FEDERAL TRADE COMMISSION

OIG

10.01.16

—

03.31.17

SEMIANNUAL REPORT TO CONGRESS

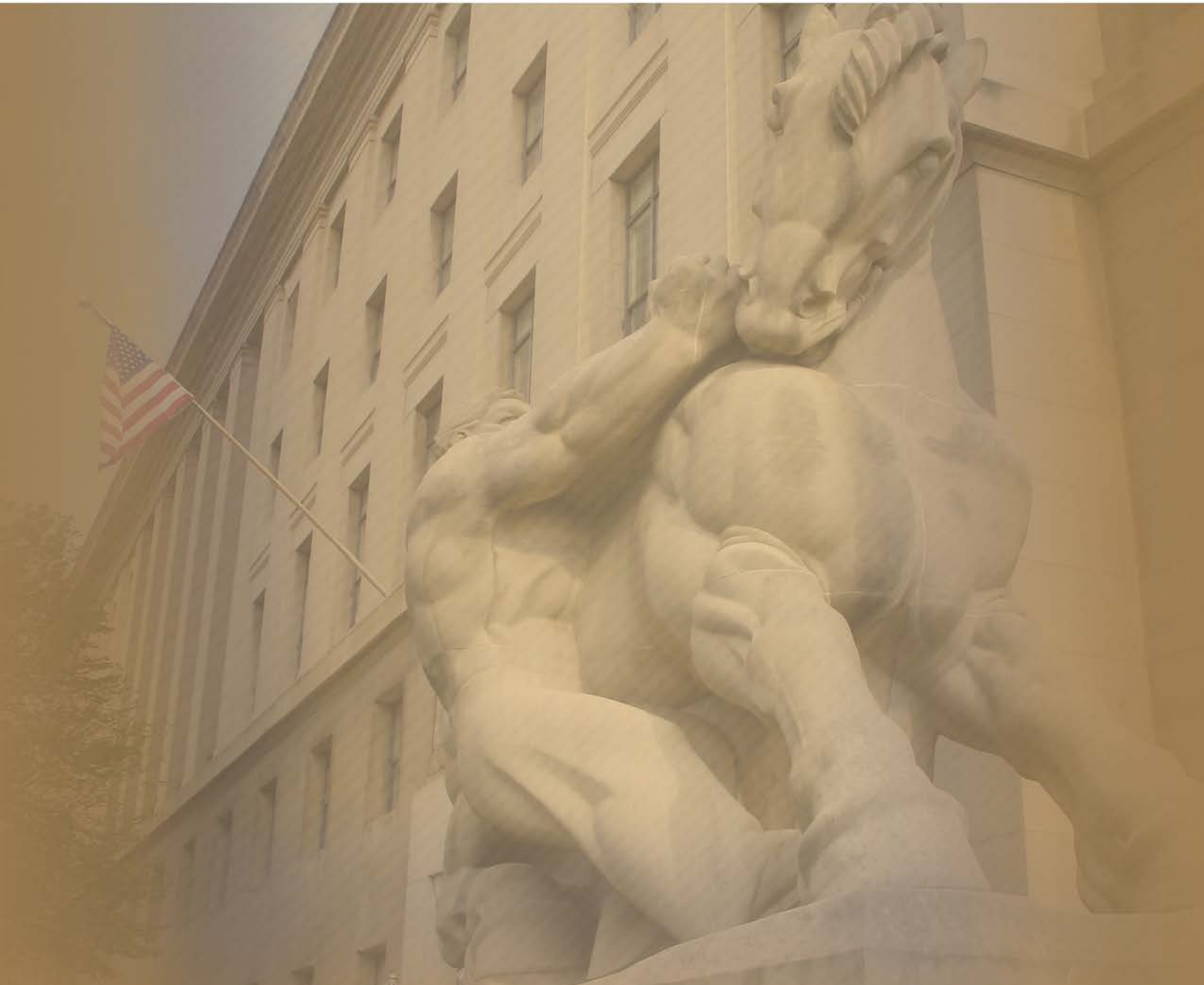


Table of Contents

Message From the Inspector General 2

About the FTC Office of Inspector General 4

Introduction and Definitions 5

Evaluations, Audits, and Related Activities 7

Completed Reports 7

Ongoing Work 12

Corrective Actions on OIG Recommendations 14

Investigative Activities 15

Investigative Summary 15

Investigations Closed or Initiated 16

Preliminary Inquiries 16

Management Advisories and Referrals 16

Other Activities 17

Liaison with Other Agencies 17

Activities within the Inspector General Community 17

Significant Management Decisions 18

Review of Legislation 18

Access to Information 19

Other Initiatives 19

AppendixI–Peer Reviews 20

Appendix II – Significant OIG Recommendations Described in Previous Semiannual Reports with Corrective Actions Pending 21

Appendix III – Inspector General Issued Reports with Questioned Costs 28

Appendix IV – Inspector General Issued Reports with Recommendations that Funds be Put to Better Use 29

Appendix V – Summaries of each Audit, Inspection, and Evaluation Report Issued before Commencement of the Reporting Period' 30

Appendix VI – OIG Investigative Activity During this Reporting Period 31

Appendix VII – Completed OIG Investigations Involving a Senior Government Employee Where Allegations of Misconduct Were Substantiated..... 32

Appendix VIII – Substantiated Instances of Whistleblower Retaliation 33

Appendix IX – Attempts by the Agency to Interfere with the Independence of the OIG..... 34

Appendix X – Closed OIG Matters Not Disclosed to the Public 35

Appendix XI – Inspector General Act Reporting Requirements Index 36

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, 2016, through March 31, 2017.

During this reporting period, the OIG completed its independent evaluation of the FTC's Information Security Program and Practices for Fiscal Year (FY) 2016. The evaluator determined that the FTC security environment continues to be strong and robust relative to its ability to protect its information assets, and did not identify any weaknesses that were specific to the FTC Privacy controls. However, the evaluator identified concerns with the agency's IT Strategy and Transition Plan, approved on September 30, 2016. Specifically, the evaluation identified the need to establish enterprise-level security and privacy control baselines, risk management procedures, acquisition plans, and project management practices that ensure the delivered modernization components meet FTC needs, can be effectively managed, and are delivered on schedule and within budget.

We issued the Financial Statement Audit for FY 2016, in which the FTC received an unmodified opinion for the 20th consecutive year. We issued the associated Management Letter, which contains findings and recommendations to improve the agency's internal controls and operating efficiencies.

Our investigative work included completion of an investigation of allegations that a former senior FTC official may have violated 18 U.S.C. § 207(c), one of the federal criminal conflict of interest statutes, which restricts post-employment activities by senior level officials. The investigation concluded that despite receiving multiple briefings on these restrictions before onboarding, during the former senior FTC official's tenure, and upon leaving the agency, the former senior official contacted agency personnel on behalf of a client of the law firm with which the former senior official was then affiliated, within eight months of resigning from the FTC, to request official action. The agency employee contacted by the former senior official conferred with an attorney in the FTC Office of General Counsel, who advised that the meeting should not be scheduled in light of the post-employment bar. The meeting did not take place. We referred our investigative findings to the Department of Justice, which declined prosecution.

To acquaint FTC regional directors and staff with the unique role and mission of the OIG; conduct proactive fraud, waste, and abuse training; and learn about unique challenges of FTC regional offices, we conducted outreach visits to two regional offices: the Southeast (Atlanta, Georgia) and Southwest (Dallas, Texas) Regional Offices. We are grateful for the useful and candid exchanges we have had with our colleagues in regional offices.

The OIG reviewed management's efforts to comply with the Digital Accountability and Transparency Act of 2014 (DATA Act). The objective was to determine if management is on track to meet the DATA Act requirements by the May 9, 2017, deadline. The attestation review found that the FTC encountered challenges related to staffing resources and the Federal Shared Service Provider's capacity to meet DATA Act requirements. Nonetheless, the OIG did not identify any indications that the FTC will not meet the DATA Act reporting requirements and deadline.

The OIG launched a promising cross-OIG community initiative to support OIG investigations of consumer fraud complaints, such as identity theft, imposter scams, and redirection of government benefit scams. Last year, consumers reported losing over $700 million in fraud; these scams often prey on vulnerable populations, such as the elderly and members of the military. I am delighted by our partnership with the FTC Bureau of Consumer Protection and, to date, four other Offices of Inspector General, and our focus on boosting the use and value of the FTC's Consumer Sentinel Network. The network is a nationwide repository of over 13 million consumer complaints accessible to over 2,300 federal, state, local, and international law enforcement agencies, who use it to build important consumer fraud investigations. This initiative furthers one of the principal objectives of the Inspector General Empowerment Act of 2016 – which was signed into law during this reporting period: to identify issues that could be better addressed through greater coordination among, and cooperation between, individual Offices of Inspector General.

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 sincere appreciation to former FTC Chairwoman Edith Ramirez, who resigned from the Commission in February 2017, for her steadfast support of the OIG mission. As the FTC transitions to new leadership, I also thank Acting Chairman Maureen Ohlhausen, Commissioner Terrell McSweeny, agency management and staff, and the Congress for their sustained support to the OIG mission.

About the FTC Office of Inspector General

OIG Mission

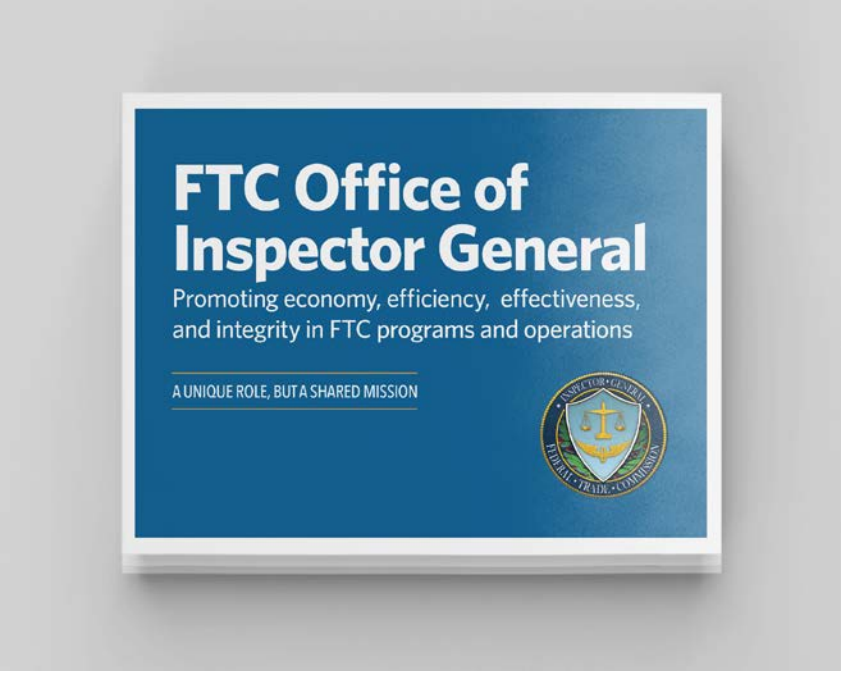
To promote economy, efficiency and effectiveness, and to detect and prevent waste, fraud, abuse, and mismanagement in the agency's operations and programs.

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 Federal Trade Commission.

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, and abuse, 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 on the OIG website via a specialized link to the FTC Consumer Response Center 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 other 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 is operating under a Continuing Resolution and has an operating budget of $1,314,000 for FY 2017.

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 OIG activity. Management advisories typically contain recommendations to address OIG findings.

Evaluations, Audits, and Related Activities

Completed Reports

During this period, the OIG issued the evaluation of the FTC's Information Security Modernization Act Program and Practices for Fiscal Year (FY) 2016. We issued three audit reports: the Financial Statement Audit for FY 2016, its associated Management Letter, and a Readiness Review of the FTC's Digital Accountability and Transparency Act (DATA Act) implementation.

FY 2016 Management Challenges

In our FY 2016 Management Challenges report, we identified the following as the most significant management challenges facing the FTC:

1. Securing the Agency's Information Systems and Networks from Destruction, Data Loss, or Compromise
2. Accelerating Maturing of the Agency's Information Technology Governance Process
3. Improving Acquisition Planning and Contract Management
4. Acquiring Employee Suitability Determinations

FY 2016 Evaluation of the FTC'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 TACG, LLC to perform the independent FISMA evaluation. The primary objective of this year's FISMA evaluation is to assess the status of the FTC information and privacy programs at September 30, 2016, as required under FISMA and the *FY 2016 Inspector General Federal Information Security Modernization Act Reporting Metrics V1*, developed by the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE). On September 30, 2016, the FTC adopted a Strategy and Transition Plan, an aggressive, multi-year strategy to design, acquire, and implement an enterprise architecture that emphasizes use of cloud technologies to expand the services available to its workforce while improving information security and resilience; ensuring compliance with FISMA, the Privacy Act, and other applicable law, policy, standards, and guidelines; and remaining within budget and staffing constraints.

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

CyberScope metrics show that FTC has substantially met the Cross-Agency Priority (CAP) goals established by OMB and DHS for agency information systems. In those areas where FTC has not met CAP goals, there are compensating countermeasures that minimize the risk of information compromise. Our independent assessment of the FTC information security and privacy environments is consistent with the information provided through the CyberScope reporting. However, as stated previously in the OIG's FY 2014 and FY 2015 FISMA reports, the FTC's information security and privacy programs continue to be stressed, requiring significant manual activity; and with the modernization effort, the stress will be increased, especially during the transition period.

In its previous FISMA reporting, the OIG recommended improvements in FTC IT governance, asset management, risk management, and contractor management. While the FTC made significant efforts to improve its governance practices, modernization planning, and acquisition documents provided as of September 30, 2016, it must continue improvement efforts so that it demonstrates the disciplined planning necessary for compliance with Federal Acquisition Regulation principles, OMB, and FTC requirements and guidance for such a complex activity and its documents demonstrate a risk-based approach where information security, privacy, and performance risks are considered and appropriate mitigations are evaluated and planned. FTC progress has been hampered by frequent turnover in the position of the Chief Information Officer and the associated disruptions due to reorganizations and changes in management focus. Further, these efforts are hampered by inconsistent adherence to FTC policies and procedures and lack of documentation. The FTC hired a new Chief Information Officer in July 2015 who is leading a reorganization of all IT resources, including strategy and planning, documentation, contract management, cyber security, and risk management.

Overall, the FY 2016 evaluation determined that the FTC security environment continues to be strong and robust relative to its ability to protect its information assets. The OIG did not identify any weaknesses that were specific to the FTC Privacy controls.

The OIG identified several areas for improvement and made the following recommendations to improve the FTC's information security program.

1. The FTC should document its system inventory management system and validate the system, database, and management procedures, at least on an annual basis, as a trusted FTC Information Security Continuous Monitoring (ISCM) component under configuration control.

2. The FTC should complete its evaluation of its system boundaries as it completes its Department of Justice *Cyber Security Assessment and Management* implementation. FTC should eliminate use of the Minor Application designation and document leveraged/common controls in accordance with National Institute of Standards and Technology (NIST) Risk Management Framework guidance and ensure that all FTC systems are covered by an FTC Authority to Operate (ATO), either specific to the system or under a related system.
3. The FTC should implement a formal procedure for documenting risk-based decisions as part of the FTC risk management program.
4. The FTC should implement a formal risk management program that addresses the requirements of OMB Circulars A-123 and A-130 and the guidance contained in NIST Special Publications 800-30, 800-37, and 800-39. The FTC should conduct risk analyses for its IT Modernization Initiative.
5. The FTC should structure modernization activities for acquiring major IT investments as useful segments that can be independently planned, acquired, and monitored.
6. The FTC should implement a fully compliant ISCM as described in its ISCM Plan in FY 2013 and its ISCM Strategy, dated November 2014.
7. The FTC should revise its Plan of Action and Milestones ("POA&M") process and content to ensure it meets OMB information requirements (e.g., all security weaknesses found, and in need of remediation, during any assessment done by, for, or on behalf of the agency, including Government Accountability Office (GAO) audits, financial system audits, and critical infrastructure vulnerability assessments) and can be an effective, authoritative, agency-wide management tool.
8. The FTC should develop viable contingency plans for the headquarters data center and hosted applications. Plans should be tested to ensure viability and ensure staff are trained to execute them. Contingency plans should clearly define actions to be performed, and individuals responsible for plan activation and other critical decisions should be identified.

Management concurred with the eight recommendations and will submit action plans within 60 days to address them.

FY 2016 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.

For the 20th 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, 2016, Brown & Company found:

- The Fiscal Years 2016 and 2015 financial statements were presented fairly, in all material respects, in accordance with U.S. generally accepted accounting principles,
- One material weakness in internal control over financial reporting, and
- No reportable instances of noncompliance with applicable provisions of laws, regulations, and contracts tested

Brown & Company identified the following material weakness

- Improved Accounting and Controls are Needed Over Receivership Receivables

Although the FTC had implemented the process of documenting the recording of accounts receivable for the estimate of proceeds from the sale of assets by receiverships, the estimate was not recorded for the financial statements as of June 30, 2016.

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 OMB audit guidance.

Management Letter from the FY 2016 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 to be reflected in the auditor's opinion report. 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:

- Improved accounting and controls are needed over disbursements to correctly identify Contract Line Item Numbers (CLIN)
- Improved accounting and controls are needed over the quarterly reporting of interest receivable

Management concurred with all recommendations and provided detailed steps to implement corrective actions. We commend management for addressing previous recommendations that enabled the OIG to close all three recommendations from prior financial statement audits.

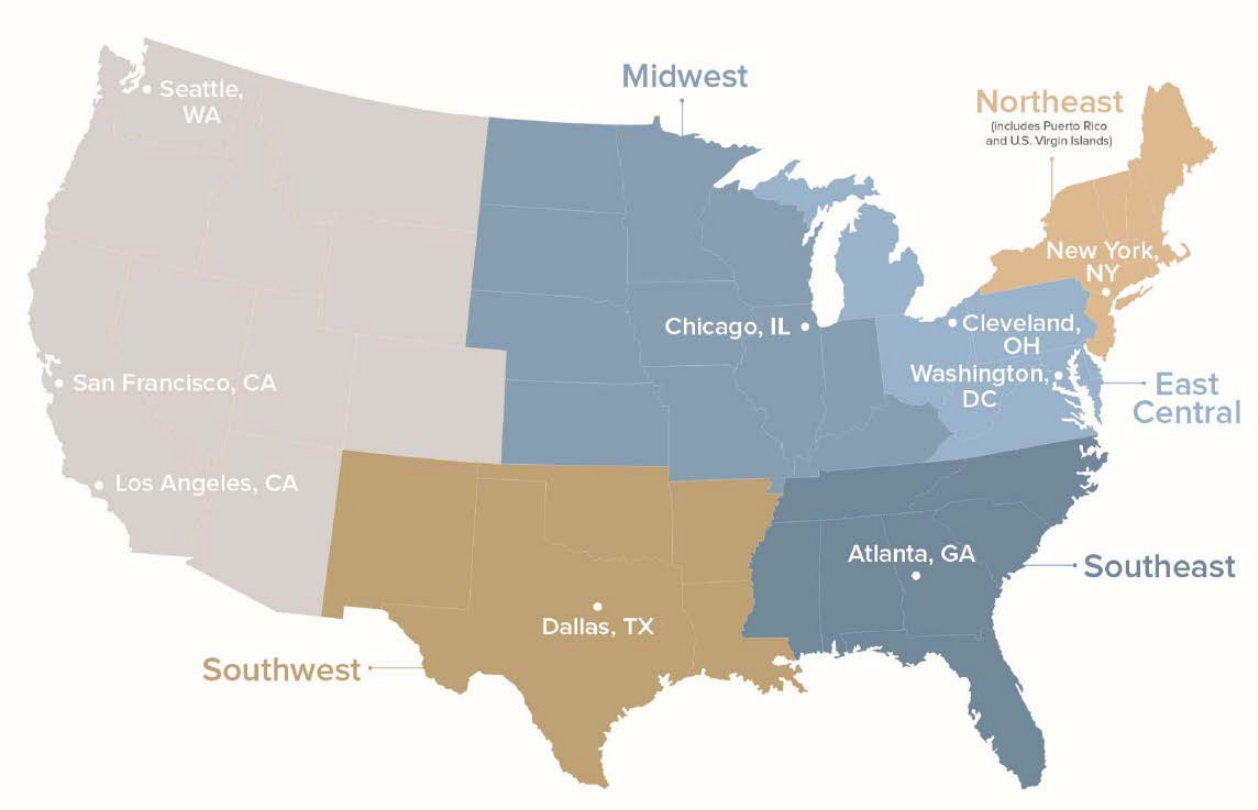
Independent Readiness Review of the FTC's Implementation of the Digital Accountability and Transparency Act of 2014

The OIG reviewed management efforts to implement the Digital Accountability and Transparency Act of 2014 (DATA Act). The review was conducted in accordance with attestation standards established by the GAO and the American Institute of Certified Public Accountants. As part of the oversight of the DATA Act implementation, a majority of the OIG community conducted reviews to determine if agencies are on track to meet the DATA Act requirements and reporting deadlines. The DATA Act expands the federal spending information required to be submitted by agencies to usaspending.gov; mandates that information be easily searchable and downloadable; and requires the establishment of data standards to generate uniform agency data that are consistent and comparable. The DATA Act guidance requires agencies to report spending activity by May 9, 2017, in accordance with standards developed and approved by the Office of Management and Budget (OMB) and the Department of the Treasury.

The OIG reviewed management's efforts to comply with the Department of Treasury/OMB DATA Act Playbook as of January 2017. The objective was to determine if management is on track to meet the DATA Act requirements by the May 9, 2017, deadline. The review found that the FTC encountered challenges related to staffing resources and the Federal Shared Service Provider's capacity to meet DATA Act requirements. Nonetheless, the OIG did not identify any indications that the FTC will not meet the DATA Act reporting requirements and deadline.

Ongoing Work

Outreach to FTC Regional Offices



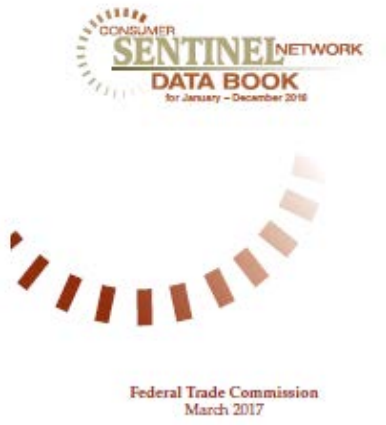
During this reporting period, the OIG continued its proactive initiative, launched earlier in FY 2017, to acquire a greater understanding of the mission, role, and special challenges of the FTC's regional offices and to acquaint these offices with the unique role of the OIG. In January 2017, the OIG conducted outreach visits to the FTC's Southeast (Atlanta, Georgia) and Southwest (Dallas, Texas) Regional Offices. In meetings with each regional office's leadership and staff, OIG staff provided an educational presentation and highlighted tips for identifying fraud schemes, reporting fraud to the OIG, and also educated employees on the whistleblower protection laws. The OIG is planning additional outreach visits to the FTC's Northwest (Seattle, Washington) and Western (San Francisco and Los Angeles, California) Regional Offices.

Cross-Community OIG Consumer Fraud Initiative

During this reporting period, the OIG collaborated with the FTC Bureau of Consumer Protection and four Offices of Inspector General to identify opportunities to boost OIG investigations of consumer fraud. The need to use all available tools in these fraud investigations is compelling, as consumer reporting of identity theft, government imposter scams, and redirection of government benefit scams are on the increase. For example, according to the FTC's Consumer Sentinel Network Data Book for 2016 (Data Book), consumers

lodged 406,500 government impostor complaints in 2016, up from 353,000 in 2015 – a 15 percent increase, which included imposters who claimed to be FTC officials or employees. Moreover, for the first time, imposter scams surpassed identity theft complaints as the second highest category of consumer complaints in 2016. These scammers often victimize particular populations, including the elderly, immigrant communities, and military consumers.

The initiative focuses on extending the use and value of the FTC's Consumer Sentinel Network (CSN) – a secure online database housing over 13 million consumer complaints dating from calendar year 2012 through calendar year 2016. CSN is a unique investigative tool that provides law enforcement members with access to millions of consumer complaints. Based on the premise that sharing complaint information can make law enforcement even more effective, CSN allows members to access consumer complaints submitted directly to the FTC, as well as to complaints shared by over 40 data contributors, including the Consumer Financial Protection Bureau, over 20 State Attorneys General, and all North American Better Business Bureaus. Over 2,300 federal, state, local, and international law enforcement agencies have access to CSN, and hundreds of individual members access the system each week.



The objectives of the OIG's ongoing collaboration are to 1) ensure that the OIG community is aware of and uses the CSN; and 2) identify opportunities to strengthen the Network's database with consumer complaints lodged with other federal agencies. During this reporting period, the OIG facilitated meetings between the CSN Program Manager and investigators from the OIGs at the Departments of Treasury and Health and Human Services. The OIG plans to facilitate such meetings with OIGs from the Department of Housing and Urban Development, the Department of Veterans Affairs, the Social Security Administration, and other OIGs who investigate different types of consumer fraud scams. The CSN Program Manager is providing tutorials on the CSN's upgraded tools for searching common schemes, identifying complainants and witnesses, and isolating key fraud indicators, such as provider names and other information used to fraudulently obtain government benefits or perpetrate other consumer scams.

This cross-OIG community initiative furthers one of the principal objectives of the Inspector General Empowerment Act of 2016 (IGEA) – which was signed into law during this reporting period. Section 4 of the IGEA calls upon the Inspectors General to identify issues that could be better addressed through greater coordination among, and cooperation between, individual Offices of Inspector General, and to identify the best practices that can be employed by OIGs to increase coordination.

Enterprise Risk Management

On July 15, 2016, OMB issued an update to Circular A-123 requiring federal agencies to implement Enterprise Risk Management (ERM) to better ensure their managers are effectively managing risks that could affect the achievement of agency strategic objectives. Circular A-123 identifies sources for agencies in completing their risk profiles, including reviewing and incorporating results from existing documentation such as OIG audit findings and OIG's Annual Report on Management Challenges. Circular A-123 encourages agency managers, Inspectors General, and other auditors 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. On July 29, 2016, the Chief Financial Officers Council and the Performance Improvement Council released the *Playbook: Enterprise Risk Management for the U.S. Federal Government* (Playbook). The Playbook includes, in its list of sources for identifying risks, the OIG Management Challenges and audits, and the outstanding corrective actions associated with those audits. The Playbook states that one of the major duties of the agency's Chief Risk Officer is to foster close ties with the OIG.

The FTC's Senior Assessment Team provides leadership and oversight of the FTC's internal control program, the goal of which is to ensure that internal controls are commensurate with identified risks and results-oriented management. The Inspector General and OIG staff periodically attend the Senior Assessment Team meetings to understand the agency's efforts to create risk profiles that are due for submission to OMB on June 2, 2017, and to witness the internal controls identification and resolution cycle. Additionally, OIG staff are increasing their proficiency in ERM principles by attending periodic training sessions and webinars. In the remaining months of FY 2017, the OIG will develop an ERM Framework to guide the identification and use of ERM principles in the OIG's own planning and operational cycles, and to lay the groundwork for assessing management's initial ERM efforts in FY 2018.

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 eleven 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 160 consumer complaints, inquiries, and reports of possible wrongdoing. The OIG redirected 154 complaints to the FTC's Consumer Response Center (CRC). No complaints were forwarded to the FTC's Freedom of Information Act office. This represents an 8% 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 an online tool that directs consumers from the OIG's homepage to the CRC, rather than through the OIG Hotline.

OIG Hotline Complaints

The OIG continued to review FY17 data accumulated from telephone calls and emails to the OIG Hotline:

- From October 1, 2016 to March 31, 2017, the weekly intake of consumer complaints via voicemail and email methods remained at a consistently low rate 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 receives via voicemail and email.

Investigations Closed or Initiated

The OIG closed one investigation during the reporting period, highlighted below:

Alleged Violation of the Post-Employment Restrictions by a Former Senior FTC Official

The OIG received a referral that a former senior FTC official may have violated the post-employment criminal conflict of interest restrictions set forth in 18 U.S.C. § 207(c). The post-employment statute prohibits certain senior government employees such as the former senior FTC official from contacting their former agencies knowingly and with the intent to influence official action within a year of departure.

The OIG established that the former senior official was briefed about the post-employment restrictions of 18 U.S.C. § 207(c) and other ethical obligations upon entering on duty at the FTC. The OIG further found that the former senior official was briefed on the post-employment restrictions at periodic ethics training and again upon departure from the FTC.

The investigation determined that, approximately eight months after the former senior official resigned from the FTC, the former senior official contacted an FTC employee and proposed a meeting at the FTC on behalf of a client of the law firm with which the former senior official was then affiliated. The OIG further determined that the proposed meeting did not take place after the FTC employee sought ethics guidance from the FTC Office of General Counsel and was advised that the meeting should not be scheduled because of the post-employment conflict of interest restrictions.

The OIG completed its investigation and referred the matter to the Department of Justice, which declined prosecution. Following the declination, the OIG asked the former senior official to submit to a voluntary interview; the former senior official declined our request. The OIG provided a report to management, and the matter is now closed.

Preliminary Inquiries

The OIG closed seven preliminary inquiries during the reporting period. We did not initiate any new preliminaries inquiries.

Management Advisories and Referrals

During this reporting period, the OIG did not issue any management advisories or referrals stemming from investigative activity.

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 and OIGs, including the Department of Justice Public Integrity Section, the U.S. Attorney's Office for the District of Columbia, the Office of Government Ethics, the Federal Reserve Board OIG, the Pension Benefit Guaranty Corporation OIG, and the Interagency Ethics Council.

Activities within the Inspector General Community

The 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. The FTC Inspector General currently serves on the CIGIE Integrity Committee, which is charged by the Inspector General Act of 1978, as amended, with receiving, reviewing, and referring for investigation allegations of wrongdoing by Inspectors General or their direct reports.

The 2016 Presidential Transition

Following the presidential election in November 2016, the OIG prepared briefing materials for representatives of the President Elect assigned to the FTC, and the Inspector General met with them to acquaint them with the OIG mission, identify major management challenges facing the FTC, and respond to requests for information that would assist their transition efforts.

Other CIGIE Engagements

The Counsel to the Inspector General participates regularly in the Council of Counsels to the Inspectors General, the Investigations Committee, and the CIGIE Cross-Cutting Projects 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 subcommittee of the CIGIE Inspections and Evaluations Committee, and contributes to the discourse involving evaluation developments and best practices.

The OIG's Auditor and Program Analyst participate in the monthly Federal Audit Executive Council Data Act Working Group meetings and required training sessions.

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 enable the OIG to host CIGIE Integrity Committee meetings. The OIG appreciates management's support for these efforts.

Significant Management Decisions

Section 5(a)(12) of the Inspector General Act of 1978, as amended, requires that if the Inspector General 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 Inspector General disagreed.

Review of Legislation

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

During this reporting period, Congress passed the Inspector General Empowerment Act of 2016 (IGEA) – landmark legislation that will protect the independence and effectiveness of Inspectors General for years to come. A key provision in the Act affirms that Inspectors General are authorized to have timely access to all available agency records, reports, audits, reviews, documents, papers, recommendations, or other materials related to their oversight functions. The IGEA also requires the reporting of critical issues ripe for collaboration among multiple OIGs.

In his remarks upon congressional passage of the IGEA, CIGIE chair and Department of Justice Inspector General Michael E. Horowitz stated in a December 12, 2016, press release:

> [p]assage of the IG Empowerment Act enhances the IGs' ability to fight waste, fraud, abuse, and misconduct, protects whistleblowers who share information with IGs, increases government transparency, and bolsters the public's confidence in the independence of IGs. For these reasons,

the Act is an important milestone for good government. The Inspector General community is grateful to the sponsors and co-sponsors of this Act and all those who stood up for independent oversight.

Access to Information

Inspectors General must have ready access to all agency records, information, or assistance when conducting an investigation or audit. Section 6(c)(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(c)(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

In furtherance of our efforts to educate the FTC workforce on the whistleblower protection laws, the OIG continued to collaborate with management with respect to 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. Management 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 OIG continues to work with management to improve the policy and practice for tracking OIG recommendations. This process includes quarterly meetings between the OIG and 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.

The OIG took a significant step in maturing the OIG's business process for closing OIG recommendations when, in collaboration with management, it issued a revised protocol for closing OIG recommendations. This revised protocol will contribute to greater agency-wide understanding of how the OIG develops and tracks recommendations, and will foster improved collaboration with management to ensure OIG recommendations are effectively scoped and timely implemented.

Appendix I – Peer Reviews

Peer Review Activity	Results
Peer Reviews conducted by another OIG	There were no peer reviews conducted by another 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 Reviews 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

Management Advisory: Strengthening the FTC Ethics Program by Extending Mandatory Annual Ethics Training to Employees at or Below the GS-13 Grade Level Who Occupy High Risk Positions (Issued: 09/2016) (Link to Report)

Recommendations	Total	3
	Mgmt. concurs	3
	Mgmt. non-concurs	--
Status of Recommendations	Closed[1]	0
	Open	3

Recommendation

- **FTC Employees at the GS-13 Grade Level and Below in High Risk Positions**
  Certain employees at the GS-13 grade level and below who occupy "high risk" positions do not receive annual ethics training. To address an area of vulnerability and risk, annual ethics training should be mandatory for such employees.
- **FTC Employees at the GS-13 Grade Level Hired Prior to 2000**
  Certain employees at or below the GS-13 grade level hired prior to 2000 likely have never received new employee ethics training, regardless of their position risk designations. This is due to the fact that the regulatory requirement to provide new employee ethics training went into effect in March 2000. Therefore, the OIG recommended the provision of a one-time training to those employees at or below the GS-13 grade level hired prior to 2000 who never received mandatory ethics training at new employee orientation, regardless of their position risk designations.
- **Inform FTC Work Force of the Modification to the OGC Ethics Program**
  We recommend that OGC use its Intranet web site, the FTC Daily, the Ethicist, and other work force communications to inform the work force of the modification to the OGC Ethics Program.

[1] 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.

Opportunities Exist to Accelerate Maturation of the FTC's Information Governance Practices (Report Issued 09/2016) (Link to Report)

Recommendations	Total	15
	Mgmt. concurs	15
	Mgmt. non-concurs	--
Status of Recommendations	Closed	0
	Open	15

Recommendations

- **1: Capital Planning and Investment Controls (Updated BCA)**
  Complete applicable Business Case Analysis (BCA) elements, including a description of security requirements and how they will be met, functional requirements document, Return on Investment 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 Federal Acquisition Regulation requirements.
- **2: Capital Planning and Investment Controls**
  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: Project Management (SOPs and Project Monitoring)**
  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: Project Management (Cost Estimating)**
  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: Risk Management**
  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: Project Management (Project Escalation)

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: Contract Management

Terminate efforts to remedy deficiencies in the current e-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: Requirements Development

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: Application Documentation/Testing

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: Systems Testing

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: Contract Management

Align an 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: Capital Planning and Investment Control

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 them to business needs.

◃ 13: System Security Plan

Develop a System Security Plan for the mobile device project based on NIST Special Publication 800-53 rev 4, *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: Contract Management**
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: Controlled Unclassified Information (CUI)**
Identify systems that may include 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 security 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 FTC remains current with the direction and status of CUI program requirements.

Ensuring Preservation of Emails Pertaining to Contract Administration (Report Issued 03/2016)

Recommendations	**Total**	4
	Mgmt. concurs	4
	Mgmt. non-concurs	--
Status of Recommendations	**Closed**	3
	Open	1

Recommendations

◃ **1:** Advise CORs at the next training opportunity on April 14, 2016, and in subsequent periodic training and written guidance, that they are required to preserve pertinent emails as described in this memo.

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

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

Recommendations

- **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 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 (CM)**
  FTC should review its CM strategy to ensure that it is addressing CM from the agency perspective and not a single system level approach
- **FY 2015 – 06: Identity and Access (I&A) Management**
  FTC should focus on achieving full compliance with Personal Identity Verification (PIV) enabled I&A so that compliance is not subject to continuing delay and PIV compliance is maintained as new technologies and contracting approaches are added as part of FTC's modernization efforts.
- **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

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

Recommendations	Total	6
	Mgmt. concurs	6
	Mgmt. non-concurs	--
Status of Recommendations	Closed	3
	Open	3

Recommendations

- **FY 2014 – 03: Infrastructure Documentation**
  FTC should take appropriate action to ensure completion of an appropriate 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

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

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 costs 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 – Summaries of each Audit, Inspection, and Evaluation Report Issued before Commencement of the Reporting Period[2]

Fiscal Year	Number of Reports with Unimplemented Recommendations	Number of Unimplemented Recommendations	Dollar Value of Aggregate Potential Cost Savings
FY 2016	4	25	0
FY 2015	1	3	0
FY 2014	1	1	0
Prior to FY 2014	0	0	0
TOTAL for All Fiscal Years	6	29	0

[2] Per section 5(a)(10) of the Inspector General Act of 1978, as amended, there are no reports for which a management decision had not been made, nor for which establishment comment was not returned within 60 days of providing the report to the establishment. Additionally, there are no cost savings associated with the recommendations in this table.

Links to completed audit and evaluation reports are provided in Appendix II and are available on the FTC OIG website at https://www.ftc.gov/about-ftc/office-inspector-general/oig-reading-room/reports-correspondence.

Appendix VI – OIG Investigative Activity During this Reporting Period[3]

	Number
A. Number of Investigative reports issued	1
B. Number of persons referred to DOJ for criminal prosecution	2
C. Number of persons referred to State and Local authorities for criminal prosecution	0
D. Number of criminal indictments and criminal informations resulting from any prior referrals to prosecutive authorities	0

[3] These statistics are based on the number of investigative reports issued during this semiannual reporting period; the number of persons referred to federal, state, or local authorities for criminal prosecution during this semiannual reporting period; and the number of criminal indictments/informations that occurred during this semiannual reporting period resulting from referrals made during the current and previous reporting periods.

Appendix VII – Completed OIG Investigations Involving a Senior Government Employee Where Allegations of Misconduct Were Substantiated[4]

Number of Investigations Involving a Senior Government Employee where Allegations of Misconduct were Substantiated
There were no investigations involving a senior government employee where allegations of misconduct were substantiated.

	Detailed Description
A. Facts and Circumstances of the investigation	N/A
B. Status and disposition of the matter, including, if referred to DOJ, the date of referral; and, if declined by DOJ, the date of declination	N/A

[4] The Inspector General Empowerment Act of 2016 defines "senior government employee" as – "(A) an officer or employee in the executive branch (including a special Government employee as defined in section 202 of title 18, United States Code) who occupies a position classified at or above GS–15 of the General Schedule or, in the case of positions not under the General Schedule, for which the rate of basic pay is equal to or greater than 120 percent of the minimum rate of basic pay payable for GS–15 of the General Schedule; and (B) any commissioned officer in the Armed Forces in pay grades O–6 and above."

Appendix VIII – Substantiated Instances of Whistleblower Retaliation

Number of Substantiated Instances of Whistleblower Retaliation
There were no substantiated instances of whistleblower retaliation.

	Detailed Description
A. Information about the official found to have engaged in retaliation	N/A
B. Any consequences the agency imposed to hold the official accountable	N/A

Appendix IX – Attempts by the Agency to Interfere with the Independence of the OIG

Number of Attempts by the Agency to Interfere with the Independence of the OIG	
The FTC OIG encountered no attempts to interfere with OIG independence.	
	Detailed Description
A. Attempts to interfere with budget constraints designed to limit OIG capabilities	None
B. Incidents where the agency has resisted or objected to OIG oversight or restricted or significantly delayed OIG access to information, including the justification of the agency for such action	None

Appendix X – Closed OIG Matters Not Disclosed to the Public

	Detailed Description
A. Inspections, evaluations, and audits conducted by the OIG that are closed and were not publicly disclosed	None
B. Investigations conducted by the OIG involving a senior government employee that are closed and were not publicly disclosed	None

Appendix XI – Inspector General Act Reporting Requirements Index

IG Act Reference	Reporting Requirements	Pages(s)
Section 4(a)(2)	Review of legislation and regulations	18 - 19
Section 5(a)(1)	Significant problems, abuses and deficiencies	None
Section 5(a)(2)	Recommendations with respect to significant problems, abuses and deficiencies	7-17
Section 5(a)(3)	Prior significant recommendations on which corrective actions have not been completed	21-27
Section 5(a)(4)	Matters referred to prosecutive authorities	15-16
Section 5(a)(5)	Summary of instances where information or assistance was unreasonably refused or not provided	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	7-11
Section 5(a)(8)	Statistical tables showing number of reports and dollar value of questioned costs	28
Section 5(a)(9)	Statistical tables showing number of reports and dollar value of recommendations that funds be put to better use	29
Section 5(a)(10)	Summary of each audit, inspection, and evaluation report issued before the commencement of the reporting period (A) for which no management decision has been made by the end of the reporting period; (B) for which no establishment comment was returned within 60 days of providing the report to the establishment; and (C) for which there are any outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations	30
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
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
Section 5(a)(17) and (18)	OIG Investigative Activity during this Reporting Period	31
Section 5(a)(19)	OIG Investigations involving Senior Government Employees Where Allegations of Misconduct Were Substantiated	32
Section 5(a)(20)	Substantiated Instances of Whistleblower Retaliation	33
Section 5(a)(21)	Attempts by the Agency to Interfere with OIG Independence	34
Section 5(a)(22)	Closed OIG Matters Not Disclosed to the Public	35

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.