This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault

The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

Discover the Truth at: **http://www.theblackvault.com**

FEDERAL TRADE COMMISSION

OIG

10.01.15

—

03.31.16

SEMIANNUAL REPORT TO CONGRESS

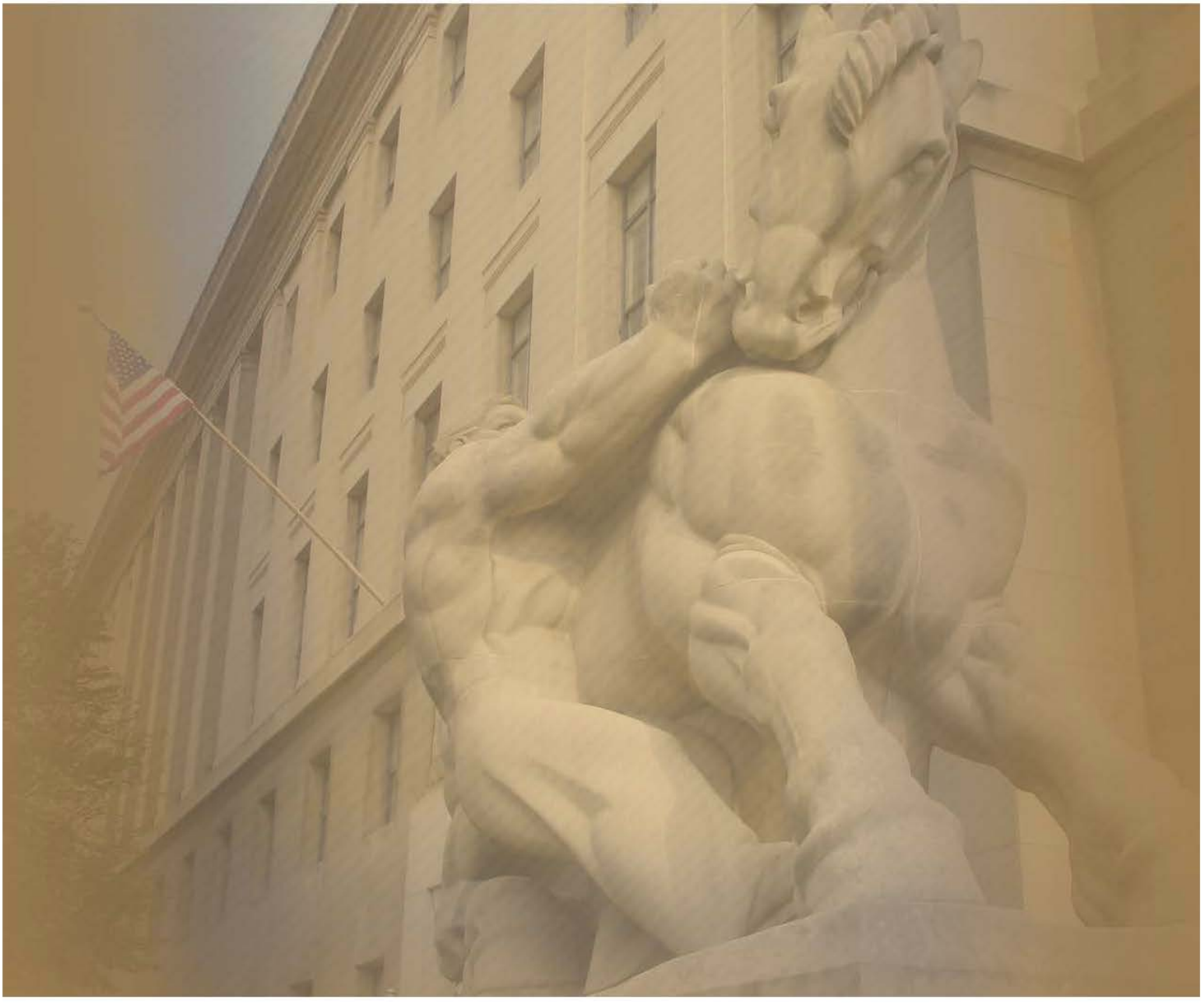


Table of Contents

Message From the Inspector General

On behalf of the Federal Trade Commission (FTC) Office of Inspector General (OIG), I am pleased to present our Semiannual Report to the Congress. The report summarizes the OIG's activities and accomplishments from October 1, 2015 through March 31, 2016.

During this reporting period, the OIG completed its evaluation of the Office of the Chief Information Officer (OCIO). The OIG performed this evaluation to determine whether the Chief Information Officer (CIO) has the authority, resources, structure, and organizational support needed to accomplish its current priorities and to assist the agency in realizing its mission. We found that the CIO's subordinate role on the FTC's Information Technology (IT) governance boards has diminished the CIO's ability to advance the CIO's authority and hampered the ability of the CIO to execute the agency's information security and IT mission. Moreover, significant turnover in the CIO's position in recent years has hampered the agency's ability to align IT investments and initiatives with enterprise-level priorities. We identified confusion among OCIO employees and customers about the responsibilities of OCIO employees and branches, and a general lack of communication and transparency about its projects. We also found deficiencies in contract administration that increase the agency's risk for poorly performing contractors and vendors, undelivered or delayed capabilities and functionality, protracted litigation, and challenges for mission success. With a new CIO having joined the agency in July 2015, management is addressing these challenges and has already implemented or is planning to implement OIG recommendations, including adding the CIO as a full voting member of the governance boards in November 2015.

We issued the FTC's Information Security Modernization Act (FISMA) evaluation for Fiscal Year (FY) 2015. The evaluation shows that FTC security and privacy programs are robust, demonstrating their ability to protect FTC assets while undergoing significant organizational, physical, and technological change. The FTC continues to evolve its information security program toward the risk-based model established by the National Institute of Standards and Technology by chartering IT governance boards to monitor IT planning, matching information security control measures to the FTC's unique threat profile, and allocating resources to mitigate vulnerabilities. Using for the first time the maturity model developed by the Council of the Inspectors General on Integrity and Efficiency, the evaluation shows opportunities to improve security control planning, the quality of security documentation, and the consistency of program implementation. The evaluation makes recommendations to improve information security planning and monitoring; program operations; the security of technology support provided from outside sources; and improved performance measurement techniques.

We issued the Financial Statement Audit for FY 2015, in which the FTC received an unmodified opinion – the highest opinion given by independent auditors – for the 19th consecutive year. We issued the associated Management Letter, which contains findings and recommendations to improve the agency's internal controls and operating efficiencies.

We identified what the OIG considers to be the agency's most important management challenges in FY 2016:

1. Securing the Agency's Information Systems and Networks from Destruction, Data Loss, or Compromise
2. Maturing the Agency's Information Technology Governance Process
3. Improving Contract Management
4. Stabilizing the Agency's eDiscovery Support System
5. Ensuring Compliance with Digital Records Management Requirements

There are several significant audits and evaluations underway, including follow-on evaluations from our FISMA reporting assessing whether the FTC's governance practices are continuing to show improvement in their ability to operate as a mature, risk-based decision support structure. The OIG continues to lean forward to embrace the Office of Management and Budget's initiative to integrate enterprise risk management into agency internal control efforts, including risks outside the financial management area.

FTC Bureaus and Offices continued to make significant progress implementing open OIG recommendations identified in previous semiannual reports, including the closing of all recommendations in our June 2015 evaluation of the Bureau of Economics.

Once again, I express my appreciation for the outstanding dedication of OIG personnel whose work is reflected in this report. I also express my appreciation to the Commission, agency leadership and staff, and to Congress for their sustained support to the OIG mission.

Roslyn A. Mazer
Inspector General
April 30, 2016

About the FTC Office of Inspector General

OIG Mission

To promote economy, efficiency and effectiveness, and to detect and prevent waste, fraud, abuse, and mismanagement in the agency's operations and programs.

OIG Vision

Optimize our value to stakeholders through high quality, independent, objective, and timely audits, investigations, and reviews.

OIG Strategic Goals

1. Maximize the Value the OIG Adds to FTC Programs and Operations
2. Enhance the Integrity of the FTC
3. Continuously Improve OIG Operations and Services

Introduction and Definitions

- **The mission of the Office of Inspector General is to promote economy, efficiency, and effectiveness, and to detect and prevent waste, fraud, abuse, and mismanagement in the agency's operations and programs.**

In compliance with the Inspector General Act Amendments of 1988 (5 U.S.C. app.), the Office of Inspector General (OIG) was established in 1989 as an independent and objective organization within the FTC.

Under the Inspector General Act of 1978, as amended, the OIG is responsible for conducting audits, evaluations, and investigations relating to the programs and operations of the FTC. Audits are conducted for the purpose of detecting and preventing fraud, waste, abuse, and mismanagement, and to promote economy, efficiency, and effectiveness within the agency. Evaluations are systematic assessments of the FTC's operations, programs or policies. OIG investigations seek out facts related to allegations of fraud and other wrongdoing on the part of FTC employees and individuals or entities having contracts with or obtaining benefits from the agency.

Individuals who wish to file a complaint about the business practices of a particular company or entity, or allegations of identity theft, deceptive advertising practices, or consumer fraud, should file a complaint with the FTC Consumer Response Center (CRC) at https://www.ftccomplaintassistant.gov or 1-877-382-4357. Individuals who wish to file a complaint with the FTC OIG about internal wrongdoing can file a complaint via a specialized link to the FTC Consumer Response Center (CRC) or by calling 202-326-2800. Complaints to the OIG from the public or from an FTC employee can be made anonymously. The identity of an FTC employee who reports waste or wrongdoing to the OIG will be protected from disclosure consistent with provisions of the Inspector General Act and privacy laws. In addition, the Inspector General Act and the Whistleblower Protection Act prohibit reprisals against employees for filing complaints or cooperating with the OIG.

The OIG is required by law to prepare a semiannual report summarizing the activities of the Office during the immediately preceding six-month period. The report is sent to the FTC Chair, the President of the Senate, the Speaker of the House, and the FTC's appropriating and authorizing committees. The OIG has an operating budget of $1,314,000 for FY 2016.

We perform the following services:

Performance Audits address the efficiency, effectiveness, and economy of the FTC's programs, activities, and functions; provide information to responsible parties to improve public accountability; facilitate oversight and decision making; and initiate corrective actions as needed.

Financial Audits provide an independent assessment of whether agency financial statements are presented fairly in accordance with generally accepted accounting principles. Reporting on financial audits in accordance with Government Auditing Standards also includes reports on internal controls and compliance with provisions of laws, regulations, and contracts as they relate to financial transactions, systems, and processes.

Inspections and Evaluations are systematic and independent assessments of the design, implementation, and/or results of the FTC's operations, programs, or policies. They provide information that is timely, credible, and useful for agency managers, policy makers, and others. Inspections or evaluations can be used to determine efficiency, effectiveness, impact, and/or sustainability of agency operations, programs, or policies.

Investigations are conducted based on alleged or suspected fraud, waste, abuse, or gross mismanagement; employee or contractor misconduct; or criminal and civil violations of law that affect the FTC's programs and operations. The OIG refers matters to the U.S. Department of Justice whenever the OIG has reasonable grounds to believe there has been a violation of federal criminal law. The OIG also identifies fraud indicators and recommends measures to management to improve the agency's ability to protect itself against fraud and other wrongdoing.

Management Advisories enable the OIG to expeditiously report findings of systemic weaknesses or vulnerabilities identified in the course of an audit, investigation or other IG activity. Management advisories typically contain recommendations to address OIG findings.

Evaluations, Audits, and Related Activities

Completed Reports

During this period, we issued two evaluations: an evaluation of the FTC's Office of the Chief Information Officer and the evaluation of the FTC's Information Security Modernization Act Program and Practices (FISMA) for Fiscal Year 2015. We issued two audit reports: the Financial Statement Audit for FY 2015 and the associated Management Letter.

Evaluation of the FTC Office of the Chief Information Officer

The Chief Information Officer (CIO) occupies a critical position within the FTC and with external stakeholders, whose sensitive information is stored in FTC's databases and repositories. 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. We found that:

- **A disconnect between authority and responsibility diminishes the CIO position.** The agency's 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. Further, while the CIO is represented and plays an important role on all three IT governance bodies, the CIO was a non-voting, ex-officio member of the two highest bodies – the IT Governance Board (ITGB) and the IT Business Council (ITBC). The CIO's subordinate role on the FTC's IT governance boards had diminished the CIO's ability to advance the CIO's authority and hampered 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. 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. 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 consequent 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 OCIO employees and customers as to OCIO responsibilities and a general lack of communication and transparency about its 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. 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.
- **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. 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. Taken together, 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.

To address these findings, we recommended that the FTC:

1. Extend voting rights to the CIO 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[1] 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 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 training, 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 FTC 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.

The FTC concurred with these recommendations and has taken significant steps to implement corrective action that will improve the agency's IT systems and program, including making the CIO a full voting member of the FTC's governance boards in November 2015.

[1] Federal enterprise architecture essentially attempts to align technology and managerial resources to provide a more unified, strategic outcome and performance.

FY 2015 Evaluation of the Federal Trade Commission's Information Security Program and Practices

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the FTC, to develop, document, and implement agency-wide information security programs. FISMA also requires Inspectors General to conduct independent evaluations of their agencies' information security program and practices.

The OIG contracted with Allied Technology Group Inc. to perform the independent FISMA evaluation. The objective was to provide an assessment of the effectiveness of the FTC's information assurance and privacy programs and compliance with Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidance. This evaluation is provided to senior management and others to enable them to determine the effectiveness of overall security programs, ensure the confidentiality and integrity of data entrusted to the FTC, and develop strategies and best practices for cost-effectively improving information security.

The evaluation determined that the FTC has established an information security program that is in substantial compliance with applicable security and privacy requirements. As required, this report uses an assessment approach that focuses on program effectiveness instead of compliance. For the first time, it also uses the maturity model developed by the Council of Inspectors General on Integrity and Efficiency (CIGIE).

FTC efforts to accelerate modernization of its IT capabilities and the increasing volume and sensitivity of FTC information assets will stress FTC systems when preventing cyber-attacks. Accordingly, continuing improvement while maintaining effective security will require increased emphasis on planning, Configuration Management, and attention to detail. We recommended that the FTC continue to evolve its governance practices, take appropriate action to ensure completion of an appropriate Configuration Management plan, and apply its revised governance process to the implementation of its Personal Identity Verification ("PIV") program so that compliance is not subject to continuing delay.

The FTC concurred with the evaluation's seven recommendations and has taken steps to implement corrective action that will improve the agency's information security program and practices.

FY 2015 Audit of the FTC's Financial Statements

Federal law requires that the FTC obtain an annual independent audit of its financial statements, which the OIG oversees. We contracted with the independent public accounting firm of Brown & Company CPAs, PLLC under a multi-year contract for which the OIG serves as the Contracting Officer's Representative (COR).

For the 19th consecutive year, the FTC received an unmodified opinion, the highest opinion given by independent auditors. As a result of the audit of the FTC's financial statements for the year ended September 30, 2015, Brown & Company found the following:

- The financial statements were presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles
- No deficiencies in internal control were identified as material weaknesses
- No reportable instances of noncompliance with applicable provisions of laws regulations, and contracts tested

Our oversight of the contractor ensures that the audit complies with generally accepted government auditing standards and meets contract requirements. The audit was performed in accordance with U.S. Generally Accepted Government Auditing Standards and Office of Management and Budget (OMB) audit guidance.

Management Letter from the FY 2015 Financial Statement Audit

When performing an audit of an agency's major financial systems and accounting processes, auditors often detect issues in internal controls that do not rise to a level of seriousness that render them necessary to report in the auditor's opinion. These findings and recommendations are communicated to the auditee in a management letter and are intended to improve the auditee's internal controls or result in other operating efficiencies.

The management letter addressed the FTC's controls in the following areas:

- The FTC did not adequately document the basis for a Small Business Administration (SBA) Sole Source Award.
- The timing of FTC's search for unrecorded liabilities and subsequent expense resulted in not properly accruing for one transaction tested.

Management concurred with these recommendations and provided detailed steps to implement corrective actions.

We commend management for addressing previous recommendations that enabled the OIG to close six of the seven open recommendations made in connection with prior financial statement audits.

Ongoing Work

Enterprise Risk Management

In FY 2016, the Office of Management and Budget (OMB) is updating Circular A-123, *Management's Responsibility for Internal Control*, to provide implementation guidance to assist federal agencies in employing Enterprise Risk Management (ERM) principles and practices to improve operational and support accountability. To prepare for these revisions, the FTC Inspector General and agency management have been discussing and defining their respective ERM roles. The OIG has increased its proficiency in applying ERM principles and techniques by attending events sponsored by OMB, the Government Accountability Office, and the Association for Federal Enterprise Risk Management; attending small agency working groups; and meeting with federal agencies with well-established ERM programs to identify best practices. The OIG is developing a methodology to identify and assess agency risks, focusing on risks affecting core mission areas that will not duplicate the areas that FTC management will address in FY 2016.

FISMA Follow-on Evaluations

The OIG continues with the following evaluations that augment our FY 2014 and 2015 FISMA evaluations:

- The OIG is evaluating whether the FTC's governance practices are continuing to show improvement in their ability to operate as a mature, risk-based decision support structure to effectively address investment and risk management challenges. The review will determine whether, in the face of increasing threats and greater public awareness that protecting information is a critical FTC role, the agency's governance practices have sufficiently matured to address the challenges resulting from a workforce requesting rapid availability of new technologies.
- Availability of reliable electronic discovery and litigation support (eDSS) capabilities is critical to the FTC's performance of its missions. The OIG will identify areas of weakness that can be corrected to ensure the eDSS provides the functionality to effectively support FTC litigation and to identify systemic issues that may be corrected to avoid similar problems in subsequent eDSS and other FTC IT acquisitions.
- As the FTC moves rapidly to make expanded mobile computing capabilities (e.g., smart phones, tablets, and "bring your own device") available to its workforce, new practices and procedures will be needed to identify and address the physical and logical risks that accompany the technological changes. The OIG is assessing whether the FTC's planning and monitoring practices are adequate to ensure that mobile computing can be safely implemented.
- The OIG is assessing FTC efforts to manage and reduce its holdings of Personally Identifiable Information (PII); how the agency has integrated its Privacy Program into its Information Security Program, and how the agency monitors performance of its PII reduction program. The review will

also assess risks associated with the collection, storage, sharing, retention, and disposal of various categories of nonpublic information held in FTC repositories that, if disclosed, compromised, or misused, pose significant risks to the FTC mission.

Corrective Actions on OIG Recommendations

During this reporting period, FTC Bureaus and Offices continued to make progress in implementing open OIG recommendations. The table in Appendix II identifies significant recommendations described in previous semiannual reports on which corrective action has not been completed. The OIG closed all of the remaining recommendations contained in the OIG evaluation report of the Bureau of Economics issued in June 2015, and one of eight recommendations contained in the evaluation report of the Office of the Chief Information Officer, issued in December 2015.

Section 5(a)(11) of the Inspector General Act of 1978, as amended, requires a description and explanation of the reasons for any significant revised management decision made during the reporting period. For this reporting period, management did not change its response to any earlier decisions on OIG recommendations.

Investigative Activities

The Inspector General Act of 1978, as amended, authorizes the Inspector General to receive and investigate allegations of employee misconduct as well as fraud, waste, abuse, and mismanagement occurring within FTC programs and operations. Matters of possible wrongdoing are referred to the OIG in the form of allegations or complaints from a variety of sources including FTC employees, other government agencies, and the general public. Reported incidents of possible fraud, waste, abuse, or mismanagement can give rise to administrative, civil, or criminal investigations.

Investigative Summary

The OIG maintains a toll-free Hotline number and a dedicated email address to enable individuals to bring matters to the attention of the OIG on a confidential basis. The toll-free Hotline number, facsimile, email address, and ground mail services are means by which FTC employees, contractors, and the general public may communicate allegations of fraud, waste, abuse, and mismanagement concerning FTC programs and operations to the OIG.

During this reporting period, the OIG received 456 consumer complaints, inquiries, and reports of possible wrongdoing. The OIG redirected 400 complaints to the FTC's Consumer Response Center (CRC) and three complaints to the FTC's FOIA office. This represents an 86% decrease in complaints received from the last reporting period. The OIG referred complaints under the jurisdiction of FTC programs to the appropriate FTC component for disposition. As described in the following discussion of the OIG Hotline, the decrease in consumer complaints during this reporting period reflects more efficient handling of these complaints through a direct online tool from the OIG's homepages to the CRC, rather than through the OIG Hotline itself.

Fake FTC Website

According to the 2015 FTC Consumer Sentinel Network Data Book, the number of government imposter complaints that the FTC received has increased from 159,000 in 2014 to over 353,000 in 2015, including imposters who claim they are with the FTC. During the last reporting period, the OIG described its referral of an FTC imposter scam involving at least 17 consumers who purportedly lost a total of $ 388,000 from this and related sweepstakes scams. During this reporting period, the United States Postal Service OIG continued to work with prosecutive authorities in developing its investigation.

Streamlining OIG Hotline Complaints

In FY 2015 the OIG reviewed the data accumulated from calls and emails to the OIG Hotline. The results

indicated opportunities to streamline this process to quickly forward the inquiries and complaints that come to the OIG Hotline that should be handled by the CRC, rather than by the OIG. The solution was to develop a business process improvement to streamline the consumer complaint collection process, with the following revisions:

- In collaboration with the FTC Bureau of Consumer Protection's Division of Consumer Response Operations, the OIG developed a specialized link on the OIG's Internet and Intranet OIG homepages that points complainants to the FTC Complaint Assistant. The link enables staff to quickly segregate the FTC OIG complaints in the Consumer Sentinel Network. All 18 complaints received during this reporting period via our specialized link concerned general FTC fraud matters, such as government imposters and automobile financing, rather than complaints within the OIG's jurisdiction.
- The OIG monitored all incoming Consumer Sentinel Network complaints submitted via the specialized link and removed the ones that concern internal FTC OIG matters. All removed complaints were tracked, logged, and maintained on an OIG log. At the end of this reporting period, only one complaint was removed using this procedure.
- The OIG revised the OIG Hotline voicemail and email greetings to promote the FTC Complaint Assistant link as the best complaint avenue. By the end of this reporting period, intake via voicemail and email methods fell from about 20 weekly complaints to one or two.
- The OIG revised the relevant OIG homepages to direct consumers to the specialized link, placing it as the first point of contact.

As a result of these modifications to OIG Hotline protocols, consumers may quickly access the direct channel for filing consumer complaints with the FTC, thereby also improving OIG office efficiency by drastically reducing consumer complaints coming into the OIG's voicemail and email.

Investigations Closed or Initiated

The OIG closed three investigations during the reporting period, two of which are highlighted below:

Allegation of Time and Attendance Fraud

The OIG received an allegation that an employee engaged in time and attendance fraud by working fewer hours than reported on his time sheets. The complaint further alleged that the employee's managers were aware of the abuse, but failed to take any action to correct the behavior. The OIG did not substantiate the allegation that the employee engaged in time and attendance fraud. The OIG also did not substantiate the allegation that the employee's supervisors were aware of time and attendance fraud allegations but failed to address them.

Allegation of Contractor Forgery

The OIG received an allegation a former FTC contractor forged the signature of an FTC contracting officer on a contract modification. It was further alleged that the contracting officer advised a supervisor that the contracting officer's signature was forged, but that the supervisor failed to notify the OIG. The OIG did not substantiate the allegation that the former contractor forged the signature of an FTC contracting officer on a contract modification. However, the OIG did find that the contracting officer reported the alleged forgery to the supervisor, but neither that supervisor nor a higher-level supervisor reported the allegation to the OIG, as required.

During this reporting period, the OIG opened three preliminary inquiries and one new investigation into allegations of employee misconduct or wrongdoing. The OIG also closed three investigations.

Preliminary Inquiries

The OIG initiated and closed a preliminary review of allegations that an FTC supervisor retaliated against a subordinate for bringing matters to the attention of management and the OIG. Based on a preliminary review of the evidence, the OIG did not find sufficient evidence to open an investigation.

Management Advisories and Referrals

During this reporting period, the OIG issued three management advisories or referrals stemming from investigative activity. These advisories identified potential internal control weaknesses and provided recommendations for improvement. We highlight two of them.

Contract Administration and Oversight

As the OIG recognized in is FY 2015 Management Challenges, the FTC obligated $104.9 million – approximately one-third of its operating budget in FY 2014 – on contracts for goods and services. The agency continues to face challenges with aspects of contract management, including guidance and oversight, execution of sound contracting techniques and approaches, and the current procurement application. As the agency continues its multi-year process to address this challenge, the OIG identified immediate opportunities to strengthen contract management and oversight.

- The FTC must manage its emails in accordance with the Federal Records Act, the Federal Acquisition Regulations System, other federal statutes, and agency policy. In so doing, the agency must ensure that Contracting Officers' Representatives and contractors archive relevant emails pertaining to the administration of FTC contracts. The OIG management advisory identified opportunities to reinforce these

responsibilities through training, contract drafting protocols, and policy clarification. Once implemented, these measures will improve both managerial oversight of FTC contracts and support of the OIG's mission to prevent and detect fraud, waste, and abuse. Management identified steps it is taking to address these recommendations.

- The OIG referred to management another matter involving contract administration and oversight growing out of the contractor forgery investigation referenced above. The OIG identified potential internal control issues that could result in unauthorized commitments or other actions during contract administration. Management identified steps it is taking to mitigate these concerns.

OTHER ACTIVITIES

Liaison with Other Agencies

During this reporting period, in conducting audits, investigations, and other activities, the OIG has sought assistance from and conferred with other federal agencies, including the following: the Government Accountability Office, the Farm Credit Administration, the Office of Government Ethics, the Department of Justice, and the Securities and Exchange Commission.

Activities within the Inspector General Community

The FTC IG is an active participant in the Council of the Inspectors General on Integrity and Efficiency (CIGIE), an independent entity within the Executive Branch comprised of federal Inspectors General. CIGIE's mission is to address integrity, economy, and effectiveness issues that transcend individual Government agencies; and increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General.

The IG's Counsel participates regularly in the Council of Counsels to Inspectors General (CCIG), and contributes to the legal discourse within the CCIG on matters that are germane to the entire OIG community.

The OIG's Audit Manager participates regularly in the monthly meeting of the Financial Statements Audit Network, a CIGIE subcommittee. She also teaches the financial statement section of the CIGIE Peer Review training offered to the greater OIG community.

The OIG's Program Analyst participates in the bimonthly meetings of the Inspection and Evaluation Roundtable, a CIGIE subcommittee, and contributes to the discourse involving evaluation developments and best practices.

The OIG also participates in CIGIE's Data Analytics Options Working Group, which is reviewing options to achieve comprehensive data analytics across the IG Community.

The Inspector General co-moderated a panel at the annual CIGIE-GAO Coordination meeting in March 2016 on Enterprise Risk Management, highlighting the varied approaches within the OIG community for promoting risk-based analyses and decisions within their agencies while maintaining the OIG's independent role and mission.

The OIG worked with FTC management to provide facilities for CIGIE training sessions at FTC Headquarters. The OIG is pleased to offer this convenient venue for CIGIE training and appreciates management's support for future planned training sessions.

Significant Management Decisions

Section 5(a)(12) of the Inspector General Act of 1978, as amended, requires that if the IG disagrees with any significant management decision, such disagreement must be reported in the semiannual report to Congress. For this reporting period, there were no significant management decisions made with which the IG disagreed.

Review of Legislation

Section 4(a)(2) of the Inspector General Act of 1978, as amended, authorizes the OIG to review and comment on proposed legislation or regulations relating to the agency or, upon request, affecting the operations of the OIG. The OIG also provides responsive information in response to direct requests from Congress.

During this reporting period, the OIG expressed support for the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) October 6, 2015, letter to the Chairman and Ranking Member of the U.S. Senate's Committee on Homeland Security and Governmental Affairs, urging support for the bipartisan substitute amendment to Senate bill S.579, *the Inspector General Empowerment Act of 2015*. The bill addresses the Department of Justice (DOJ) Office of Legal Counsel's (OLC) July 20, 2015, opinion stating that Section 6(a) of the IG Act does not give the DOJ OIG independent access to all records available to DOJ that are needed to perform its oversight functions. Recognizing that the OLC interpretation of the IG Act could have a profound negative impact on the entire OIG community, the FTC OIG continues to support CIGIE efforts to urge Congress to immediately pass legislation affirming the authority of Inspectors General under the IG Act to access independently and without delay all information in an agency's possession that the Inspector General deems necessary to conduct oversight functions.

Access to Information

Inspectors General must have ready access to all agency records, information, or assistance when conducting an investigation or audit. Section 6(b)(2) of the Inspector General Act of 1978, as amended, requires the Inspector General to report to the agency head, without delay, if the Inspector General believes that access to required information, records, or assistance has been unreasonably refused, or otherwise has not been provided. A summary of each report submitted to the agency head in compliance with Section 6(b)(2) must be provided in the semiannual report in accordance with Section 5(a)(5) of the Act. During this reporting period, the OIG did not encounter problems or delays in obtaining assistance or access to agency records.

Other Initiatives

The Inspector General participated in several meetings with Office of Management and Budget (OMB) officials and representatives of the OIG community to discuss OMB objectives and plans for revising Circular A-123, *Management's Responsibility for Risk Management and Internal Control.* In the first update to the circular in over ten years, the revision will incorporate principles of enterprise risk management in the federal government.

In furtherance of our efforts to educate the FTC workforce on the whistleblower protection laws, the OIG collaborated with agency management to register the FTC in the Office of Special Counsel's 2302(c) certification program. This program assists agencies in meeting their statutory requirements to inform employees of their rights and remedies under 5 U.S.C. § 2302. The FTC's enhanced program will be fully implemented within the next reporting period.

The OIG continues to work with FTC management to improve the policy and practice for tracking OIG recommendations. This process includes quarterly meetings between the OIG and FTC management. These meetings facilitate regular communication between the OIG, the Executive Director, and FTC Bureaus and Offices about progress made or impediments encountered in implementing OIG recommendations.

Appendix I – Peer Reviews

Peer Review Activity	Results
Peer Reviews conducted by another OIG	No other agency OIG conducted peer reviews of the FTC OIG during this reporting period.
Outstanding recommendations from peer reviews of the FTC OIG	There are no outstanding recommendations from peer reviews of the FTC OIG.
Peer Review conducted by the FTC OIG	The FTC OIG did not conduct any peer reviews during this reporting period.
Outstanding recommendations from peer reviews conducted by FTC OIG	There are no outstanding recommendations from peer reviews conducted by the FTC OIG.

Appendix II – Significant OIG Recommendations Described in Previous Semiannual Reports with Corrective Actions Pending

Independent Assessment of Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2014 (Report Issued: 05/2015)

Recommendations	Total	7
	Mgmt. concurs	7
	Mgmt. non-concurs	--
Status of Recommendations	Closed*	4
	Open*	3

Recommendations

- **FY 2014 – 03: Infrastructure Documentation**

  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.

- **FY 2014 – 04: Certification and Accreditation**

  FTC should revise its process for determining Minor Applications and documenting security controls.

- **FY 2014 – 06: Contingency Plans**

  FTC should develop a disaster recovery strategy and implementation plan.

* A recommendation is closed if the OIG determines that (1) the corrective action has been taken, or (2) the recommendation is no longer applicable. A recommendation is open if FTC management agrees with the recommendation and is in the process of taking corrective action. Some corrective actions may have been completed by management and are awaiting verification by the OIG.

Independent Assessment of Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2013 (Report Issued: 03/2015)

Recommendations	Total	5
	Mgmt. concurs	5
	Mgmt. non-concurs	--
Status of Recommendations	Closed	4
	Open	1

Recommendation

- FY 2013–07: Identity and Access Management

  FTC should revise its infrastructure access procedure to restrict access until background screening is completed per FTC policy.

Financial Statement Audit for Fiscal Year 2013 Management Letter (Report Issued: 05/2014)

Recommendations	Total	5
	Mgmt. concurs	5
	Mgmt. non-concurs	--
Status of Recommendations	Closed	4
	Open	1

Recommendation

- ML-13-2

  We recommend FTC perform the following:

  1. Review and determine the validity of undelivered orders on a semi-annual basis;
  2. Develop policy requiring certification for all open obligation balances that are inactive for more than 12 months.

Appendix III – Inspector General Issued Reports with Questioned Costs

	Number	Questioned Costs (dollar value)	Unsupported Costs(dollar value)
A. For which no management decision has been made by the commencement of the reporting period	0	0	0
B. Which were issued during the reporting period	0	0	0
Subtotals (A+B)	0	0	0
C. For which a management decision was made during the reporting period	0	0	0
i. dollar value of the disallowed costs	0	0	0
ii. dollar value of the cost not disallowed	0	0	0
D. For which no management decision was made by the end of the reporting period	0	0	0
E. Reports for which no management decision was made within six months of issuance	0	0	0

Appendix IV – Inspector General Issued Reports with Recommendations that Funds be Put to Better Use

	Number	Dollar Value
A. For which no management decision has been made by the commencement of the reporting period	0	0
B. Which were issued during the reporting period	0	0
C. For which a management decision was made during the reporting period	0	0
i. dollar value of recommendations that were agreed to by management	0	0
• based on proposed management actions	0	0
• based on proposed legislative action	0	0
ii. dollar value of recommendations that were not agreed to by management	0	0
D. For which no management decision was made by the end of the reporting period	0	0
E. Reports for which no management decision was made within six months of issuance	0	0

Appendix V – Inspector General Act Reporting Requirements Index

IG Act Reference	Reporting Requirements	Pages(s)
Section 4(a)(2)	Review of legislation and regulations	18
Section 5(a)(1)	Significant problems, abuses and deficiencies	none
Section 5(a)(2)	Recommendations with respect to significant problems, abuses and deficiencies	6-16
Section 5(a)(3)	Prior significant recommendations on which corrective actions have not been made	21-22
Section 5(a)(4)	Matters referred to prosecutive authorities	13-16
Section 5(a)(5)	Summary of instances where information was refused	none
Section 5(a)(6)	List of reports by subject matter, showing dollar value of questioned costs and funds put to better use	none
Section 5(a)(7)	Summary of each particularly significant report	6-10
Section 5(a)(8)	Statistical tables showing number of reports and dollar value of questioned costs	23
Section 5(a)(9)	Statistical tables showing number of reports and dollar value of recommendations that funds be put to better use	24
Section 5(a)(10)	Summary of each report issued before this reporting period for which no management decision was made by the end of the reporting period	none
Section 5(a)(11)	Significant revised management decisions	none
Section 5(a)(12)	Significant revised management decisions with which the Inspector General disagrees	none
Section 5(a)(14)	Peer reviews conducted by another OIG	20

IG Act Reference	Reporting Requirements	Pages(s)
Section 5(a)(15)	Outstanding recommendations from peer reviews of the OIG	none
Section 5(a)(16)	Outstanding recommendations from peer reviews conducted by the OIG	none

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.

FEDERAL TRADE COMMISSION

OIG

04.01.16

—

09.30.16

SEMIANNUAL REPORT TO CONGRESS

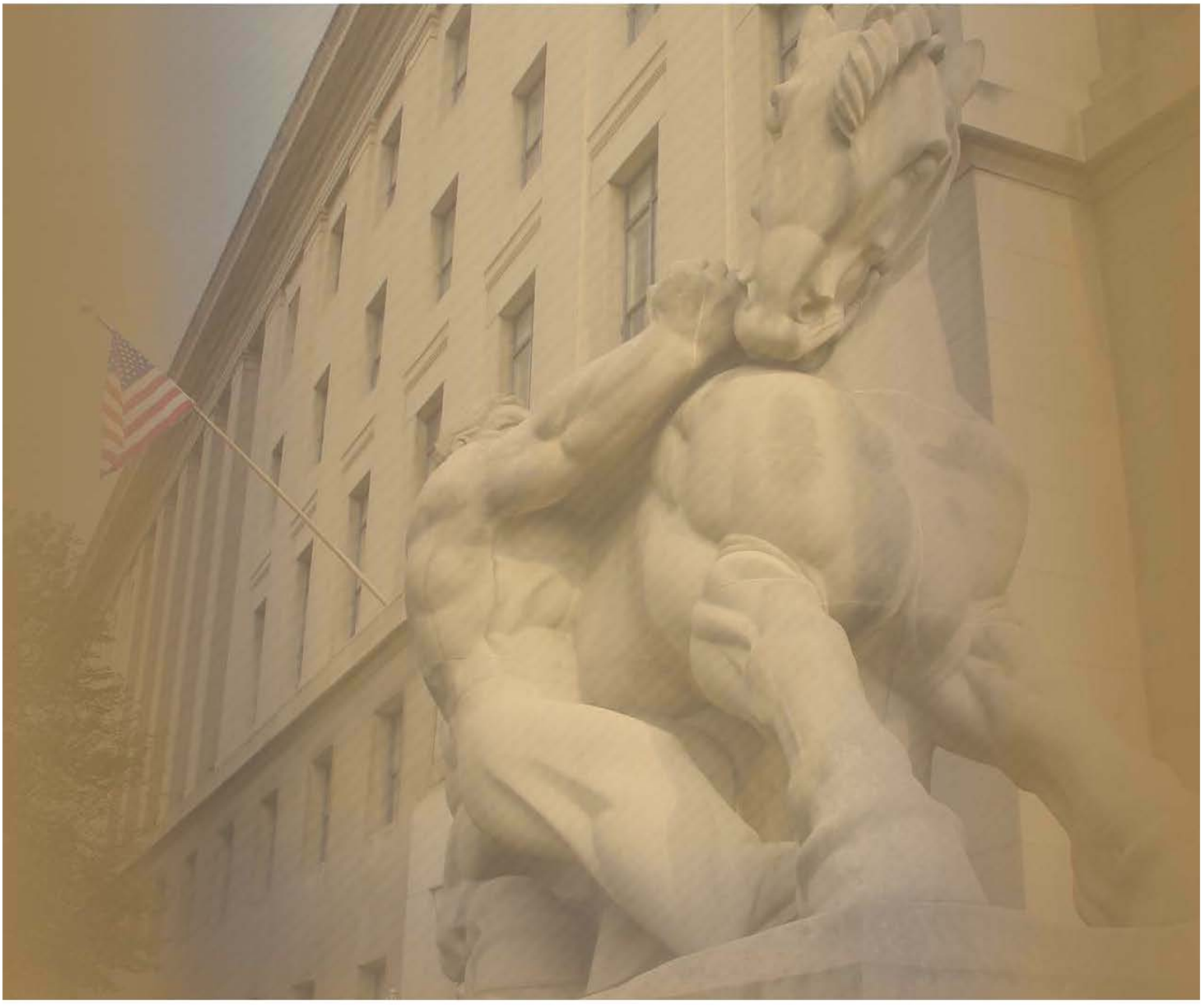


Table of Contents

Message From the Inspector General

On behalf of the Federal Trade Commission (FTC) Office of Inspector General (OIG), I am pleased to present our Semiannual Report to the Congress. The report summarizes the OIG's activities and accomplishments from April 1, 2016 through September 30, 2016.

During this reporting period, the OIG completed its evaluation of the FTC's Information Technology (IT) Governance Practices. This is the most recent in a series of evaluations performed by the OIG since the FTC chartered its governance program in 2011. Each year, the OIG has assessed that, while the program is maturing, progress has been slow, it is not documented through repeatable processes, and it continues to have a project focus, rather than the enterprise-wide focus urged by the Office of Management and Budget (OMB) and National Institute of Standards and Technology. Our recent evaluation assessed the governance program's progress through close analysis of two ongoing, mission-critical acquisitions: the FTC's electronic discovery platform (eDSS) and its mobile device modernization project. The OIG concluded that the IT Governance Program continues to mature, with participants "taking ownership" by raising security and system performance concerns, more actively monitoring approved projects, and explicitly including risk as a decision factor under revised IT Governance Board project approval criteria. However, the evaluation identified governance process weaknesses that affect all investments to varying degrees, and project-specific weaknesses caused by a failure to follow FTC procedures. Both weaknesses had significant impacts. For example, the Governance Board approved project funding for the eDSS project even when significant Business Case Analysis elements were identified as deficient or omitted, without establishing milestone review requirements. This allowed identified deficiencies in the eDSS solicitation to remain unresolved through procurement, resulting in poor or slow performance and poor reliability of eDSS services for the work force. The report contained recommendations that address both types of governance program weaknesses.

Our investigative work included completion of an investigation of a veteran FTC employee who served in a "high risk" position, as defined by the Office of Personnel Management. The investigation determined that the employee had misused the employee's official position "for personal use" by sending a letter on behalf of the employee and the employee's relative to another federal agency on official FTC letterhead. The letter requested a hearing by the other federal agency regarding a personal matter. The OIG determined that the communication constituted a misuse of public office for private gain, misuse of government property, and misuse of official time in violation of the federal employee Standards of Ethical Conduct regulations. Because of the employee's relatively low General Schedule (GS) level, the employee had never received agency ethics training. The OIG issued a Management Advisory with recommendations for additional training under the auspices of the FTC's Ethics Program.

To continue to mature the OIG's investigations program, we conducted outreach visits to three of the FTC's seven regional offices. The objective of the visits was to acquaint FTC managers and staff with the unique role and mission of the OIG; to conduct proactive fraud, waste, and abuse training; and for OIG staff to learn about the mission and often unique challenges of working in FTC regional offices. We appreciate the agency's enthusiastic support for our ongoing efforts to be deeply knowledgeable about all aspects of the FTC mission, work force, and priorities.

The OIG continues its support for incorporating enterprise risk management principles into the culture, fabric, and business processes of the FTC and the OIG. With the July 2016 revision of OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, the OIG plans to continue its effort to acquire expertise to enable it to champion this vital shift in addressing and mitigating financial and non-financial risks in FTC and OIG programs and operations.

This reporting period coincided with the months leading up to the Presidential election of 2016. I served on a working group established by the Council of the Inspectors General on Integrity and Efficiency that met with OMB officials and others involved in implementing the Presidential Transition Act of 2012. The working group helped identify opportunities to acquaint the Presidential nominees' transition teams, the President Elect's transition team, and incoming Administration officials with the unique role and mission of the OIG community. As part of this effort, the working group developed the Presidential Transition Handbook to address the need for a concise, readable synopsis of the history of the Inspector General Act of 1978, authorities of inspectors general, recurring reports, significant accomplishments over the years, and other aspects of the OIG mission.

FTC Bureaus and Offices continued to make progress implementing open OIG recommendations identified in previous semiannual reports.

Once again, I express my appreciation for the outstanding dedication of OIG personnel whose work is reflected in this report. I also express my appreciation to the Commission, agency leadership and staff, and to Congress for their sustained support to the OIG mission.

About the FTC Office of Inspector General

OIG Mission

To promote economy, efficiency and effectiveness, and to detect and prevent waste, fraud, abuse, and mismanagement in the agency's operations and programs.

OIG Vision

Optimize our value to stakeholders through high quality, independent, objective, and timely audits, investigations, and reviews.

OIG Strategic Goals

1. Maximize the Value the OIG Adds to FTC Programs and Operations
2. Enhance the Integrity of the FTC
3. Continuously Improve OIG Operations and Services

Introduction and Definitions

- **The mission of the Office of Inspector General is to promote economy, efficiency, and effectiveness, and to detect and prevent waste, fraud, abuse, and mismanagement in the agency's operations and programs.**

In compliance with the Inspector General Act Amendments of 1988 (5 U.S.C. app.), the Office of Inspector General (OIG) was established in 1989 as an independent and objective organization within the FTC.

Under the Inspector General Act of 1978, as amended, the OIG is responsible for conducting audits, evaluations, and investigations relating to the programs and operations of the FTC. Audits are conducted for the purpose of detecting and preventing fraud, waste, abuse, and mismanagement, and to promote economy, efficiency, and effectiveness within the agency. Evaluations are systematic assessments of the FTC's operations, programs or policies. OIG investigations seek out facts related to allegations of fraud and other wrongdoing on the part of FTC employees and individuals or entities having contracts with or obtaining benefits from the agency.

Individuals who wish to file a complaint about the business practices of a particular company or entity, or allegations of identity theft, deceptive advertising practices, or consumer fraud, should file a complaint with the FTC Consumer Response Center (CRC) at https://www.ftccomplaintassistant.gov or 1-877-382-4357. Individuals who wish to file a complaint with the FTC OIG about internal wrongdoing can file a complaint via a specialized link to the FTC Consumer Response Center (CRC) or by calling 202-326-2800. Complaints to the OIG from the public or from an FTC employee can be made anonymously. The identity of an FTC employee who reports waste, fraud, or wrongdoing to the OIG will be protected from disclosure consistent with provisions of the Inspector General Act and privacy laws. In addition, the Inspector General Act and the Whistleblower Protection Act prohibit reprisals against employees for filing complaints or cooperating with the OIG.

The OIG is required by law to prepare a semiannual report to Congress summarizing the activities of the Office during the immediately preceding six-month period. The report is sent to the FTC Chair, the President of the Senate, the Speaker of the House, and the FTC's appropriating and authorizing committees. The OIG had an operating budget of $1,314,000 for FY 2016.

We perform the following services:

Performance Audits address the efficiency, effectiveness, and economy of the FTC's programs, activities, and functions; provide information to responsible parties to improve public accountability; facilitate oversight and decision making; and initiate corrective actions as needed.

Financial Audits provide an independent assessment of whether agency financial statements are presented fairly in accordance with generally accepted accounting principles. Reporting on financial audits in accordance with Government Auditing Standards also includes reports on internal controls and compliance with provisions of laws, regulations, and contracts as they relate to financial transactions, systems, and processes.

Evaluations are systematic and independent assessments of the design, implementation, and/or results of the FTC's operations, programs, or policies. They provide information that is timely, credible, and useful for agency managers, policy makers, and others. Evaluations can be used to determine efficiency, effectiveness, impact, and/or sustainability of agency operations, programs, or policies.

Investigations are conducted based on alleged or suspected fraud, waste, abuse, or gross mismanagement; employee or contractor misconduct; or criminal and civil violations of law that affect the FTC's programs and operations. The OIG refers matters to the U.S. Department of Justice whenever the OIG has reasonable grounds to believe there has been a violation of federal criminal law. The OIG also identifies fraud indicators and recommends measures to management to improve the agency's ability to protect itself against fraud and other wrongdoing.

Management Advisories enable the OIG to expeditiously report findings of systemic weaknesses or vulnerabilities identified in the course of an audit, investigation or other IG activity. Management advisories typically contain recommendations to address OIG findings.

Evaluations, Audits, and Related Activities

Completed Reports

During this period, the OIG issued an evaluation on the FTC's Information Technology Governance Practices, a report on the FTC's covered systems as required by the Cybersecurity Act of 2015, and a review of FTC's compliance with the Improper Payments Information Act of 2002.

Opportunities Exist to Accelerate Maturation of the FTC's Information Technology Governance Practices

As a follow on to its FY 2014 Federal Information Security Management Act of 2012 (FISMA) evaluation, the OIG tasked TACG, LLC to perform an evaluation of the governance practices the FTC uses to plan, evaluate, fund, and monitor Information Technology (IT) projects. The objective was to determine if the FTC governance process includes procedures and controls to identify and resolve potential problems and minimize the risk of project failure. IT governance is the framework an organization uses to align its IT strategy with its business strategy and ensure that the organization meets its mission and associated strategic goals and objectives.

The OIG identified three projects (two approved for FTC funding and a government-wide program that might be reflected in an FTC project) for inclusion in the analysis: the e-Discovery Support System (eDSS), the Mobile Device Project, and FTC planning for information system changes resulting from the government-wide Controlled Unclassified Information (CUI) program. Each of three projects has a high impact on the FTC mission and the day-to-day activities of its work force and contractors.

- e-Discovery Support System (eDSS) – The eDSS project was initiated in 2013 to replace and modernize tools used by the FTC to collect and analyze information produced as part of FTC litigation activities. The new eDSS was planned to be more reliable, have expanded capabilities, and be capable of processing the large volumes of data associated with FTC litigation activities in shorter timeframes than legacy software. The eDSS is used principally to support the Bureau of Competition (BC) and the Bureau of Consumer Protection (BCP), but may be used by the Bureau of Economics and Offices with large-scale data collection and analysis needs.

- Mobile Device Modernization Project – The Mobile Device Modernization Project is part of the FTC initiative to modernize the mobile computing and communications devices used by FTC personnel. The project evaluated was the replacement and upgrade of the FTC's Blackberry personal data assistant (telephone and e-mail) with state-of-the-art smart phones.

- Controlled Unclassified Information (CUI) – The National Archives and Records Administration (NARA) is the Executive Agent for a program to standardize the categorization, marking, and safeguarding of information that is sensitive, but unclassified. FTC information systems may need to be modified to address changes in marking and labeling requirements originating from NARA and CUI protection requirements originating from the National Institute of Standards and Technology (NIST). Current direction from NARA is to pause changes involving categorization, labeling, and marking. Current direction from NIST is to implement moderate level safeguarding measures to all information and systems that collect, transmit, process, or store CUI. The OIG evaluated the process for integrating current direction and potential CUI changes into the governance process.

Generally, the OIG evaluation showed that the IT Governance Program is beginning to mature. Governance Program materials show that participants are "taking ownership" and are raising security and system performance concerns. In addition, the FTC revised the criteria for Governance Board review to include risk as a decision factor and instituted increased monitoring of approved projects. The FTC made significant changes in approach and business process that demonstrate the Chief Information Officer's commitment to maturing Governance Board deliberations and decisions, and show that the Governance Boards recognize that compromise of even a very low cost project that contains no sensitive information can result in severe damage to FTC's reputation. They also reflect a core principle of enterprise risk management (ERM), now explicitly embedded in the Office of Management and Budget's (OMB) revised Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 2016).

The OIG evaluation of these projects also identified areas for improvement. Although both the eDSS and mobile device modernization projects met FTC criteria for a large, complex, high performance risk investment and required a full Business Case Analysis and an Acquisition Plan, the OIG evaluation found that neither project had an Acquisition Plan. The OIG also found that neither the Governance Program charter nor the IT Acquisition Strategy described how the Governance Program would work in concert with the Acquisition Strategy to maximize the potential for successful outcomes (i.e., goods and services that meet FTC needs for functionality, reliability, security, and cost effectiveness).

The OIG identified two types of governance weaknesses: *governance process weaknesses* that affect all investments subject to the FTC Governance Program to varying degrees, and *project-specific weaknesses* caused by a failure to follow FTC procedures. The OIG assessed that governance process weaknesses affected the FTC's ongoing acquisitions for eDSS and mobile devices and described how these same weaknesses could, if unaddressed, complicate and delay the FTC's ability to assimilate current guidance and new requirements for the CUI program as well as future IT acquisitions to which the FTC Governance Program applies. Key findings were that 1) a failure to integrate the FTC IT Governance Program Charter with the Federal Acquisition Regulation / *FTC OCIO Acquisition Strategy for Information Technology* principles

increase the potential for inconsistent planning and oversight and delivery of products and services that do not meet FTC requirements; 2) governance decisions did not include milestones or other restrictions to monitor and verify resolution of identified deficiencies; 3) Business Case Analyses provided to the Governance Boards did not include appropriate workload analyses; and 4) FTC Governance Board procedures do not include a formal problem escalation process. The governance process weaknesses had the following impacts on the three projects evaluated:

- The FTC's Governance Program Charter identifies the Business Case Analysis as the primary decision document, but fails to mention that FTC acquisitions are also governed by the Federal Acquisition Regulation (FAR) Part 7. This results in a situation where a Business Case Analysis can be prepared in accordance with FTC guidance but not incorporate FAR policies. Lack of integration of FAR principles into the BCA had a significant impact on the eDSS project. For example, had the eDSS followed a FAR analytical framework, the cost and workload estimate deficiencies identified in the Business Case Analysis and the deferred performance and evaluation procedures (e.g., performance criteria and solicitation documents) would have been reflected as milestones or "stage gates," where deficiencies were resolved before the project proceeded. While use of FAR analysis and acquisition management practices do not guarantee project success, they minimize performance risk and allow for timely problem resolution.
- The Governance Board approved project funding even when significant Business Case Analysis elements were identified as deficient or omitted, without establishing milestone review requirements. This allowed identified deficiencies in the eDSS solicitation to remain unresolved through procurement, resulting in poor or slow performance and poor reliability of eDSS services provided to FTC users.
- The FTC developed an eDSS workload projection that substantially underestimated resource requirements. The underestimate was due to different storage approaches and different resource utilization rates of the new eDSS software versus the legacy software. This resulted in poor performance and inability to process the volumes of data needed to meet FTC requirements.
- The lack of a formal problem escalation process resulted in problem projects continuing for multiple years without resolution. For example, the eDSS acquisition did not include the legal features such as Litigation Hold necessary to support FTC e-discovery needs and the processing capacity to effectively support FTC workloads. These deficiencies required Bureaus to use manual procedures or other products to compensate for functional deficiencies, and to take turns preparing productions to opposing counsel or courts to compensate for the lack of processing capability.

The OIG identified several areas for improvement and made the following recommendations to accelerate the maturity of the IT Governance Board practices:

1. Complete applicable Business Case Analysis elements, including a description of security requirements and how they will be met, functional requirements document, Return on Investment (ROI) analysis, and risk assessment; and document instances where a BCA requirement is waived or revised, with supporting justification and risk mitigations. Ensure the BCA considers related FAR requirements.
2. Accurately and consistently capture Information Technology Governance Board planning decisions related to business needs and supporting rationales for those decisions. Information documenting Board decisions may be included in separate documentation or meeting minutes.
3. Develop and institute standard operating procedures with associated work instructions to support acquisition proposals and decisions, including workflows, milestones, escalation criteria, and project monitoring and tracking procedures.
4. Issue guidance for developing and documenting reliable cost and workload estimates used to support acquisitions. The guidance should include selection and documentation of cost and workload models, development of a basis of estimate that documents procedures used to develop the estimates, and factors affecting estimate reliability.
5. Require the development of FTC Information Technology and security organizational priorities to guide Governance Board review and approval of projects and investments by identifying and ranking topic areas where information systems or processes need improvement to reduce costs or improve performance; establish risk thresholds by identifying the level of risk of a system failure or data breach that the FTC is willing to tolerate; and periodically review and revise organizational priorities and risk thresholds.
6. Implement an escalation process that promotes, though FTC's continuous monitoring processes, identification of potential performance problems or opportunities for improvement; identifies organizations with the skills and skill levels necessary to research and resolve project issues by problem area and skill level; implements problem tracking from identification to resolution; and establishes timelines for problem resolution and for routine (e.g., weekly, monthly, quarterly) monitoring of compliance with those timelines.
7. Terminate efforts to remedy deficiencies in the current Electronic Discovery Support System (eDSS) product, except those actions necessary to continue support for cases in progress; prepare an After Action Report that documents the problems encountered with the current software for use as input for the acquisition of a replacement contract; and initiate a new acquisition to obtain a follow-on contract using lessons learned under the current contract to avoid similar problems.
8. Develop an eDSS functional requirements document that specifies the required capabilities (including security, privacy, and performance monitoring controls), acceptance criteria, or performance

characteristics of the supplies or the performance standards for the services being acquired and state how they are related to the business need; identifies requirements for compatibility with existing or future systems or programs; describes any known cost, schedule, and capability or performance constraints; and associates requirements with acceptance criteria and performance standards.

9. Require maintenance of an eDSS traceability matrix that identifies authorized functions and how they have been implemented and successfully tested. The traceability matrix should be scaled to acquisition complexity, allowing required functions to be tracked from the functional requirement document, through solicitation and acceptance testing.
10. Maintain a set of comprehensive benchmarks that can perform acceptance testing whenever the eDSS is changed; maintain a test database that will support eDSS workload analysis and troubleshooting; and use benchmark testing to establish performance baselines that can be validated throughout the eDSS contract life. Identify approaches that may be used to support stress testing analysis on a limited basis without the need to maintain a hosting facility.
11. Align a eDSS follow-on contract period of performance to allow cases/matters to proceed from initiation to completion with little or no disruption from a transfer to a new system or hosting facility.
12. Prepare a Business Case Analysis that provides the rationale and support for the mobile device project and its ongoing operation; include a discussion of the risks associated with the technological model deployed; and identify system functionality and relate it to business needs.
13. Develop a System Security Plan for the mobile device project based on National Institute of Standards and Technology (NIST) Special Publication 800-53 r4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The plan should leverage the existing Data Center ATO and Maas360 PATO as appropriate.
14. Provide training in best practices for establishing and managing project schedules; ensure project schedules contain milestones for evaluating project performance; allow slack time for resolution of unintended events; and ensure that critical tasks are completed or justification is provided if project tasks or schedules are not to be completed or are delayed.
15. Identify systems that may include Controlled Unclassified Information (CUI) using FTC policy effective on the date a project is submitted for approval. Include control requirements of the CUI program as identified in NIST Special Publications in FTC planning for systems, information inventories, and information protection controls. Monitor ongoing National Archives and Records Administration and NIST CUI program activities to ensure the FTC remains current with the direction and status of CUI program requirements.

The FTC concurred with the fifteen recommendations and has taken steps to implement corrective actions that will improve the agency's IT governance practices.

OIG Report on the FTC's Covered Systems under the Cybersecurity Act of 2015

In accordance with Section 406 (b) of the Cybersecurity Act of 2015, the FTC OIG provided to Congress the required Report on Covered Systems.

The OIG submitted the questions contained in the Cybersecurity Act to the System Owners for FTC Covered Systems. The information received was reviewed for accuracy and consistency by comparing responses against information obtained through OIG Federal Information Security Modernization Act of 2014 (FISMA) assessments (e.g., System Security Plans, security and performance monitoring reports, and contracts for Covered System support). The results of the OIG analysis were provided as responses to the specific questions posed in the Act. However, the OIG did not independently verify through testing or performance audit that Covered Systems are operating as intended under the referenced policies.

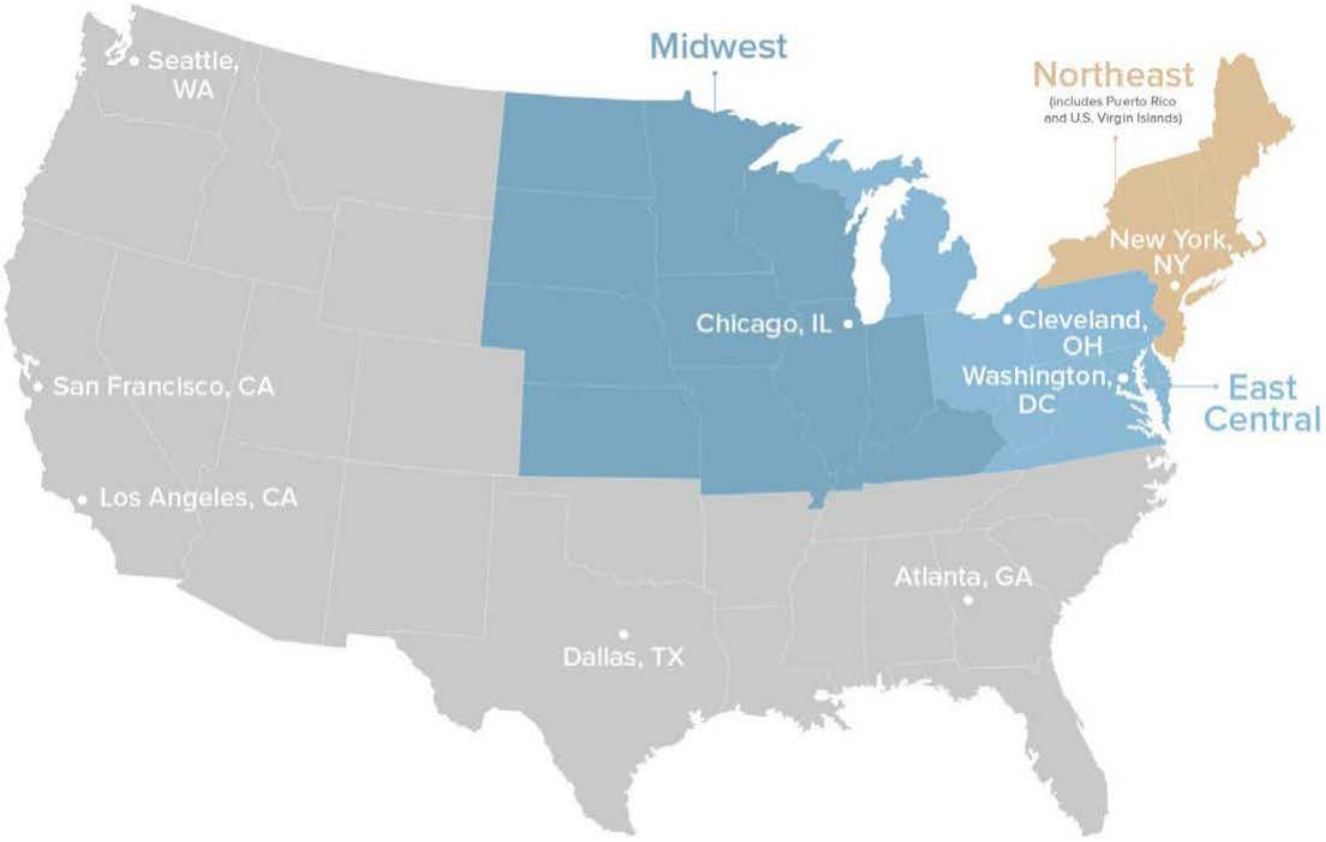
FTC Covered Systems included systems that are owned and operated by the FTC (39 systems), systems that are contractor owned and operated but are dedicated for FTC use (6 systems), systems operated as shared services by other Federal agencies (6 systems), and commercial shared systems (9 systems). The responses provided in this report encompassed all 60 systems.

Review of the FTC's Compliance with the Improper Payments Information Act of 2002, as Amended

The OIG assessed the FTC's compliance with improper payment reporting requirements of the Improper Payments Information Act of 2002, as amended. The OIG determined that the FTC is compliant, in all material respects, for FY 2015. The FTC reported in its FY 2015 Agency Financial Report that it performed a risk assessment of the agency's programs and activities; determined that it presented a low risk of improper payments and none of the agency's programs or activities were determined to be susceptible to significant improper payments.

Ongoing Work

Outreach to FTC Regional Offices



During this reporting period, the OIG launched a proactive initiative to acquire a greater understanding of the mission, role, and specials challenges of the FTC's regional offices and to acquaint these offices with the unique role of the OIG. In September 2016, the OIG conducted outreach visits to the FTC's East Central (Cleveland, Ohio), Midwest (Chicago, Illinois), and Northeast (New York City, New York) Regional Offices. In meetings with each Regional Office's leadership and staff, OIG staff provided a presentation titled, "The FTC Office of Inspector General: Unique Role, Shared Mission." In the course of its visits, the OIG also highlighted tips for identifying fraud schemes, how to report fraud to the OIG, and whistleblower protection laws. The OIG is planning additional outreach visits in FY 2017.

Enterprise Risk Management

In July 2016, OMB issued revised Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control.* The guidance integrates risk management and internal control activities into an ERM framework "to improve mission delivery, reduce costs, and focus corrective actions towards key risks." The guidance acknowledges the role of internal auditors in complementing agency efforts to identify and detect risks, including fraud risks.

During this reporting period, the OIG increased its proficiency in ERM principles and techniques by attending events sponsored by OMB, the Government Accountability Office (GAO), the Partnership for Public Service, the Association for Federal Enterprise Risk Management (AFERM), and the AFERM Small Agency Community of Practice. The OIG also developed a methodology to identify and assess risks in one of the FTC's Bureaus, focusing on risks affecting core mission areas, without duplicating the areas that FTC management addressed in FY 2016.

> "Successful implementation of this Circular will require Agencies to establish an open, transparent culture that encourages people to communicate information about potential risks and other concerns with their superiors without fear of retaliation or blame. Similarly, agency managers, Inspector Generals and other auditors will have to establish a new set of parameters encouraging the free flow of information about agency risk points and corrective measure adoption. An open and transparent culture results in the earlier identification of risk, allowing the opportunity to develop a collaborative response, ultimately leading to a more resilient government."
>
> **OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016), page ii.**

FISMA Evaluation for FY 2016

The Federal Information Security Modernization Act of 2014 requires an annual evaluation of each agency's information security and privacy program and practices to determine their effectiveness. The evaluation is performed by an independent contractor. It includes evaluating the adequacy of the FTC's information security program and practices for its major systems. Objectives of the FY 2016 evaluation include an assessment of whether FTC governance processes continue to mature and identifies opportunities to increase the effectiveness of FTC information security, privacy, and risk management efforts.

FTC Financial Statement for FY 2016

A financial statement audit is required annually by the Accountability of Tax Dollars Act of 2002. The purpose of the audit is to express an opinion on the financial statement of the FTC for the fiscal year ending September 30, 2016. The audit will also test the internal controls over financial reporting and assess compliance with selected laws and regulations. The audited financial statement will be included in the financial section of the FTC's FY 2016 Agency Financial Report.

Corrective Actions on OIG Recommendations

During this reporting period, FTC Bureaus and Offices continued to make progress in implementing open OIG recommendations. The table in Appendix II identifies significant recommendations described in previous semiannual reports on which corrective action has not been completed. The OIG closed seven recommendations during this reporting period.

Section 5(a)(11) of the Inspector General Act of 1978, as amended, requires a description and explanation of the reasons for any significant revised management decision made during the reporting period. For this reporting period, management did not change its response to any earlier decisions on OIG recommendations.

Investigative Activities

The Inspector General Act of 1978, as amended, authorizes the Inspector General to receive and investigate allegations of employee misconduct as well as fraud, waste, abuse, and mismanagement occurring within FTC programs and operations. Matters of possible wrongdoing are referred to the OIG in the form of allegations or complaints from a variety of sources including FTC employees, other government agencies, and the general public. Reported incidents of possible fraud, waste, abuse, or mismanagement can give rise to administrative, civil, or criminal investigations.

Investigative Summary

The OIG maintains a toll-free Hotline number and a dedicated email address to enable individuals to bring matters to the attention of the OIG on a confidential basis. The toll-free Hotline number, facsimile, email address, and ground mail services are means by which FTC employees, contractors, and the general public may communicate allegations of fraud, waste, abuse, and mismanagement concerning FTC programs and operations to the OIG.

During this reporting period, the OIG received 174 consumer complaints, inquiries, and reports of possible wrongdoing. The OIG redirected 135 complaints to the FTC's Consumer Response Center (CRC) and 3 complaints to the FTC's Freedom of Information Act office. This represents a 66% decrease in complaints received from the last reporting period. The OIG referred complaints under the jurisdiction of FTC programs to the appropriate FTC component for disposition. As described in the following discussion of the OIG Hotline, the decrease in consumer complaints during this reporting period reflects more efficient handling of these complaints through a direct online tool that directs consumers from the OIG's homepages to the CRC, rather than through the OIG Hotline itself.

Streamlining OIG Hotline Complaints

In FY 2016, the OIG continued to review the data accumulated from telephone calls and emails to the OIG Hotline:

- From October 1, 2015 to September 30, 2016, intake of consumer complaints via voicemail and email methods fell from a high of 15 to 20 weekly complaints to a low of three to five.

As a result of recent modifications to OIG Hotline processes, consumers may quickly access the direct channel for filing consumer complaints with the FTC, thereby also improving OIG office efficiency by drastically reducing consumer complaints the OIG received via voicemail and email.

Investigations Closed or Initiated

The OIG closed three investigations during the reporting period, which are highlighted below:

Allegations against Employees of an FTC Organization

The OIG received a series of complaints against several FTC employees in an FTC organization alleging systemic issues of mismanagement, employee misconduct, and privacy violations, which implicated potential violations of federal laws, rules, regulations, and agency policy. Specific allegations included: misuse of contractor personnel, time and attendance abuse, misuse of government property, and contractual improprieties. The OIG reviewed all of the complaints that fell within its jurisdiction and did not substantiate any of the allegations. The allegations regarding matters outside of the OIG's jurisdiction were referred to the appropriate managers for further review and appropriate action.

Allegation of Misuse of Official Position

The OIG received a referral alleging that a veteran lower General Schedule (GS)-level FTC employee, who was in a "high risk" position, as defined by the Office of Personnel Management, had misused the employee's official position "for personal use" in possible violation of federal law and the federal employee Standards of Ethical Conduct regulations. Specifically, the OIG sought to determine whether the employee had sent a letter to another federal agency on official FTC letterhead on behalf of the employee and the employee's relative in order to influence official agency action on a personal matter. The OIG determined that in sending the letter, the employee violated the federal employee Standards of Ethical Conduct regulations governing misuse of public office for private gain, misuse of government property, and misuse of official time. The OIG also determined that certain aspects of the employee's conduct fell outside of the FTC's "limited personal use" exception. At the conclusion of the investigation, the OIG referred the matter to management for appropriate action.

The investigation further determined that the employee had never received ethics training while at the FTC. Additional research determined that other employees at or below the GS-13 grade level who occupy high risk positions, as well as other employees who were hired prior to 2000 when mandatory training for new employees became effective, also had not received any ethics training. The OIG subsequently issued a Management Advisory with recommendations to address these gaps in the agency's Ethics Program.

Allegation of Recording an FTC Employee

The OIG received a complaint that an FTC employee had recorded the employee's annual performance appraisal meeting with the employee's supervisor without the supervisor's approval. The OIG identified several email exchanges between the employee and a third person suggesting that the employee had recorded the meeting, including emails discussing the legal standards for nonconsensual recordings of individuals in

the District of Columbia. The OIG concluded that, while the employee likely recorded the appraisal meeting without the supervisor's consent, the employee's actions recording the meeting did not violate any law, rule, or regulation. In the course of its investigation, despite contradictory statements provided to the OIG, logical inconsistencies, and other evidence, the OIG did not substantiate violations of federal criminal law. However, it was the opinion of the OIG that two FTC employees lacked candor during their OIG interviews. The OIG referred the matter to management for appropriate action.

During this reporting period, the OIG also opened one new investigation into allegations of employee misconduct or wrongdoing.

Preliminary Inquiries

The OIG initiated three preliminaries inquiries. These preliminary inquiries are currently ongoing.

Management Advisories and Referrals

During this reporting period, the OIG issued a management advisory stemming from investigative activity. The management advisory identified gaps in the FTC's Ethics Program and provided recommendations for improvement, which are highlighted below.

Ethics Training for High Risk Positions

An OIG investigation determined that a veteran FTC employee in a "high risk" but relatively low GS-level position under Office of Personnel Management regulations violated multiple provisions of the federal employee Standards of Ethical Conduct regulations by using public office for private gain and using government property and government time for private activities. As a result of that investigation, the OIG issued a Management Advisory to identify opportunities to strengthen the FTC Ethics Program. The Management Advisory recommends that the FTC Office of General Counsel (OGC) consult managers in identifying non-covered employees at or below the GS-13 grade level who occupy high risk positions, and that OGC provide mandatory annual ethics training to this cohort. It also recommends that OGC provide one-time training to FTC employees at or below the GS-13 grade level who were hired prior to 2000, which is when the FTC's new employee ethics training requirement went into effect. Doing so will alert these employees to federal ethics rules, reduce the likelihood of ethics violations, and protect the FTC's integrity and reputation.

Other Activities

Liaison with Other Agencies

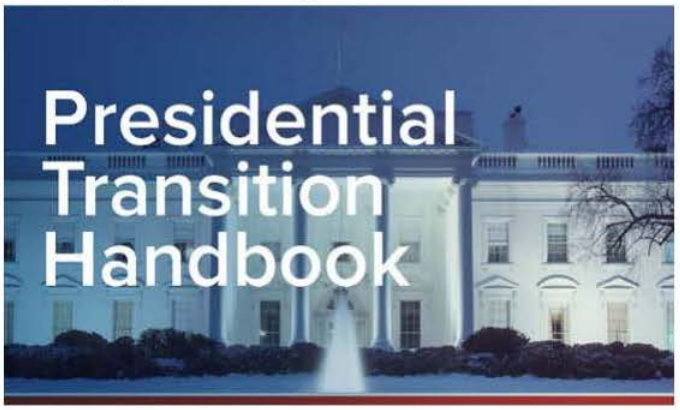
During this reporting period, in conducting audits, investigations, and other activities, the OIG sought assistance from and conferred with other federal agencies, including the following: Office of Government Ethics, Department of Justice, Federal Deposit Insurance Corporation, United States Department of Agriculture, United States Postal Service, Farm Credit Administration, and Social Security Administration (SSA). With respect to SSA, the FTC OIG provided technical assistance to the SSA OIG's Office of Investigations by identifying the opportunity for SSA OIG investigators to obtain a network account on the FTC's Consumer Sentinel Network. Through access to the FTC's consolidated database of consumer complaints, SSA OIG can enhance its consumer protection investigations involving SSA programs.

Activities within the Inspector General Community

The FTC Inspector General is an active participant in the Council of the Inspectors General on Integrity and Efficiency (CIGIE), an independent entity within the Executive Branch comprised of federal Inspectors General. CIGIE's mission is to address integrity, economy, and effectiveness issues that transcend individual Government agencies; and increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General.

Inspectors General and the 2016 Presidential Transition

This semiannual reporting period coincided with the period leading up to the 2016 Presidential election. With significant agency leadership changes on the horizon, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) appointed a working group to identify ways to ensure that the IG community's unique, independent mission was conveyed to the Office of Management and Budget and others involved in implementing the Presidential Transition Act of 2012. The FTC Inspector General served on the CIGIE Presidential Transition Working Group. The Working Group identified the need for a concise, readable document that acquaints Presidential Transition Teams and incoming agency officials with the unique role of Inspectors General and the importance of engaging them during the transition and upon assuming office.



The Working Group presented the Presidential Transition Handbook to CIGIE in September 2016, and it is being used by the Office of Management and Budget, Inspectors General, and others participating in various stages of the Presidential Transition.

The FTC Inspector General also participated in a study conducted under the auspices of the Partnership for Public Service that addressed the opportunity for incoming administration officials to develop productive relationships with the OIG community. In its report published in September 2016, Walking the Line: Inspectors General Balancing Independence and Impact, the Partnership for Public Service recommends that incoming agency leaders understand the unique mission and role of Inspectors General, look to their Inspectors General for insights into the OIG's management challenges reports, and rely on their IGs' assessments of the agency's enterprise risk management efforts under OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.

Other CIGIE Engagements

The Counsel to the Inspector General participates regularly in the Council of Counsels to Inspectors General (CCIG), the Investigations Committee working group, and contributes to the legal and investigative discourse on matters germane to the entire OIG community.

The OIG's Audit Manager participates regularly in the monthly meeting of the Financial Statements Audit Network, a CIGIE subcommittee. She also teaches the financial statement section of the CIGIE Peer Review training offered to the greater OIG community.

The OIG's Program Analyst participates in the bimonthly meetings of the Inspection and Evaluation Roundtable, a CIGIE subcommittee, and contributes to the discourse involving evaluation developments and best practices.

The OIG also participates in CIGIE's Data Analytics Options Working Group, which is reviewing options to achieve comprehensive data analytics across the IG Community.

The OIG worked with FTC management to provide access to FTC facilities for CIGIE training sessions. The OIG appreciates management's support for future planned training sessions.

Significant Management Decisions

Section 5(a)(12) of the Inspector General Act of 1978, as amended, requires that if the IG disagrees with any significant management decision, such disagreement must be reported in the semiannual report to Congress. For this reporting period, there were no significant management decisions made with which the IG disagreed.

Review of Legislation

Section 4(a)(2) of the Inspector General Act of 1978, as amended, authorizes the OIG to review and comment on proposed legislation or regulations relating to the agency or, upon request, affecting the operations of the OIG. The OIG also provides responsive information in response to direct requests from Congress.

During this reporting period, the OIG continued to support the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) October 6, 2015, letter to the Chairman and Ranking Member of the U.S. Senate's Committee on Homeland Security and Governmental Affairs, urging support for the bipartisan substitute amendment to Senate bill S.579, *the Inspector General Empowerment Act of 2015*. The bill addresses the Department of Justice (DOJ) Office of Legal Counsel's (OLC) July 20, 2015, opinion stating that Section 6(a) of the IG Act does not give the DOJ OIG independent access to all records available to DOJ that are needed to perform its oversight functions. Recognizing that the OLC interpretation of the IG Act could have a profound negative impact on the entire OIG community, the FTC OIG continues to support CIGIE efforts to urge Congress to immediately pass legislation affirming the authority of Inspectors General under the IG Act to access independently and without delay all information in an agency's possession that the Inspector General deems necessary to conduct oversight functions.

Access to Information

Inspectors General must have ready access to all agency records, information, or assistance when conducting an investigation or audit. Section 6(b)(2) of the Inspector General Act of 1978, as amended, requires the Inspector General to report to the agency head, without delay, if the Inspector General believes that access to required information, records, or assistance has been unreasonably refused, or otherwise has not been provided. A summary of each report submitted to the agency head in compliance with Section 6(b)(2) must be provided in the semiannual report in accordance with Section 5(a)(5) of the Act. During this reporting period, the OIG did not encounter problems or delays in obtaining assistance or access to agency records.

Other Initiatives

The Inspector General participated in several meetings with OMB officials and representatives of the OIG community to discuss OMB objectives and plans for revising Circular A-123, *Management's Responsibility for Risk Management and Internal Control.* In the first update to the circular in over ten years, the newly revised circular issued in July 2016 incorporates principles of enterprise risk management in the federal government.

In furtherance of our efforts to educate the FTC workforce on the whistleblower protection laws, the OIG collaborated with agency management to register the FTC in the Office of Special Counsel's Section 2302(c) certification program. This program assists agencies in meeting their statutory requirements to inform employees of their rights and remedies under 5 U.S.C. § 2302. The FTC continues to take the necessary steps towards becoming "OSC certified," including educating employees on their whistleblower protections and providing FTC supervisors with interactive whistleblower training.

The FTC OIG joined the CIGIE Data Analytics Options Working Group, which meets to implement the following GAO Recommendation: "to develop a legislative proposal to reconstitute the essential capabilities of the ROC to help ensure federal spending accountability. The proposal should identify a range of options at varying scales for the cost of analytic tools, personnel, and necessary funding, as well as any additional authority CIGIE may need to ensure such enduring, robust analytical and investigative capability for the oversight community." The Working Group devised three options to establish a comprehensive data analytics capability across the IG Community, and then presented the options to the CIGIE Information Technology Committee.

The OIG continues to work with FTC management to improve the policy and practice for tracking OIG recommendations. This process includes regular meetings conducted under the auspices of the FTC Senior Assessment Team (SAT). The SAT is responsible for tracking implementation of all internal control recommendations, including those generated by the OIG. The SAT meetings facilitate regular communication between the OIG, the Executive Director, and FTC Bureaus and Offices about progress made or impediments encountered in implementing OIG recommendations.

Appendix I – Peer Reviews

Peer Review Activity	Results
Peer Reviews conducted by another OIG	During this reporting period, the Architect of the Capitol OIG conducted a peer review of the FTC OIG's investigative operations. The review determined that the FTC OIG's system of internal safeguards and management procedures in effect as of June 9, 2016, is compliant with the CIGIE quality standards and the applicable Attorney General guidelines.
Outstanding recommendations from peer reviews of the FTC OIG	There are no outstanding recommendations from peer reviews of the FTC OIG.
Peer Review conducted by the FTC OIG	The FTC OIG did not conduct any peer reviews during this reporting period.
Outstanding recommendations from peer reviews conducted by FTC OIG	There are no outstanding recommendations from peer reviews conducted by the FTC OIG.

Appendix II – Significant OIG Recommendations Described in Previous Semiannual Reports with Corrective Actions Pending

Independent Assessment of Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2015 (Report Issued: 02/2016)

Recommendations	Total	7
	Mgmt . concurs	7
	Mgmt . non-concurs	--
Status of Recommendations	Closed*	1
	Open	6

Recommendation

- **FY 2015 – 01: Security Management and Governance Structure**
  FTC should continue to evolve FTC Continuous Monitoring Management practices through improvements in governance practices and providing improved documentation and estimating guidance.
- **FY 2015 – 02: FTC Security Policies and Procedures/System Accreditation Borders**
  FTC should continue its review of Accreditation Boundaries for Minor Applications, re-designating those systems that are significant resource investments or have special security considerations as Major Applications.
- **FY 2015 – 03: Certification and Accreditation**
  To support FTC Approval to Operate/Authorization (ATO) decisions, FTC should provide staff applicable NIST guidance, including risk assessment criteria, for reviewing security artifacts provided by other federal organizations that are using the same software or services
- **FY 2015 – 05: Configuration Management**
  FTC should review its CM strategy to ensure that it is addressing CM from the agency perspective and not a single system level approach

* A recommendation is closed if the OIG determines that (1) the corrective action has been taken, or (2) the recommendation is no longer applicable. A recommendation is open if FTC management agrees with the recommendation and is in the process of taking corrective action. Some corrective actions may have been completed by management and are awaiting verification by the OIG.

- **FY 2015 – 06: Identity and Access Management**
  FTC should focus on achieving full compliance with PIB enabled I&A so that compliance is not subject to continuing delay

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

OIG Evaluation of the Federal Trade Commission's Office of the Chief Information Officer (Report Issued: 12/2015)

Recommendations	Total	8
	Mgmt . concurs	8
	Mgmt . non-concurs	--
Status of Recommendations	Closed	3
	Open	5

Recommendations

- **2 IT Governance**
  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 IT Strategic Plan**
  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

- **6 Contract and Project Management**
  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

- **7 IT Strategic Plan and Service Management**
  Publish IT services and 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 IT Staff Recruitment and Development**
  Using the core competency assessment (recommendation 2) and publish 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

Financial Statement Audit for Fiscal Year 2015 Management Letter (Report Issued: 11/2015)

Recommendations	Total	2
	Mgmt . concurs	2
	Mgmt . non-concurs	--
Status of Recommendations	Closed	0
	Open	2

Recommendations

- **ML-15-1**
  OIG recommends the FTC Contracting Officer develop, document and implement internal control procedures to ensure the agency adequately documents the basis for Small Business Act 8 (a) program awards
- **ML-15-2**
  OIG recommends that FTC Financial Operations improve internal control procedures to ensure accounts payable transactions are promptly recorded to maintain their relevance and value to management in controlling operations and making decisions

Independent Assessment of Implementation of the Federal Information Security Management Act for Fiscal Year 2014 (Report Issued: 5/2015)

Recommendations	Total	7
	Mgmt . concurs	7
	Mgmt . non-concurs	--
Status of Recommendations	Closed	4
	Open	3

Recommendations

- **FY 2014 – 03: Infrastructure Documentation**
  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.
- **FY 2014 - 04: Certification and Accreditation**
  FTC should revise its process for determining Minor Applications and documenting security controls.
- **FY 2014 - 06: Contingency Plan**
  FTC should develop a disaster recovery strategy and implementation plan

Financial Statement Audit for Fiscal Year 2013 Management Letter (Report Issued: 03/2014)

Recommendations	Total	5
	Mgmt . concurs	5
	Mgmt . non-concurs	--
Status of Recommendations	Closed	4
	Open	1

Recommendation

- **ML-13-2 Contract Close out**
  We recommend FTC perform the following:
  1. Review and determine the validity of undelivered orders on a semi-annual basis;
  2. Develop policy requiring certification for all open obligation balances that are inactive for more than 12 months.

Independent Assessment of Implementation of the Federal Information Security Management Act for Fiscal Year 2013 (Report Issued: 2/2014)

Recommendations	Total	5
	Mgmt . concurs	5
	Mgmt . non-concurs	--
Status of Recommendations	Closed	4
	Open	1

Recommendation

- **FY 2013 – 07: Identity and Access Management**
  FTC should revise its infrastructure access procedure to restrict access until background screening is completed per FTC policy.

Appendix III – Inspector General Issued Reports with Questioned Costs

	Number	Questioned Costs (dollar value)	Unsupported Costs(dollar value)
A. For which no management decision has been made by the commencement of the reporting period	0	0	0
B. Which were issued during the reporting period	0	0	0
Subtotals (A+B)	0	0	0
C. For which a management decision was made during the reporting period	0	0	0
i. dollar value of the disallowed costs	0	0	0
ii. dollar value of the cost not disallowed	0	0	0
D. For which no management decision was made by the end of the reporting period	0	0	0
E. Reports for which no management decision was made within six months of issuance	0	0	0

Appendix IV – Inspector General Issued Reports with Recommendations that Funds be Put to Better Use

	Number	Dollar Value
A. For which no management decision has been made by the commencement of the reporting period	0	0
B. Which were issued during the reporting period	0	0
C. For which a management decision was made during the reporting period	0	0
i. dollar value of recommendations that were agreed to by management	0	0
• based on proposed management actions	0	0
• based on proposed legislative action	0	0
ii. dollar value of recommendations that were not agreed to by management	0	0
D. For which no management decision was made by the end of the reporting period	0	0
E. Reports for which no management decision was made within six months of issuance	0	0

Appendix V – Inspector General Act Reporting Requirements Index

IG Act Reference	Reporting Requirements	Pages(s)
Section 4(a)(2)	Review of legislation and regulations	20
Section 5(a)(1)	Significant problems, abuses and deficiencies	none
Section 5(a)(2)	Recommendations with respect to significant problems, abuses and deficiencies	6-17
Section 5(a)(3)	Prior significant recommendations on which corrective actions have not been made	23-28
Section 5(a)(4)	Matters referred to prosecutive authorities	15-16
Section 5(a)(5)	Summary of instances where information was refused	none
Section 5(a)(6)	List of reports by subject matter, showing dollar value of questioned costs and funds put to better use	none
Section 5(a)(7)	Summary of each particularly significant report	6-11
Section 5(a)(8)	Statistical tables showing number of reports and dollar value of questioned costs	29
Section 5(a)(9)	Statistical tables showing number of reports and dollar value of recommendations that funds be put to better use	30
Section 5(a)(10)	Summary of each report issued before this reporting period for which no management decision was made by the end of the reporting period	none
Section 5(a)(11)	Significant revised management decisions	none
Section 5(a)(12)	Significant revised management decisions with which the Inspector General disagrees	none
Section 5(a)(14)	Peer reviews conducted by another OIG	22

IG Act Reference	Reporting Requirements	Pages(s)
Section 5(a)(15)	Outstanding recommendations from peer reviews of the OIG	none
Section 5(a)(16)	Outstanding recommendations from peer reviews conducted by the OIG	none

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.