the policies and procedures for performance-based acquisitions. Using a performance-based approach, agencies describe the results to be achieved or the deliverables to be provided, as opposed to specifying the procedures to be used (i.e., what is to be accomplished as opposed to how much activity is accomplished). FAR Subsection 37.601(b) requires that:

> Performance-based contracts for services shall include – (1) A performance work statement (PWS); (2) Measurable performance standards (i.e., in terms of quality, timeliness and quantity, etc.) and the method of assessing contractor performance against performance standards; and (3) Performance incentives where appropriate.

The FAR mandate that performance standards establish the performance level required by the government to meet the contract requirements. The FAR also require that performance standards be measurable and structured to permit an assessment of the contractor's performance.[24] As stated in the FTC's Administrative Manual, the Acquisition Branch is to assist the FTC Bureaus/Offices in developing full technical specifications, including performance-based specifications, when drafting contract requirements.[25]

[23] FTC OIG FISMA FY2014 Summary Report, *available at* https://www.ftc.gov/system/files/documents/reports/fisma-2014-summary-report/150526fismareport.pdf.
[24] FAR Section 37.603(a).
[25] FTC Administrative Manual, Section 300.

Contract Requirements and Drafting

The majority of complaints stakeholders voiced during our review concerned poorly written contract documents on the part of the OCIO. A few distinct issues emerged. First, end users stated that the OCIO did not correctly capture their requirements in initial contract solicitations. Second, end users did not anticipate how their future needs may change, and consequentially, end users' initial needs expanded beyond the initially defined contract boundaries. Third, IT contracts often did not specify proper performance metrics or state how goals were to be measured. The OIG's FY 2014 FISMA evaluation report identifies contractor performance and user-centric system monitoring measures as essential for successful evolution of the FTC information assurance and privacy programs.

These recurring problems reveal fundamental weaknesses in the performance of the Acquisition Branch, and, on a larger scale, an inability to execute one of the CIO's core missions. Without a competent contract management staff who are well trained and experienced in developing user-based metrics and effectively administering contracts, the OCIO risks losing money on underperforming contracts, unnecessary contract modifications, and poorly written contracts that do not capture or deliver on the users' or mission's intended needs.

Through effective performance management and complementary contractor support where needed, the FTC has begun to address these weaknesses. OCIO's government personnel must have stronger technical writing skills, effectively collect and document end user requirements, establish and track performance metrics, and plan for contingencies.[26]

Contract Oversight

FTC oversight of IT contracts is also a significant and ongoing challenge. COR duties in the FTC are "collateral duties," meaning that CORs are expected to perform their regular responsibilities – such as issuing cryptographic Secure Sockets Layer certificates for the agency – in addition to servicing contracts. Currently, 20 OCIO employees (or approximately 50% of the OCIO FTE workforce) serve as a Level 1, 2, or 3 COR on IT contracts. Most of these CORs oversee multiple contracts, with one employee serving as a COR on 15 separate contracts. With staff spread thin, few CORs have adequate time, training (e.g., project/contract management, technical writing), knowledge of the FAR, or subject matter expertise of the contract they are overseeing to effectively monitor contract details. As one interviewee noted, vendors are given leeway "to do what they want or think they need to do." Moreover, our review of OCIO managers' position descriptions show that these managers are not clearly or uniformly assigned responsibility for overseeing COR performance. Additionally, the FTC's Acquisition Branch has experienced high turnover within the past year, resulting in a lack of continuity in contract management or oversight. Each new contracting officer oversees contracts differently and views the role of the COR differently, causing added confusion.

[26] The SEC/OIT is on a similar path, taking steps to improve the fundamentals of contract management. The SEC/OIT has historically experienced challenges identifying technical requirements for its business customers and drafting contracts at fiscal year close when IT employees hurriedly submit contracts to the SEC's Acquisitions Office for approval. To remedy this shortfall, the SEC/OIT is partnering with the agency's Office of Acquisition to establish a "Requirements Center of Excellence" within its Solution's Branch. The objective of the Requirements Center of Excellence is to help ensure project requirements are clearly defined and that all infrastructure standards and security requirements are considered prior to contract solicitation. While the FTC is not resourced to create such a unit, the CIO is identifying other ways to strengthen its requirement collection and writing process.

It is a common practice across the federal government for IT employees to serve in collateral duty COR positions – including at both the EEOC/OIT and FDIC/DIT. The vast majority of the SEC/OIT's CORs serve in collateral duty positions, too, except for three of its CORs whose sole job is to manage the agency's large infrastructure contract and its approximately 250 contractors. However, unlike in FTC OCIO, CORs in benchmarked agencies are assigned contracts based on the complexity of the contract as well as the technical expertise involved. For example, for simple IT maintenance or licensing contracts, a COR at benchmarked agencies may be assigned 10 contracts, but generally manage only one complex contract. Similarly, FDIC/DIT assigns at least one oversight manager (the FTC equivalent of a COR) and multiple technical monitors to oversee complex contracts. Technical monitors provide the first line of review to ensure the soundness of contractors' work. The oversight manager provides administrative supervision. Both the oversight manager and technical monitors are required to complete internal certification training that is based on the complexity of contracts they are responsible for and have some degree of competency in the contract subject matter being performed so they can intervene if warranted.

Taken together, we found that the OCIO's shortcomings in requirements documentation, contract drafting, and contractor oversight result in increased risk for poorly performing contractors and vendors, undelivered or delayed capabilities and functionality, protracted litigation, and, ultimately, in challenges for mission success. While FTC management continues to implement OIG FISMA recommendations to improve contract management and to adopt acquisition best practices captured in GAO guidance, opportunities exist to accelerate these efforts. FTC leadership should do so.[27]

[27] GAO Report 15-371T, *GAO's 2015 High-Risk Series: An Update* 5 (February 2015).

Recommendations

The new CIO's arrival in July 2015 provides an opportunity for the FTC to address long-standing challenges in serving the OCIO's customers and stakeholders to advance the agency's competition and consumer protection mission.

The OIG makes the following recommendations to address the OIG's major findings from this evaluation:

To afford the CIO authority commensurate with the intent of the Clinger-Cohen Act, best practices among federal agencies, and to position the CIO to help accomplish the FTC's strategic goals for information security and information technology:

1. Extend voting rights to the Chief Information Officer on the FTC IT Governance Board and the IT Business Council (The Executive Director).

To improve the OCIO's support for the FTC's core mission and align the agency's IT investments to the needs of customers and stakeholders:

2. Identify the current OCIO core competencies and determine how they align with stakeholder needs, and identify performance shortfalls and gaps and their root causes (e.g., personnel, policy, business processes, resources, or technology), within 120 days (CIO).

3. Using the data developed through the core competency assessment (recommendation 2), the FTC's Quadrennial Strategic Plan, and other agency priorities and initiatives, develop an IT Strategic Plan. The IT Strategic Plan should establish goals and objectives to serve both a) internal customers (operations and infrastructure) and b) external stakeholders (including federal partners, litigants, contractors, and consumers) that incorporate principles of enterprise risk management, performance-based metrics, and change management, within 120 days following completion of the core competency assessment (recommendation 2) (CIO).

4. Assign ongoing responsibility to staff for conducting a) strategic planning, b) enterprise architecture planning that accommodates the Federal Enterprise Architecture relevant to the FTC mission, c) prototypes of emerging technology activities, and d) agency IT acquisition strategy to help anticipate and plan for the agency's future IT and information security requirements, within 90 days (CIO).

To better clarify the roles and responsibilities of OCIO staff and communicate them effectively to the FTC workforce:

5. Update all OCIO employees' position descriptions to delineate current job descriptions, correct grade and promotion potential, and supervisory status; ensure position descriptions for OCIO managers include review of Contracting Officer's Representative (COR) performance in collecting and drafting contract requirements and monitoring contractor performance, within 120 days (CIO and HCMO).

To strengthen contract management and project management execution and oversight:

6. Using established OMB, FAR, Federal Acquisition Institute, and other guidance, and in coordination with the development of the IT Strategic Plan (recommendation 3), develop an acquisition strategy that reduces the complexity of current procurements and increases stakeholder visibility into contractor performance, within 240 days (CIO).

7. Publish IT services that align with stakeholder requirements and the Quadrennial FTC Strategic Plan, service levels, and corresponding levels of resources required to provide these service levels, and post this data on the FTC Intranet, within 180 days (CIO).

8. Using the core competency assessment (recommendation 2) and published IT services (recommendation 7), and in coordination with the development of the IT Strategic Plan (recommendation 3), develop a recruitment, hiring, and training plan to acquire and sustain personnel needed for improved contract management, program management, and oversight within OCIO and in the FTC's Bureaus and Offices, and for IT service delivery across the FTC, within 300 days (CIO).

While our report identifies challenges in the positioning of the CIO and the CISO within the FTC organizational structure, we are not at this time recommending organizational changes. We believe the new CIO should have the opportunity to assess these and other organizational challenges as he acquaints himself with the agency's mission, strategies, and priorities, participates in IT governance activities, and contributes to their planned maturation.

Appendix A Acronyms and Abbreviations

ACOR	Assistant Contract Officer's Representative
BC	Bureau of Competition
BCP	Bureau of Consumer Protection
BE	Bureau of Economics
CISO	Chief Information Security Officer
CM	Configuration Management
COR	Contract Officer's Representative
CPIC	Capital Planning and Investment Control
EEOC	U.S. Equal Employment Opportunity Commission
ERM	Enterprise Risk Management
FAR	Federal Acquisitions Regulation
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Management Act of 2002
FITARA	Federal IT Acquisition Reform Act
FMO	Financial Management Office
FTC	Federal Trade Commission
FY	Fiscal Year
GAO	Government Accountability Office
GPRA	Government Performance and Results Act
GPRAMA	GPRA Modernization Act
GSS	General Support System
HCMO	FTC Human Capital Management Office
ISCM	Information Security Continuous Monitoring
ITBC	IT Business Council
ITGB	IT Governance Board
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	FTC Office of the Chief Information Officer
OED	FTC Office of the Executive Director
OIG	Office of Inspector General
OMB	Office of Management and Budget
PRS	Premerger Notification System
SEC	U.S. Securities and Exchange Commission
SSP	System Security Plans

Appendix B Management Response to OIG Evaluation of the FTC Office of the Chief Information Officer

Office of the CIO
Chief Information Officer
Raghav Vajjhala

UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION

WASHINGTON, D.C. 20580

TO: Roslyn A. Mazer
Inspector General

FROM: Raghav Vajjhala RV
Chief Information Officer

DATE: December 16, 2015

SUBJECT: Management Response to OIG Evaluation of the FTC Office of the Chief Information Officer

This memorandum provides management's consolidated response to the OIG's recommendations resulting from its evaluation of the Office of the Chief Information Officer's resources.

We appreciate the Evaluation by the Office of the Inspector General (IG) of the Office of the Chief Information Officer (OCIO) of the Federal Trade Commission (FTC), and the opportunity to provide a response to the evaluation. As the IG's report points out, the FTC has experienced significant turnover in the leadership of OCIO since 2000, and while the average tenure of the five Chief Information Officers who have served since that time is not outside the average across federal agencies, for a small agency, like the FTC, the impact of that turnover has been demonstrable.

Since July 2015, however, we have had a new Chief Information Officer (CIO) in place, and we are confident that the issues of concern identified by the IG already are being addressed and soon will be resolved. As set forth below, we have agreed to address each of the recommended action items identified by the IG.

We agree that short term and long term planning is critical, as is having an organizational structure for OCIO that supports the agency in meeting its mission and strategic goals. I have already undertaken an extensive analysis of OCIO, the skillsets of OCIO's federal employees and contractors, the agency's IT infrastructure and security posture, OCIO's operation, its budget and actual spend, gaps in performance as reported by various stakeholders and as assessed by OCIO management and staff. I have determined what competencies are needed to deliver IT services and support to the agency to meet its mission, and have drafted a proposed Agency Strategy and Transition Plan that addresses OCIO organizational structure, employee performance management expectations, additional critical positions that must be filled, and an acquisition plan, among other things. I have shared this draft Plan with all OCIO employees and stakeholders from throughout the agency in an iterative manner -- soliciting comment, revising

the Plan based on suggestions received, and recirculating the revised Plan for further discussion and assessment. We believe that we are on a firm path that will not only address the specific issues raised by the IG's report, but also determine whether OCIO is right skilled, right sized, and right budgeted to do the job required of it.

Finally, the IG's report voices concern that the CIO be positioned for success and have a seat at the table among agency leaders to ensure that the agency has the critical IT support equipment and services and budget necessary to support the mission and secure the agency's sensitive documents and IT assets. We agree and can assure the IG that the CIO has the support of the entire agency to ensure that OCIO gets what it needs to support the agency's mission. Our CIO has served as co-chair of the Business Council and has set the agenda for that body and the Governance Board, since its inception. And, as the IG has recommended, the CIO now has voting rights on the IT Business Council and on the Governance Board which was done with the full concurrence of the Bureaus and Executive Director.

The CIO, historically and regularly, meets with the FTC Chairperson and has direct interaction with the various Directors of the Bureaus and Offices. He, along with the Chief Financial Officer and the Chief Human Capital Officer – all of whom report to the Executive Director – are among a small cadre of SES'ers from throughout the agency that collectively run the FTC on a day-to-day basis. Although FITARA does not apply to the FTC, the strong working relationship between the CIO, CFO, and CHCO, as envisioned by that Act is facilitated by our current structure.

FTC Responses to the Proposed Actions Recommended by the IG

To afford the CIO authority commensurate with the intent of the Clinger-Cohen Act, best practices among federal agencies and to position the CIO to help accomplish the FTC's strategic goals for information security and information technology:

1. Extend voting rights to the Chief Information Officer on the FTC IT Governance board and the IT Business Council (The Executive Director).

   Responsible Official: David Robbins, Executive Director

   Action Plan: The IT Governance Board and the IT Business Council have extended voting rights to the Chief Information Officer (CIO).

   Expected Completion Date: Completed.

To improve the OCIO's support for the FTC's core mission and align the agency's IT investments to the needs of customers and stakeholders:

2. Identify the current OCIO core competencies and determine how they align with stakeholder needs, and identify performance shortfalls and gaps and their root causes (e.g., personnel, policy, business processes, resources, or technology), within 120 days (CIO).

Responsible Official: Raghav Vajjhala, CIO

Action Plan: Since his arrival in July 2015, the CIO has undertaken an extensive analysis of: 1) the skillsets of OCIO's current personnel (both FTE and contractor); 2) the agency's IT budget and spend; 3) OCIO's structure, operation, and use of contractors; 4) and the state of the agency's IT security and infrastructure. He also has met with agency stakeholders to get feedback on OCIO performance and stakeholder requirements and concerns. He has identified the core competencies required for OCIO to deliver IT services, whether it uses external vendors or federal employees.

He has directed his managers to document current areas of expertise for all federal employees and contractor staff, and he has met with OCIO staff, one-on-one or in small groups, to further assess their capabilities, determine their interests, and solicit their views about how best to proceed. The analysis identified, among other things, areas for improvement for FTEs, including project management and contract procurement and management, as evidenced by additional contractor services procured to address these gaps. Through discussion with OCIO managers, root causes for gaps include lack of a cohesive IT plan and clear explanation of roles and responsibilities across the organization, as would be identified through an updated organization chart with documented position descriptions.

To ensure all OCIO staff have an opportunity to share their concerns regarding potential changes in performance expectations, the CIO also has documented proposed roles, core competencies, and assignments in the Agency IT Strategy and Transition Plan. In October 2015, the CIO began sharing this information, including sharing the draft of the Agency IT Strategy and Transition Plan, with, and soliciting feedback from, all stakeholders (OCIO employees; the IT Business Council and Governance Board; Bureau and Office representatives; the Executive Director, his deputies, and the OED Directors; the Chief Privacy Officer; the Chief Technology Officer; the Chief of Staff; and the Chairwoman). This iterative process of sharing information, receiving feedback, and modifying the Plan as appropriate will continue through January 2016. The CIO has also begun posting those positions of highest need and has secured additional resources to draft position descriptions that align with the final IT workforce restructuring.

The final Agency IT Strategy and Transition Plan will identify core competencies required of OCIO to operate and provide IT services using either external vendors or federal employees. The Plan will align services with the Agency's Strategic Plan.

Expected Completion Date: FY2016 Q2

3. Using the data developed through the core competency assessment (recommendation 2), the FTC's Quadrennial Strategic Plan, and other agency priorities and initiatives, develop an IT Strategic Plan. The IT Strategic Plan should establish goals and objectives to serve both a) internal customers (operations and infrastructure) and b) external stakeholders (including federal partners, litigants, contractors, and consumers) that incorporate principles of enterprise risk management, performance-based metrics, and change

management, within 120 days following completion of the core competency assessment (recommendation 2) (CIO).

Responsible Official: Raghav Vajjhala, CIO

Action Plan: As noted above, the CIO has already shared drafts of the Agency IT Strategy and Transition Plan with all OCIO employees; the IT Business Council and Governance Board; Bureau and Office representatives; the Executive Director, his deputies, and the OED Directors; the Chief Privacy Officer; the Chief Technology Officer; the Chief of Staff; and the Chairwoman, and he continues to receive feedback on the Plan. In addition to aligning with the FTC's Quadrennial Strategic Plan and other agency initiatives and incorporating the principles identified by the IG above, the Plan will also address acquisition strategy, workforce restructuring, and budget management.

Expected Completion Date: FY2016 Q3

4. Assign ongoing responsibility to staff for conducting a) strategic planning b) enterprise architecture planning that accommodates the Federal Enterprise Architecture relevant to the FTC mission c) prototypes of emerging technology activities, and d) agency IT acquisition strategy to help anticipate and plan for the agency's future IT and information security requirements, within 90 days (CIO).

   Responsible Official: Raghav Vajjhala, CIO

   Action Plan: OCIO has already posted positions on USAJobs.gov critical to obtaining the right skillset to lead an IT Strategy and Planning team. Contingent on the identification of appropriately skilled resources through hiring and organization of OCIO FTEs, the CIO shall assign ongoing responsibility to staff for the conduct of a, b, c & d above. Also, OCIO shall use strategic planning to identify how best to apply and prioritize IT management practices, such as application of industry standard approaches including but not limited to enterprise architecture.

   Expected Completion Date: FY2016 Q2

To better clarify the roles and responsibilities of OCIO staff and communicate them effectively to the FTC workforce:

5. Update all OCIO employees' position descriptions to delineate current job descriptions, correct grade and promotion potential, and supervisory status; ensure position descriptions for OCIO managers include review of Contracting Officer's Representative (COR) performance in collecting and drafting contract requirements and monitoring contractor performance, within 120 days (CIO and HCMO).

   Responsible Official: Raghav Vajjhala, CIO

   Action Plan: The CIO has already shared updated draft position descriptions with expected areas of competency to all OCIO staff and the Chief Human Capital Officer and

appropriate Human Capital Management Office staff. Additionally, contract resources have been procured to formalize all draft position descriptions. Following review and input from employees as part of overall feedback on the IT Strategy and Transition Plan, all employees shall be given new position descriptions and performance plans, based on their assigned areas of work. Specific delivery commitments will be identified through the normal course of individual employee performance plan management.

Expected Completion Date: FY2016 Q3

To strengthen contract management and project management execution and oversight:

6. Using established OMB, FAR, Federal Acquisition Institute, and other guidance, and in coordination with the development of the IT Strategic Plan (recommendation 3), develop an acquisition strategy that reduces the complexity of current procurements and increases stakeholder visibility into contractor performance, within 240 days (CIO).

   Responsible Official: Raghav Vajjhala, CIO

   Action Plan: The Agency IT Strategy and Transition Plan will include an acquisition strategy that reduces the complexity of current procurements and increases stakeholder visibility regarding contractor performance. The CIO and Chief Financial Officer have been working in tandem to develop an IT acquisition strategy, including using the contract resources of the Financial Management Office (FMO) to identify various potential options. OCIO has also solicited the views of Bureau of Consumer Protection (BCP) staff that have made effective use of contract services to support large IT projects and continues to consult with other internal and external partners that have used government-wide guidance to reduce the complexity of procurements. As with other elements of the IT Strategy and Transition Plan, OCIO will engage stakeholders through iterative review, with additional coordination and support from FMO procurement staff and the CFO.

   Expected Completion Date: FY2016 Q3

7. Publish IT services that align with stakeholder requirements and the Quadrennial FTC Strategic Plan, service levels, and corresponding levels of resources required to provide these service levels, and post this data on the FTC Intranet, within 180 days (CIO).

   Responsible Official: Raghav Vajjhala, CIO

   Action Plan: OCIO will immediately publish its weekly operations review, which includes service levels and corresponding levels of resources required to provide these service levels. Long term – after vendors are brought on board following completion of a number of the critical acquisitions as part of the Acquisition Strategy -- OCIO will publish a formal service catalog of IT services, along with specific service level agreements.

B6
B5

Expected Completion Date: FY2016 Q3

8. Using the core competency assessment (recommendation 2) and published IT services (recommendation 7), and in coordination with the development of the IT Strategic Plan (recommendation 3), develop a recruitment, hiring, and training plan to acquire and sustain personnel needed for improved contract management, program management, and oversight within OCIO and in the FTC's Bureaus and Offices, and for IT service delivery across the FTC, within 300 days (CIO).

   Responsible Official: Raghav Vajjhala, CIO

   Action Plan: OCIO will update the Agency IT Strategy and Transition Plan with a recruitment, hiring, and training plan after restructuring the organization. OCIO requires individual development plans for each of its employees. Training to ensure that all OCIO employees are equipped to perform the requirements of the job shall be a part of individual development plans written at least yearly by each employee with their manager. As noted above, the CIO has already identified, posted, and is conducting interviews for, a number of critical positions.

   Expected Completion Date: FY2016 Q4

Contact the OIG

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

(202) 326-2800
Fax (202) 326-2034
OIG@ftc.gov
600 Pennsylvania Avenue, NW, CC-5206
Washington, DC 20580

Complaints may be made anonymously.

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