FEDERAL TRADE COMMISSION

OIG

10.01.17

—

03.31.18

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, 2017, through March 31, 2018.

During this reporting period, the OIG identified serious, ongoing concerns with management's failure to effectively implement critical recommendations from the OIG's reporting pursuant to the Federal Information Security Modernization Act (FISMA) of 2014. The OIG assessed that the current state, legacy systems remained effective in protecting FTC information assets. However, we also assessed that the agency can expect increased system outages, and lost productivity and associated costs, as its legacy systems exceed their projected life span, and management focuses on its delayed IT modernization effort while not effectively and concurrently maintaining the security of its legacy operations.

Our FY 2017 FISMA assessment showed that the FTC information security program continues to decline. In our FY 2017 evaluation, using the maturity model created by the Council of the Inspectors General on Integrity and Efficiency, we assessed four of the five functional areas as "Defined" and only one as "Consistently Implemented." This demonstrates a decline in two of the five functions (Identify and Respond), and no improvement in the other three. The OIG developed nine recommendations to improve the FTC's information security program. The table below shows the status of OIG open recommendations after consolidation of all open FISMA-related recommendations:

OPEN OIG RECOMMENDATIONS AS OF 4/30/18		
OIG Report	**Issued**	**Open Recommendations**
FY 2015 FISMA	Feb 2016	3 of 7
IT Governance	Sep 2016	12 of 15
FY 2016 FISMA	Mar 2017	2 of 8
FY 2017 OIG DATA Act Report	Nov 2017	1 of 1
FY 2017 Financial Statement Management Letter	Dec 2017	1 of 1
FY 2017 FISMA	Mar 2018	9 of 9

The OIG's collaboration with the FTC Bureau of Consumer Protection (BCP) and the larger OIG community to boost OIG investigations of consumer fraud matured during the reporting period. The initiative seeks to promote awareness and use of the Consumer Sentinel Network – a secure online database available to law enforcement that currently houses over 13 million consumer complaints. Since our initiative began in December 2016, CSN has witnessed a 65 percent increase in usage by federal OIG investigators, as well as a 13 percent increase in the number of OIGs using this valuable resource for their investigative work.

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

As I retire this month from federal service, I want to express my appreciation for the outstanding dedication of OIG personnel whose work is reflected in this report. Together we have strengthened the OIG by recruiting, integrating and supporting new OIG personnel; matured our business processes to become a more efficient and cohesive team; acquired a deeper understanding of the FTC mission through outreach to all regional offices and "deep dives" with Bureaus and Offices; and promoted the OIG mission through periodic in reach sessions at Headquarters.

It has been a genuine privilege to lead the OIG's talented staff, who joined with me to generate valuable work on behalf of the FTC, the larger OIG community, and the American people. As the FTC and the OIG transition to new leadership, I thank new FTC Chairman Joseph Simons, former Chair Edith Ramirez, former Acting Chairman and Commissioner Maureen Ohlhausen, agency management and staff, and the Congress for their sustained support to the OIG mission. I also thank the Council of the Inspectors General on Integrity and Efficiency, its inspiring leadership and staff, and all of its members for their deep commitment to the unique and vital role of the federal Inspector General community.

About the FTC Office of Inspector General

OIG Mission

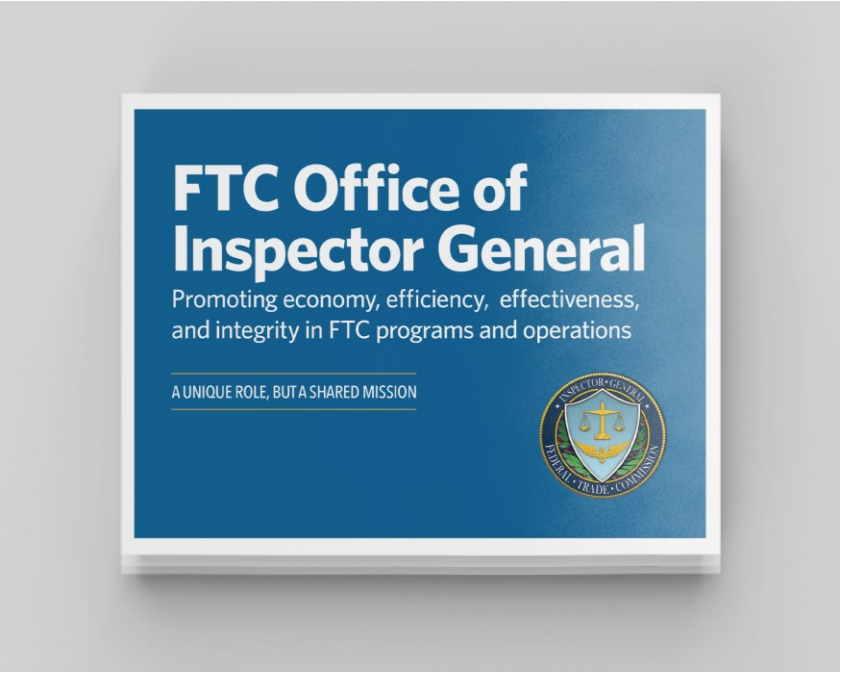
To promote economy, efficiency and effectiveness, and to detect and prevent waste, fraud, abuse, and mismanagement in the agency's operations and programs.

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 has an operating budget of $1,674,100 for FY 2018.

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) 2017. We issued three audit reports: the Financial Statement Audit for FY 2017, its associated Management Letter, and the FTC's Digital Accountability and Transparency Act Report. In accordance with section 5(a)(6) of the Inspector General Act of 1978, as amended, none of these reports had questioned costs or recommendations that funds be put to better use.

FY 2017 Management Challenges

In our FY 2017 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

FY 2017 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 was to assess the effectiveness of the FTC information and privacy programs at September 30, 2017, as required under FISMA and the *FY 2017 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.0*, 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).

For more than five years, the OIG assessed the FTC information security and privacy programs as strong and robust, but overly dependent on manual operations and with planning and governance deficiencies. The FTC gradually improved its information security and privacy control environments and evolved toward the

National Institute of Standards and Technology information security approach that focuses on defined, documented, and repeatable processes with risk-based decisions. For example, the FTC completed its Personal Identity Verification (PIV) implementation. Individual access to FTC systems is now controlled through the common credentialing and standard background investigation process required by Homeland Security Presidential Directive 12 (HSPD-12). The HSPD-12 process requires strong individual authentication for issuance of PIV credentials and two-factor authentication to validate individual access. The FTC's implementation of PIV significantly strengthens access control for agency systems.

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

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

- The FTC should document its system inventory management system and validate the system, database, and management procedures as a trusted FTC Information Security Continuous Monitoring component under configuration control and that supports continuous monitoring. The FTC should also implement a capability to view its inventory as a single database even though it may be constructed as three separate components.
- The FTC should institute configuration management of its Cyber Security Assessment and Management (CSAM) process; produce security artifacts that support effective analysis of CSAM security controls and granting of an FTC Authority to Operate; and validate the CSAM database.
- The FTC governance documentation should include a Charter that describes the scope and purpose of the governance program and the roles and responsibilities of those entities responsible for its execution and a graphic or other documentation that shows the FTC entities with information governance responsibilities. The governance documentation should

show how risk and information security requirements are identified and resolved. Governance artifacts should be subject to configuration management that includes change management for security artifacts and other system documentation.

- The FTC should conduct risk analyses to identify the risks associated with its modernization initiative. These risk assessments should identify the risks associated with maintaining the legacy system until its retirement, the risks associated with the proposed cloud-based target environment, and the risks associated with the transition to the target environment. The assessments should be sufficiently documented to inform an FTC decision to mitigate, transfer, or accept risk. Where a risk is accepted, the FTC should include in its documentation a description of the risk accepted and an estimate of the duration and potential impact of an event should the risk be realized.
- The FTC should implement an information security risk management strategy that operates as a component of the FTC Enterprise Risk Management program and is applied to all the FTC information systems operated by the FTC or under contract to support the FTC.
- The FTC should collect metrics describing the status and progress of its modernization effort. These metrics should be used to routinely (at least every 6 months) report project cost, schedules and performance status using the September 2016 version as the baseline.
- The FTC should develop an Information Resources Management (IRM) Plan that addresses the topics OMB identified for inclusion. The FTC should incorporate metrics into its IRM Plan that allow the performance and cost to be monitored. The FTC should monitor IRM Plan status and costs at least on an annual basis.
- The FTC should develop an agency-wide configuration management policy that applies to any information systems supporting the FTC. The policy should require development of procedures that are specific to individual systems. The FTC configuration management policy should also require configuration control for all system and information security artifacts.
- The FTC should revise its incident response and information system contingency plans to ensure they provide viable procedures for responding to system outages and potential sensitive information compromises. The revised plans should include policies and protocols for US-CERT reporting, maintaining activity logs, communications with stakeholders, and After-Action reporting that includes root cause analyses, activity log analyses, and timely reporting. Plans should be tested at least annually.

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

FY 2017 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's Audit Manager serves as the Contracting Officer's Representative (COR).

For the 21st 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, 2017, Brown & Company found:

- The Fiscal Years 2017 and 2016 financial statements were presented fairly, in all material respects, in accordance with U.S. generally accepted accounting principles,
- There were no material weaknesses in internal control over financial reporting, and
- No reportable instances of noncompliance with applicable provisions of laws, regulations, and contracts tested.

Management Letter from the FY 2017 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 area:

- Employee Debt Receivables over 120 Days For Which FTC Financial Management Operations Had Taken No Recent Follow-Up Action

Management concurred with this recommendation and is in the process of implementing actions to address the issue identified.

OIG Independent Evaluation of the Federal Trade Commission's Compliance with Provisions of the Digital Accountability and Transparency Act of 2014

The Digital Accountability and Transparency Act of 2014 (DATA Act) requires that the FTC obtain an independent audit of the FTC's reporting and implementation of the DATA Act. We contracted with the independent public accounting firm of Brown & Company CPAs, PLLC to perform this audit under the financial statement contract for which the OIG's Audit Manager serves as the COR. The objectives of the audit were to assess the: (1) completeness, timeliness, quality, and accuracy of FY 2017, second quarter financial

and award data submitted for publication on USASpending.gov; and (2) the FTC's implementation and use of the Government-wide financial data standards established by the OMB and the Department of the Treasury (Treasury).

In its audit of the FTC, Brown & Company found that the FTC's FY 2017 second quarter financial and award data for the quarter ended March 31, 2017, is presented in accordance with the OMB's and Treasury's published 57 data definition standards for DATA Act reporting in all material respects.

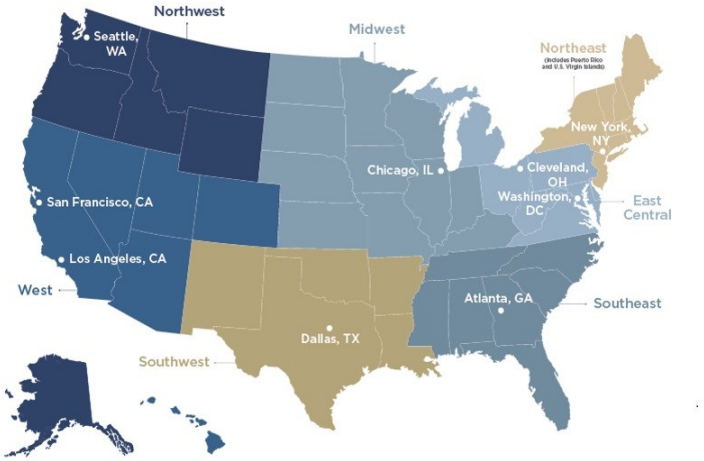
Brown & Company made one recommendation in the following area:

- Entering the correct period of performance dates and action dates prior to finalizing awards in the agency's financial system. noncompliance with applicable provisions of laws, regulations, and contracts tested.

Management concurred with this recommendation and is in the process of implementing actions to address the issue identified.

Ongoing Work

Outreach to FTC Regional Offices

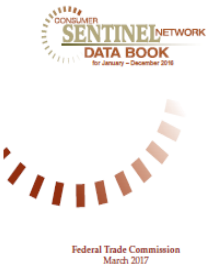


During this reporting period, the OIG completed an initiative, launched in September 2016, to acquire a greater understanding of the mission, role, and any special challenges of the agency's regional offices and to acquaint these offices with the unique role of the OIG. In October 2017, the OIG conducted outreach visits to the FTC's Western (Los Angeles and San Francisco, California) and Northwest (Seattle, Washington) Regional Offices. In meetings with each regional office's leadership and staff, OIG provided an educational presentation, highlighting tips for identifying fraud schemes and reporting fraud to the OIG and educating employees on whistleblower protection laws. Following these engagements, several employees in regional offices have contacted the OIG to refer matters relevant to the OIG mission or confer about agency activities.

FTC High Risk Contracts Performance Audit

The OIG is conducting a performance audit of the FTC's acquisition planning of procured contracts. The objective of our audit is to determine if the FTC properly plans and awards contracts in accordance with applicable laws, regulations, and policy. We will review applicable federal laws and regulations pertaining to procurement planning and contract oversight. We will conduct interviews with FTC officials to gain an understanding of the contracting process and review controls over contracting actions.

Cross-Community OIG Consumer Fraud Initiative



During this reporting period, the OIG continued its collaboration with the FTC Bureau of Consumer Protection and various Offices of Inspector General to identify opportunities to boost OIG investigations of consumer fraud. The initiative focuses on extending the use and value of the FTC's Consumer Sentinel Network (CSN) – a secure online database currently housing over 13 million consumer complaints dating from calendar year (CY) 2013 through CY 2017. CSN has observed a 65 percent increase in usage by individuals within the OIG community since the initiative began in December 2016.

CSN is a unique investigative cyber 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 36 data contributors, including the Consumer Financial Protection Bureau, 20 State Attorneys General, and all North American Better Business Bureaus. Over 2,300 federal, state, local, and international law enforcement users have access to CSN, and hundreds of individual members access the system each week.

The top identifiable trends in these complaints during the last reporting period were debt collection, imposter scams, and identity theft. There are currently 25 OIG's utilizing CSN, reflecting a 13 percent increase in the number of OIGs using this valuable resource since the initiative began.

During this reporting period, the FTC received positive feedback about the utility of CSN in OIG investigations. Users have commented that CSN has greatly facilitated their ability to research and identify individuals suspected of committing fraud, such as impersonation scams, through such search tools as name, address, email, and telephone numbers. Additionally, CSN continues to add key system upgrades, search tools, and sources of data.

Sentinel 3.0 was released in June 2017, which promises to augment OIG investigations of consumer fraud. Sentinel 3.0 contains new analytical and visualization tools, phrase cloud and phrase trending, and search results that will personalize user experiences. One of the most useful new tools is the Sentinel Spotlight, which enables the user to view summary data and see the latest consumer protection trends, such as imposter scams, so the user can quickly identify possible targets and areas needing focus, and gather complaint records quickly and efficiently. Graph analytics, which was recently unveiled, is a new tool for investigators looking to make connections between data points that are not necessarily intuitive. With this tool, users can explore and visualize new and important relationships between key data points for fraud and Do Not Call complaints.

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 the previous reporting period. Section 4 of 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. The OIG looks forward to continuing to facilitating additional tutorials with other OIGs and identifying opportunities to strengthen the CSN database with information valuable to OIGs conducting consumer fraud investigations.

Enterprise Risk Management

OMB Circular A-123 requires 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 the OIG's Annual Report on Management Challenges.

The FTC's Senior Assessment Team provides leadership and oversight for the FTC's internal control program, the goal of which is to ensure 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, and to witness the internal controls' identification and resolution cycles. Additionally, OIG staff is increasing its proficiency in ERM principles by attending periodic training sessions and webinars. The OIG developed 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 five recommendations during this reporting period. For the listed reports, the OIG did not close any recommendations. The Acting Chairman, her Chief of Staff, the Executive Director, and the Chief Information Officer and his team have devoted significant time, effort, and additional resources to address legacy FISMA recommendations, and these efforts position the agency to better protect legacy systems and improve other cybersecurity efforts. The OIG hopes that, with sustained leadership from the incoming FTC Chairman and Commissioners, these efforts will meaningfully improve the FTC's information security program during the balance of FY 2018 and beyond.

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 142 consumer complaints, inquiries, and reports of possible wrongdoing. The OIG redirected 124 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 6% 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 FY 2018 data accumulated from telephone calls and emails to the OIG Hotline:

- From October 1, 2017 to March 31, 2018, 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 initiated two investigations and closed zero investigations during the reporting period.

Preliminary Inquiries

The OIG closed one preliminary inquiry during the reporting period. We initiated four new preliminaries inquiries.

Management Advisories and Referrals

During this reporting period, the OIG issued one management advisory and one management referral stemming from investigative activity, as highlighted below. The management advisory identified deficiencies in the FTC's incident response policies and procedures with respect to a multi-day outage of the FTC's email system in FY 2017. The management referral identified potential violations of the FTC's purchase card program, summarized below:

Management Referral

In late 2017, the OIG received several complaints about an FTC employee related to the performance of official duties. One of these complaints included an allegation that the employee was misusing an assigned FTC purchase card by providing the card and account information to other FTC personnel, including contractors, for agency purchases, in violation of FTC policy. The OIG identified approximately 40 purchases between April 1, 2016 and September 30, 2017, by individuals other than the employee, totaling approximately $40,000. Due to the ongoing risk to FTC resources and integrity of its operations, we referred this matter to management for prompt review. In response, management cancelled the employee's purchase card and required the employee to complete the Government Services Administration's and the FTC's purchase card training. Management conducted a reassessment of the affected office and took steps to eliminate vulnerabilities in that office, including reducing the number of purchase cardholders.

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 Federal Bureau of Investigation, the Department of Justice's Public Integrity Section, the Department of the Treasury, the Federal Communications Commission OIG, the National Labor Relations Board OIG, the Corporation of National Community Service OIG, and the Architect of the Capitol OIG.

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 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 OIG is also participating on an OIG community-wide effort to commemorate the 40th anniversary of the Inspector General Act, which was signed into law in October 1978. The commemoration, entitled *Building on 40 Years of Excellence in Independent Oversight*, will celebrate significant contributions the IG community has made towards better government and will highlight major contributions from across the OIG community. Additional information on this important commemoration is available on the CIGIE website at: https://www.ignet.gov/2018-commemoration.

On October 1, 2017, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) announced the official launch of Oversight.gov. This new website provides a "one stop shop" to follow the ongoing oversight work of all Inspectors General that publicly post reports.

The FTC OIG, like the other OIGs, will continue to post reports to its own website. But with the launch of Oversight.gov, users can now sort, search, and filter the site's database of public reports from all of CIGIE's member OIGs to find reports of interest. In addition, the site features a user-friendly map to find reports based on geographic location, and contact information for each OIG's whistleblower hotline. Users can receive notifications when new reports are added to the site by following CIGIE's new Twitter account: @OversightGov.

Other CIGIE Engagements

The Counsel to the Inspector General is an active member on the CIGIE Council of Counsels to the Inspectors General working group, Small OIG Counsels working group, and the Investigations Committee, and he contributes to the legal and investigative discourse on matters germane to the entire OIG community.

The OIG's Audit Manager is an adjunct trainer for 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. Additionally, the Program Analyst is a member of the CIGIE Enterprise Risk Management Working Group, as well as the workgroup for the central OIG community electronic work papers Contract.

The OIG's Audit and Evaluation Team participates in the monthly Federal Audit Executive Council Data Act Working Group meetings.

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.

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.

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 collaborated with management on the implementation of the Office of Special Counsel's (OSC) 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. During this reporting period, the OIG updated the agency's Whistleblower Protection Website with guidance on the new prohibited personnel practice (PPP) enumerated in the Dr. Chris Kirkpatrick Whistleblower Protection Act of 2017, which prohibits an agency official from accessing the medical record of another employee or applicant in furtherance of any conduct proscribed by the other PPPs. New

legislation also mandates annual whistleblower protection training for supervisors, requires mandatory disciplinary action up to removal for supervisors found to have violated certain PPPs, and mandates the incorporation of a new critical element in supervisors' performance plans that includes protecting and constructively responding to whistleblowers. The OIG also participated in the FTC's supervisory development program for new supervisors to educate them on their whistleblower protection responsibilities, and we will participate in additional trainings throughout the fiscal year.

The OIG continues to work with management to improve the policy and practice for tracking OIG recommendations. The OIG periodically meets with the Senior Assessment Team to 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	There were no peer reviews conducted by another OIG during this reporting period. The last peer review was dated June 30, 2015.
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

Independent Assessment of Implementation of the Federal Information Security Modernization Act (FISMA) for Fiscal Year 2016 (Report Issued: 03/2017) (Link to Report)

Recommendations	Total	8
	Mgmt. concurs	8
	Mgmt. non-concurs	--
Status of Recommendations	Closed[1]	0
	Open	8

Recommendations

- **FY 2016 – 01: Complete the System Inventory**
  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.
- **FY 2016 – 02: Review Application Classification**
  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.
- **FY 2016 – 03: Document Risk-Based Decisions**
  The FTC should implement a formal procedure for documenting risk-based decisions as part of the FTC risk management 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.

- **FY 2016 – 04: Develop Risk Analyses for FTC's IT Modernization Initiative**
  The FTC should implement a formal risk management program that addresses the requirements of OMB Circulars A-123 and A-130 and the guidance contained in NIST Special Publications 800-30, 800-37, and 800-39. The FTC should conduct risk analyses for its IT Modernization Initiative.
- **FY 2016 – 05: Segment Modernization Activities into Useful Segments**
  The FTC should structure modernization activities for acquiring major IT investments as useful segments that can be independently planned, acquired, and monitored.
- **FY 2016 – 06: Implement an Information Security Continuous Monitoring**
  The FTC should implement a fully compliant ISCM as described in its ISCM Plan in FY 2013 and its ISCM Strategy, dated November 2014.
- **FY 2016 – 07: Revise the Plan of Action and Milestones Process**
  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 audits, financial system audits, and critical infrastructure vulnerability assessments) and can be an effective, authoritative, agency-wide management tool.
- **FY 2016 – 08: Develop Contingency Plans for the FTC HQ data center**
  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.

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

Recommendations	Total	15
	Mgmt. concurs	15
	Mgmt. non-concurs	--
Status of Recommendations	Closed	2
	Open	13

Recommendations

- **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.

13: System Security Plan

Develop a System Security Plan for the mobile device project based on NIST Special Publication 800-53, Revision 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.

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 Authority to Operate 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.

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		
• based on proposed legislative actions		
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
. 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 2017	1	8	0
FY 2016	2	19	0
FY 2015	1	3	0
TOTAL for All Fiscal Years	4	30	0

[2] In accordance with 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	0
B. Number of persons referred to DOJ for criminal prosecution	0
C. Number of persons referred to State and Local authorities for criminal prosecution	0
D. Number of criminal indictments and criminal information 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 was 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	N/A
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	N/A

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	0
B. Investigations conducted by the OIG involving a senior government employee that are closed and were not publicly disclosed	0

Appendix XI – Inspector General Act Reporting Requirements Index

IG Act Reference	Reporting Requirements	Pages(s)
Section 4(a)(2)	Review of legislation and regulations	19
Section 5(a)(1)	Significant problems, abuses and deficiencies	None
Section 5(a)(2)	Recommendations with respect to significant problems, abuses and deficiencies	None
Section 5(a)(3)	Prior significant recommendations on which corrective actions have not been completed	22-27
Section 5(a)(4)	Matters referred to prosecutive authorities	None
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	7-14
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	21
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.