



SEMIANNUAL REPORT

TO CONGRESS

04.01.14 TO 09.30.14

Office of Inspector General

U.S. SECURITIES AND EXCHANGE COMMISSION

OFFICE OF INSPECTOR GENERAL
SEMIANNUAL REPORT TO CONGRESS

APRIL 1, 2014 THROUGH SEPTEMBER 30, 2014



The mission of the Office of Inspector General (OIG) is to prevent and detect fraud, waste, and abuse and to promote the integrity, economy, efficiency, and effectiveness in the critical programs and operations of the U.S. Securities and Exchange Commission (SEC or agency). This mission is best achieved by having an effective, vigorous, and independent office of seasoned and talented professionals. Those individuals carry out the OIG's mission by performing these functions:

- conducting independent and objective audits, evaluations, inspections, investigations, and other reviews of SEC programs and operations;
- preventing and detecting fraud, waste, abuse, and mismanagement in SEC programs and operations;
- identifying vulnerabilities in SEC systems and operations and recommending constructive solutions;
- offering expert assistance to improve SEC programs and operations;
- communicating timely and useful information that facilitates management decision making and the achievement of measurable gains; and
- keeping Congress and the Commission fully and currently informed of significant issues and developments.

CONTENTS

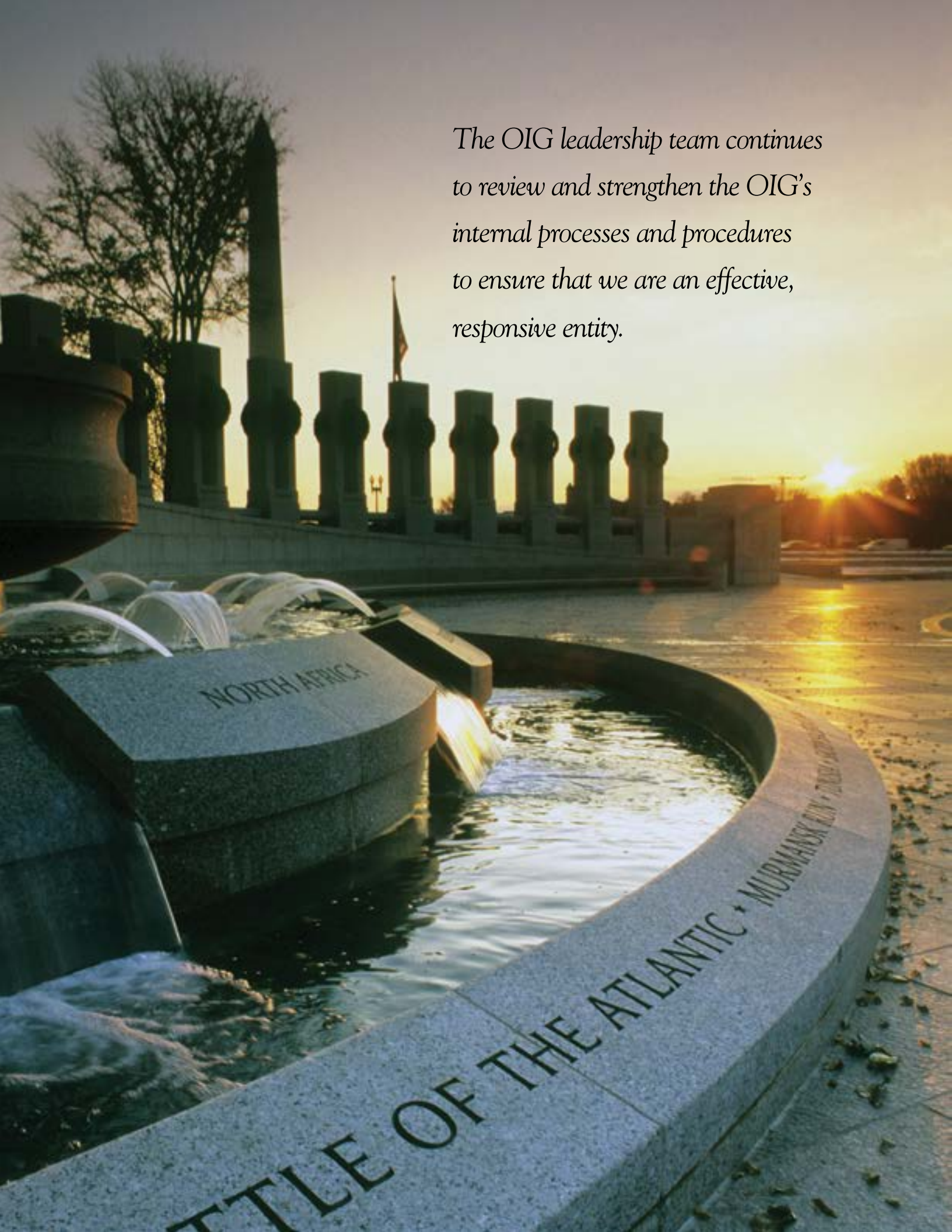
MESSAGE FROM THE INSPECTOR GENERAL	1
MANAGEMENT AND ADMINISTRATION	3
Agency Overview	3
OIG Staffing	3
OIG Outreach	4
CONGRESSIONAL REQUESTS AND BRIEFINGS	5
THE OIG'S STATEMENT ON THE SEC'S MANAGEMENT AND PERFORMANCE CHALLENGES	6
Management and Performance Challenges	6
<i>Regulatory Oversight</i>	6
<i>Information Security</i>	7
<i>Acquisition Management</i>	9
<i>Financial Management</i>	9
<i>Human Capital Management</i>	10
COORDINATION WITH OTHER OFFICES OF INSPECTOR GENERAL	12
AUDITS AND EVALUATIONS	14
Overview	14
Completed Audits and Evaluations	14
<i>Review of the SEC's Practices for Sanitizing Digital Information</i> <i>System Media (Report No. 521)</i>	14
<i>Audit of the SEC's Physical Security Program (Report No. 523)</i>	15
<i>Controls Over the SEC's Inventory of Laptop Computers (Report No. 524)</i>	16
<i>Analysis of the SEC's Compliance with Conference Approval and</i> <i>Reporting Requirements for Fiscal Year 2014</i>	17
Ongoing Audits and Evaluations	17
<i>Audit of the SEC Office of the Ethics Counsel's Oversight of</i> <i>Employee Security Holdings</i>	17
<i>Audit of the Representation of Minorities and Women in the SEC's Workforce</i>	18
<i>Federal Information Security Management Act: Fiscal Year 2014 Evaluation</i>	18

INVESTIGATIONS	19
Overview	19
Status of Previously Reported Investigations	19
<i>Violation of SEC Supplemental Ethics Rules by a Staff Accountant</i> <i>(Case No. 14-0070-I; previously OIG-585)</i>	19
<i>False Statements Related to Prohibited Financial Holdings</i> <i>(Case No. 14-0071-I; previously OIG-598)</i>	20
<i>Departing SEC Employee’s Attempt to Remove Nonpublic Information</i> <i>From the SEC (Case No. 14-0012-I; previously OIG-600)</i>	20
<i>Unauthorized Disclosure of Nonpublic Information from Executive</i> <i>Session Commission Meeting (Case No. 14-0013-I; previously OIG-601)</i>	21
Completed Investigations	21
<i>SEC Senior Officer’s Acceptance of Direct Payment for International Travel</i> <i>(Case No. 14-0009-I)</i>	21
<i>Allegations of Time and Attendance Fraud by SEC Managers (Case No. 14-0017-I)</i>	21
<i>Fraudulent SEC Internet Domains (Case No. 14-0182-I)</i>	22
<i>Unauthorized Transmission of Personally Identifiable Information by an</i> <i>SEC Employee (Case No. 14-0516-I)</i>	22
<i>Allegation of Misconduct by an SEC Manager (Case No. 14-0543-I)</i>	22
<i>Unauthorized Transmission of Nonpublic Information by an</i> <i>SEC Attorney (Case No. 14-0552-I)</i>	22
REVIEW OF LEGISLATION AND REGULATIONS.	24
MANAGEMENT DECISIONS	25
Status of Recommendations With No Management Decisions	25
Revised Management Decisions	25
Agreement With Significant Management Decisions	25
Instances Where the Agency Refused or Failed to Provide Information to the OIG	25

TABLES	27
Table 1 List of Reports: Audits and Evaluations.	27
Table 2 Reports Issued With Costs Questioned or Funds Put to Better Use (Including Disallowed Costs)	27
Table 3 Reports With Recommendations on Which Corrective Action Has Not Been Completed.	28
Table 4 Summary of Investigative Activity for the Reporting Period of April 1, 2014 to September 30, 2014.	30
Table 5 References to Reporting Requirements of the Inspector General Act.	31
APPENDIX A. PEER REVIEWS OF OIG OPERATIONS	32
Peer Review of the SEC OIG’s Audit Operations	32
Peer Review of the SEC OIG’s Investigative Operations	32
APPENDIX B: OIG SEC EMPLOYEE SUGGESTION PROGRAM ANNUAL REPORT.	33
Overview	33
Summary of Employee Suggestions and Allegations	33
Examples of Suggestions and Allegations.	34
<i>Print Font Requiring Less Space (ES-0214)</i>	34
<i>Training System Automatic Notification and Calendar Reminders</i> <i>(ES 14-0274; ES 14-0574)</i>	34
<i>Fees for Local Travel Expense Reimbursement (ES 14-0583).</i>	35
Conclusion	35

ABBREVIATIONS

Agency	U.S. Securities and Exchange Commission
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
DOJ	Department of Justice
EDGAR	Electronic Data Gathering, Analysis and Retrieval
FAEC	Federal Audit Executive Council
FASB	Financial Accounting Standards Board
FHFA	Federal Housing Finance Agency
FINRA	Financial Industry Regulatory Authority
FISMA	Federal Information Security Management Act
FTE	fulltime equivalents
FY	fiscal year
GAGAS	Generally Accepted Government Auditing Standards
GAO	U.S. Government Accountability Office
IG	Inspector General
IRS	Internal Revenue Service
IT	Information Technology
JOBS Act	Jumpstart Our Business Startups Act
Laptops	laptop computers
LEAP	Lead, Learn, and Perform
LSC	Legal Services Corporation
Media	Digital Information System Media
MSRB	Municipal Securities Rulemaking Board
OCOO	Office of the Chief Operating Officer
OEC	Office of the Ethics Counsel
OEE0	Office of Equal Employment Opportunity
OFM	Office of Financial Management
OHR	Office of Human Resources
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OMWI	Office of Minority and Women Inclusion
OPM	Office of Personnel Management
OS	Office of the Secretary
OSS	Office of Security Services
PCAOB	Public Company Accounting Oversight Board
PII	personally identifiable information
SEC	U.S. Securities and Exchange Commission
SIPC	Securities Investor Protection Corporation
SO	Senior Officer
Treasury	Department of the Treasury
USAO	United States Attorney's Office



The OIG leadership team continues to review and strengthen the OIG's internal processes and procedures to ensure that we are an effective, responsive entity.



MESSAGE FROM THE INSPECTOR GENERAL



I am pleased to present this Semiannual Report to Congress as Inspector General (IG) of the SEC. This report describes the work of the SEC OIG from April 1, 2014 to September 30, 2014. It also reflects our responsibility to report independently to both Congress and the Commission. The audits, evaluations, and investigations that we describe illustrate the OIG's efforts to promote the efficiency and effectiveness of the SEC and demonstrate the impact that our work has had on the agency's programs and operations.

During this semiannual reporting period, the OIG hired a number of seasoned professionals to fill staffing shortages. Notably, I appointed a Counsel with significant legal experience in the IG community. I will continue to work closely with the Commission to ensure that the OIG has the necessary resources to carry out its mission of promoting the integrity, efficiency, and effectiveness of the SEC's programs and operations.

The OIG leadership team continues to review and strengthen the OIG's internal processes and procedures to ensure that we are an effective, responsive entity. To that end, we have updated the OIG audit and investigation manuals and are enhancing our support functions and developing office-wide poli-

cies and procedures. Further, our audits and evaluations are now conducted using a team approach that is designed to improve their efficiency and quality. In July 2014, the Office of Audits implemented an audit management software system that is designed to increase auditor productivity and facilitate supervisory review. Moreover, in June 2014, the Office of Investigations received approval from the Attorney General to exercise law enforcement authority under the Inspector General Act and the Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority. This authority allows the OIG's special agents to exercise law enforcement powers and enhances our ability to conduct criminal investigations.

During this reporting period, the Office of Audits issued three reports. First, on May 30, 2014, we issued a report on our review of the SEC's practices for sanitizing digital information system media. The focus of this report was to assess whether the SEC effectively sanitized surplus media before its disposal, thereby minimizing the risk of the unauthorized release of sensitive information. Next, on August 1, 2014, we completed an audit of the SEC's physical security program to assess the SEC's policies, procedures, and controls for safeguarding personnel and preventing unauthorized access to the agency's facilities. Lastly, on September 22, 2014, we issued a report on our audit of the effectiveness of the SEC Office of Information Technology's (OIT) inventory program and its controls over laptop computers.

The Office of Investigations completed or closed 11 investigations during this reporting period on various topics, including prohibited securities holdings by SEC employees, the direct reimbursement of travel expenses from an outside entity, allegations of misconduct by SEC managers, fraudulent SEC Internet domains, and the unauthorized transmission of personally identifiable information and other nonpublic SEC information. Our investigations resulted in nine referrals to the Department of Justice (DOJ), two of which were accepted for possible prosecution. Based on our completed investigations, we made three referrals to agency management for appropriate administrative action.

The Office of Audits and the Office of Investigations also worked with SEC management to close 22 recommendations made in OIG reports issued during this and previous semiannual reporting periods.

Additionally, the OIG continued to implement its SEC outreach program during this reporting period. To date, OIG managers and I have visited all of the SEC's regional offices and have met with the majority of the headquarters divisions and offices. We plan to meet with the remaining headquarters divisions and offices during the next semiannual reporting period. Also, the OIG's outreach presentation is included in the SEC's biweekly new employee orientation sessions. These outreach efforts are increasing the OIG's visibility and further enhancing SEC employees' understanding of the role and functions of the OIG. They also serve to educate employees on the applicable ethics requirements and their obligations to report fraud, waste, and abuse to the appropriate authorities.

In closing, I want to reiterate my firm commitment to executing the SEC OIG's mission of promoting the integrity, efficiency, and effectiveness of the SEC's programs and operations and to reporting our findings and recommendations to Congress and the Commission. The OIG will continue to strive to improve its efficiency and effectiveness by making organizational and procedural changes and increasing its staffing levels. We will also continue to work collaboratively with SEC management to assist the agency in addressing the challenges it faces in its unique and important mission of protecting investors, maintaining fair, orderly, and efficient markets, and facilitating capital formation.

I appreciate the significant support that the OIG has received from Congress and the Commission. We look forward to continuing to work closely with the SEC Chair, Commissioners, and employees, as well as Congress, to increase efficiency and effectiveness in the SEC's programs and operations.



Carl W. Hoecker

Inspector General



MANAGEMENT AND ADMINISTRATION

AGENCY OVERVIEW

The SEC's mission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. The SEC strives to promote a market environment that is worthy of the public's trust and characterized by transparency and integrity. Its core values consist of integrity, accountability, effectiveness, teamwork, fairness, and commitment to excellence. The SEC's goals are to foster and enforce compliance with the Federal securities laws; establish an effective regulatory environment; facilitate access to the information investors need to make informed investment decisions; and enhance the SEC's performance through effective alignment and management of human resources, information, and financial capital.

The agency currently oversees more than 25,000 market participants, including over 11,000 investment advisers, approximately 10,000 mutual funds and exchange traded funds, 4,450 broker-dealers, 450 transfer agents, 18 securities exchanges, as well as the Public Company Accounting Oversight Board (PCAOB), the Financial Industry Regulatory Authority (FINRA), the Municipal Securities Rulemaking Board (MSRB), the Securities Investor Protection Corporation (SIPC), and the Financial Accounting Standards Board (FASB). The SEC also has responsibility for reviewing the disclosures and financial statements of approximately 9,000 report-

ing companies, and has new and expanded responsibilities over the derivatives markets, an additional 2,500 exempt reporting advisers to hedge funds and other private funds, close to 1,000 municipal advisers, 10 registered credit rating agencies, and 7 registered clearing agencies. And, between the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) and the Jumpstart Our Business Startups Act (JOBS Act), the SEC was given nearly 100 new rulemaking responsibilities.

The SEC accomplishes its mission through 5 main divisions—Corporation Finance, Enforcement, Investment Management, Trading and Markets, and Economic and Risk Analysis—and 22 functional offices. The SEC's headquarters is in Washington, DC, and there are 11 regional offices located throughout the country. As of the end of FY 2014, the SEC employed 4,199 fulltime equivalent (FTE) employees.

OIG STAFFING

During this semiannual reporting period, the OIG continued to add key staff as the OIG moved towards operating at full capacity. Specifically, the OIG appointed a Counsel, whose biography is on the OIG's website at www.sec.gov/about/offices/oig/inspector_general_admin_bios.shtml. The OIG also hired four criminal investigators, an audit manager, three auditors, and two program support specialists.

To aid the OIG staff in performing their oversight responsibilities, the OIG is working with SEC University to develop a comprehensive training program that will focus on the complexities of the SEC's regulatory responsibilities and authorities.

The OIG plans to continue to add personnel to ensure it has the necessary staffing levels to effectively perform its oversight responsibilities.

OIG OUTREACH

In the reporting period, the IG regularly met with the Chair, Commissioners, and senior officers from various SEC divisions and offices to foster open communication at all levels between the OIG and the agency. Through these efforts, the OIG was kept up to date on significant, current matters that were relevant to the OIG's work. These regular communications also allowed the OIG and agency management to work cooperatively to identify the most important areas for the OIG's work, as well as the best means of addressing the results of that work. The OIG continually strives to keep apprised of changes to agency programs and operations and will keep SEC management informed of the OIG's activities and concerns raised in the course of its work.

Further, the OIG continued to implement its SEC outreach program. The goal of this program is to increase the OIG's visibility and further enhance SEC employees' understanding of the OIG's role and functions. The program also educates employees on the applicable ethics requirements and their obligations to report fraud, waste, and abuse to the appropriate authorities.

During the previous reporting period, the OIG initiated the outreach program, visited 10 of the 11 SEC regional offices, and met with the Office of the Chief Operating Officer. In this period, the OIG visited the remaining regional office and met with the staff of the majority of the headquarters divisions and offices. The OIG plans to meet with the remaining headquarters divisions and offices during the next semiannual reporting period. Also, the OIG's outreach presentation is included in the SEC's biweekly new employee orientation sessions.

Further, between June and July 2014, as part of fiscal year (FY) 2015 audit planning, OIG Office of Audits personnel met with officials from each of the SEC's divisions and offices, including regional offices. Through these meetings, the Office of Audits staff both obtained an understanding of the organizations' roles, responsibilities, structure, and risks, and performed outreach about the OIG's missions and operations.



CONGRESSIONAL REQUESTS AND BRIEFINGS

The OIG continued to keep Congress fully and currently informed of OIG activities through briefings, reports, meetings, and responses to Congressional inquiries. Throughout the semiannual reporting period, OIG staff briefed Congressional staff about OIG work and issues impacting the SEC.

For example, in April 2014, senior OIG staff met with bipartisan staff of the U.S. House of Representatives Committee on Financial Services to update the Committee on the OIG's planned audit work.

Further, in July 2014, the OIG provided an updated response to a request from the Ranking Members of the U.S. Senate Committee on the Judiciary and the Permanent Subcommittee on Investigations of the U.S. Senate Committee on Homeland Security and Governmental Affairs for information about closed audits, evaluations, and investigations that were not publicly disclosed. The OIG also responded to a formal request from the U.S. House of Representatives Committee on Oversight and Government Reform for the OIG's March 2014 report about the leak of nonpublic information from an Executive Session of a closed Commission meeting.



THE OIG'S STATEMENT ON THE SEC'S MANAGEMENT AND PERFORMANCE CHALLENGES

The Reports Consolidation Act of 2000 requires the SEC OIG to identify and report annually on the most serious management challenges that the SEC faces. To identify management challenges, we review past and ongoing audit, investigation, and evaluation work. In deciding whether to identify an issue as a challenge, we consider its significance in relation to the SEC's mission; its susceptibility to fraud, waste, and abuse; and the SEC's progress in addressing the challenge. We compiled this statement on the basis of the work we completed over the past year; our knowledge of the SEC's programs and operations; and feedback from SEC staff and the U.S. Government Accountability Office (GAO) auditors who conduct the SEC's annual financial statement audit.

MANAGEMENT AND PERFORMANCE CHALLENGES

Regulatory Oversight

Over the past decade, the markets, products, and participants that the SEC oversees and regulates—including investment advisers, mutual and exchange-traded funds, and broker-dealers—have grown in size and complexity, creating several challenges for the SEC as it carries out its mission

to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. For example, following the 2007–2009 financial crisis and enactment of the Dodd-Frank Act, the SEC's responsibilities for providing regulatory oversight expanded significantly. The Dodd-Frank Act mandated that the agency undertake the largest and most complex rulemaking agenda in its history. Specifically, the Dodd-Frank Act includes some 90 provisions that require SEC rulemaking and more than 20 other provisions that require studies or reports. In addition, the JOBS Act requires the SEC to write new rules and issue studies on capital formation, disclosure, and registration requirements. In her September 9, 2014 testimony before the United States Senate Committee on Banking, Housing, and Urban Affairs, the SEC Chair stated that the Commission has proposed or adopted rules with respect to approximately 90 percent of the provisions of the Dodd-Frank Act that mandate Commission rulemaking. However, more remains to be done on both the Dodd-Frank Act and JOBS Act rulemakings, and the agency's ability to effectively prioritize and manage its resources will be key to the successful and timely completion of this work.

In addition to the resources needed for rulemaking, the SEC has identified an immediate and pressing

need for ensuring sufficient examination coverage of registered investment advisers. According to the Chair's recent Congressional testimony, during FY 2013, due to significant resource constraints, the SEC examined only about 9 percent of these advisers, although the total amount of assets managed by SEC-registered advisers increased from \$43.8 trillion in April 2011 to \$62.3 trillion in August 2014. The Chair further testified that the number of examiners per trillion dollars in investment adviser assets under management dropped from 19 in 2004 to 8 in 2014. In its first Report on Objectives, the SEC's Office of Investor Advocate, which was established by the Dodd-Frank Act, described the agency's ability to properly oversee registered investment advisers as a "substantial and continuing risk to investors." To ensure the SEC can adequately protect investors, the Office of Investor Advocate recommended that Congress immediately appropriate funds to increase the number of SEC staff who examine registered investment advisers, and authorize the SEC to collect fees from investment advisers to create a more stable and scalable source of revenue for investment adviser examinations in future years.

Finally, to keep pace with increasingly complex markets, the SEC is investing in its information technology (IT) infrastructure, developing new analytic capabilities, and deploying tools and platforms to store and process increasing volumes of data. Such improvements include:

- standardizing enterprise-wide platforms;
- modernizing the agency's SEC.gov website and the Electronic Data Gathering, Analysis and Retrieval (EDGAR) filer systems;
- integrating structured and unstructured data sources;
- improving internal search and electronic discovery capabilities and providing complex, predictive analytical capabilities; and
- assisting with automated triage and early detection of fraud or abuse at the earliest possible stage.

We are planning audit work in these areas to assess the SEC's approaches for addressing newly expanded responsibilities, effectively targeting and monitoring market participants based on risk and available resources, and establishing an effective approach to modernizing its IT infrastructure.

Information Security

The SEC generates and collects commercially valuable, market-sensitive, proprietary, and other nonpublic information. To accomplish the SEC's mission, the agency shares sensitive information internally among its divisions and offices and externally with the regulated community and financial regulators. During FY 2014, we completed several evaluations and investigations of weaknesses in the agency's controls over information security.

For example, we completed our FY 2013 evaluation of the effectiveness of the SEC's information security programs and practices and whether the SEC's OIT has policies, procedures, and practices consistent with Federal Information Security Management Act (FISMA) requirements (*Federal Information Security Management Act: Fiscal Year 2013 Evaluation*, Report No. 522, issued March 31, 2014). Overall, we found several areas in which the SEC has improved controls over its information security. Specifically, OIT has made significant progress establishing (1) a risk management program; (2) an incident response and reporting program; and (3) an enterprise-wide business continuity and disaster recovery program, consistent with FISMA requirements and Office of Management and Budget (OMB) and National Institute of Standards and Technology guidelines. However, as we previously reported in 2013, we found that OIT had not taken corrective action on some issues identified during the prior FISMA evaluations. We also found that the agency needs to enhance its efforts regarding contractor systems, multi-factor authentication, user accounts, and configuration management. The agency is taking steps to address our concerns.

In addition, in our *Review of the SEC's Practices for Sanitizing Digital Information System Media*, Report No. 521, issued May 30, 2014, we identified deficiencies in the agency's digital media sanitization and disposal practices, which increased the risk of unauthorized release of information that is potentially damaging to the agency, its employees and contractors, and entities that the SEC regulates. We recommended improvements in the SEC's storage of media awaiting sanitization; processes for ensuring all laptop computer hard drives are encrypted; controls over inventorying and tracking hard drives during the sanitization process; sanitizing failed disks that were part of the agency's data center redundant storage arrays; and controls over the third-party destruction of media. The agency concurred with the recommendations and has developed a corrective action plan. During the course of the review, we also found on the SEC's enterprisewide network drives a large amount of sensitive, nonpublic information that was available to all employees and contractors with access to the network—a situation the agency took immediate action to correct.

In FY 2014, the OIG also investigated allegations that a departing SEC employee may have stolen sensitive documents. Specifically, the OIG learned that the SEC's Office of Records Management Services had identified sensitive information in materials that were being shipped from the SEC to the employee's new employer, a private firm, and SEC management was concerned about the potential release of nonpublic information. The OIG reviewed the employee's documents, identified nonpublic information, prevented information from leaving the SEC, and recovered other nonpublic information from the employee's residence. As a result, the OIG recommended improvements to the agency's exit procedures and policies. In response, the SEC instituted a revised records clearance form, offered additional training, and has regularly reminded employees via email about proper care of nonpublic information.

We opened another investigation into concerns about the unauthorized disclosure of nonpublic information from an Executive Session of a "closed" (nonpublic) Commission meeting. The OIG was notified that information about the Commission's deliberations and voting during the closed Commission meeting had been disclosed, without authorization, to a news reporter. Subsequently, nonpublic information was included in a news article by several reporters that was published before information about the closed Commission meeting was made public. The OIG was unable to determine which specific individual or individuals had improperly disclosed information from the closed Commission meeting. However, we determined that an SEC employee may have confirmed to one of the news reporters certain nonpublic information. The OIG also learned during its investigation that certain Commission-related information was transmitted using personal, nonsecure email. The OIG provided the results of its investigation to the agency for appropriate action. The SEC has taken a number of positive steps to address control weaknesses we identified.

Further, the OIG investigated allegations that a former SEC employee, who was a candidate for a position with an SEC regional office, possessed documents containing SEC nonpublic information that the former employee had obtained through his prior employment with the SEC. During the course of its investigation, the OIG interviewed the former employee, who admitted possessing copies of SEC examination reports that he had worked on while employed with the SEC. The former employee agreed to cooperate with the investigation, and we recovered SEC documents containing nonpublic information from that former employee. We determined that one of the documents that the former employee had copied and taken with him when he left the SEC was marked "Privileged & Confidential." The OIG provided a report of its findings to SEC management for informational purposes.

Finally, as part of its audit of SEC's FY 2013 and FY 2012 financial statements, GAO assessed the effectiveness of the SEC's information security controls for protecting the confidentiality, integrity, and availability of the SEC's key financial systems and information. Although GAO reported¹ that the SEC had implemented and made progress in strengthening information security controls, GAO found weaknesses in several controls over a key financial system's network, servers, applications, and databases. GAO reported that "[t]he information security weaknesses existed, in part, because SEC did not effectively oversee and manage the implementation of information security controls during the migration of this key financial system to a new location." GAO concluded that until the SEC mitigates control deficiencies and strengthens the implementation of its security program, "its financial information and systems may be exposed to unauthorized disclosure, modification, use, and disruption."

We will continue to review the SEC's controls over sensitive, nonpublic information, including OIT's security controls for the SEC's information systems.

Acquisition Management

Although the SEC has made progress in improving its acquisitions policies and procedures, the OIG continues to find the SEC's monitoring of its contracts to be a challenge. For example, during our *Review of the SEC's Practices for Sanitizing Digital Information System Media*, we observed that SEC policy and the contract with the agency's media disposal vendor required the vendor to provide certificates of destruction that included the name of the individual(s) who witnessed the destruction and indicated the type and quantity of media destroyed and the destruction method used. However, SEC employees did not always witness the vendor's destruction of the agency's digital media (including computer hard drives, compact discs, digital video discs, and data tapes used to process and

store often sensitive information), or ensure that the vendor provided accurate or complete certificates of destruction. According to the Contracting Officer's Representative for the media disposal contract, the vendor provided certificates that included only an inventory of the media by weight. Without recording hard drive serial numbers or other identifying information for destroyed devices, there is no proof of which devices were destroyed. For example, one certificate of destruction from a regional office indicated that 15 hard drives were destroyed when, in fact, 15 boxes of hard drives were destroyed. In response to our draft report, SEC management stated that the contract with the media disposal vendor is being transferred from the Facilities Branch to OIT, and it will be the Contracting Officer's Representative's responsibility to ensure the correctness of certificates of destruction.

In addition, we completed the *Audit of the SEC's Physical Security Program*, Report No. 523, issued on August 1, 2014, and reported that the SEC's Office of Security Services (OSS) outsourced security systems responsibilities to a contractor but did not provide sufficient oversight to monitor the contractor's performance. Also, the competencies of contractor security specialists did not always match their assigned roles and responsibilities.

We will perform additional work in FY 2015 to assess the SEC's progress in improving its acquisitions management and contract oversight.

Financial Management

GAO's audit of the SEC's FY 2013 financial statements² found that the SEC's financial statements were fairly presented, in all material respects, in conformity with U.S. generally accepted accounting principles.³ In addition, GAO reported that, during FY 2013, the SEC made notable progress in addressing internal control deficiencies that GAO had reported in FY 2012. Specifically, in December 2013, GAO reported that the SEC "sufficiently

addressed the deficiencies in its financial reporting for budgetary resources and property and equipment such that [GAO] no longer consider[s] the remaining control deficiencies in these areas, individually or collectively, to represent significant deficiencies as of September 30, 2013.” However, as previously discussed, GAO’s FY 2013 audit identified new deficiencies in the SEC’s internal control over information security. GAO also reported that the SEC was not able to adequately address certain control deficiencies in information security reported in FY 2012. GAO considered the aggregate of these deficiencies in information security to represent a significant deficiency in SEC’s internal control over financial reporting.⁴

In addition, in May 2014, GAO reported identifying several new deficiencies in the SEC’s internal control over financial reporting that GAO did not consider to be material weaknesses or significant deficiencies, either individually or collectively, but nonetheless warranted SEC management’s attention.⁵ These deficiencies were related to:

- procedures for transferring disgorgement and penalty-related funds to the Department of the Treasury;
- monitoring of disgorgement and penalty related cases filed in courts;
- segregation of duties for recording disgorgement and penalty-related financial data;
- safeguarding of SEC cash receipts received at its service provider;
- recording of property and equipment transactions; and
- management’s review of legal contingencies and significant events.

GAO made 9 new recommendations to address these deficiencies in the SEC’s controls over financial reporting and noted that, with these new recommendations, the SEC has 25 recommendations that need to be addressed. Corrective action is in prog-

ress for all outstanding recommendations. We will continue to monitor the SEC’s financial management and reporting controls and actions to address open recommendations.

Human Capital Management

In 2013, we reported that GAO had assessed the SEC’s organizational culture and its personnel management challenges and efforts to address those challenges. In its July 2013 report,⁶ GAO concluded that the SEC “has not consistently or fully implemented effective personnel management” and, although the agency had taken some steps, most of its efforts were in the early stages and could be enhanced. GAO identified four key areas where continued improvement was needed: (1) workforce planning; (2) performance management; (3) communication and collaboration; and (4) personnel management assessment. GAO made seven recommendations to improve the SEC’s personnel management, including developing comprehensive workforce plans,⁷ implementing mechanisms to monitor how supervisors use the performance management system, conducting periodic validations of the system, exploring collaboration practices of leading organizations, and regularly assessing these efforts. SEC management agreed with GAO’s recommendations and, on May 5, 2014, the Office of Human Resources (OHR) submitted a proposal to GAO to close the recommendations.

In June 2014, the Office of Personnel Management (OPM) issued a report on its evaluation of the SEC. OPM reported “commendable [human resources] process improvement initiatives and a system of transparency and accountability which resulted in continuous improvement of human resources programs.” OPM also reported improvements to the agency’s delegated examining operations since a previous evaluation in 2010. However, OPM found issues that were repeat findings from the 2010 review, including the “lack of evidence of an effective quality review process, incorrect [job opportu-

nity announcement] content, insufficient applicant notifications, insufficient documentation of minimum qualifications, and problems with auditing of certificates.” OPM also reported that the SEC still did not have a comprehensive workforce plan, although the agency had a workforce planning process conducted by the senior executive within each office. Finally, OPM identified a violation of merit promotion procedures under 5 CFR 335.103(c)(1)(iv). In February 2013, the SEC discontinued the promotion practice that caused the violation; however, OPM required the SEC to take corrective action and recommended other actions to improve the SEC’s human capital management.

Lastly, as an employer, the SEC seeks to hire and retain a skilled and diverse workforce, and to ensure that all decisions affecting employees and applicants are fair and ethical. Attracting, engaging, and retaining a technically proficient and diverse workforce is one of the agency’s stated strategic objectives.⁸ Section 342 of the Dodd-Frank Act required specific federal financial agencies, including the SEC, to establish, by January 21, 2011, an Office of Minority and Women Inclusion (OMWI), responsible for matters relating to diversity in management, employment, and business activities. In fiscal year 2014, we initiated an audit of the representation of minorities and women in the SEC’s workforce to help identify factors that may impact the SEC’s ability to increase the representation of minorities and women at the SEC, in general, and in senior management positions, in particular. We anticipate completing this work and issuing a report in FY 2015.

We will continue to monitor the SEC’s implementation of corrective actions from GAO’s and OPM’s reviews and the steps taken to improve the agency’s human capital management, including its efforts to hire and retain a skilled and diverse workforce.

Endnotes

- 1 GAO, *Information Security: SEC Needs to Improve Controls over Financial Systems and Data*, GAO-14-419 (April 17, 2014).
- 2 GAO’s FY 2013 financial statement audit included the SEC’s general purpose and Investor Protection Fund (IPF) financial statements.
- 3 GAO, *Financial Audit: Securities and Exchange Commission’s Financial Statements for Fiscal Years 2013 and 2012*, GAO-14-213R (December 16, 2013).
- 4 This significant deficiency pertained to SEC’s overall financial reporting, but not that of IPF because of the nature of IPF’s financial transactions during FY 2013.
- 5 GAO, *Management Report: Improvements Needed in SEC’s Internal Controls and Accounting Procedures*, GAO-14-416R (May 12, 2014).
- 6 GAO, *Securities and Exchange Commission Improving Personnel Management Is Critical for Agency’s Effectiveness*, GAO-13-621 (July 2013).
- 7 GAO first recommended that SEC develop such a plan in 2001. See GAO-01-947.
- 8 U.S. Securities and Exchange Commission Strategic Plan, Fiscal Years 2014–2018.



COORDINATION WITH OTHER OFFICES OF INSPECTOR GENERAL

During this semiannual reporting period, the SEC OIG coordinated its activities with those of other OIGs, pursuant to Section 4(a)(4) of the Inspector General Act of 1978, as amended.

Specifically, the OIG participated in the meetings and activities of the Council of Inspectors General on Financial Oversight (CIGFO), which the Dodd-Frank Act established. The chairman of CIGFO is the IG of the Department of the Treasury (Treasury). Other members of the Council, in addition to the IGs of the SEC and Treasury, are the IGs of the Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Department of Housing and Urban Development, the Federal Deposit Insurance Corporation, the Federal Housing Finance Agency, the National Credit Union Administration, and also the Special Inspector General for the Troubled Asset Relief Program. As required by the Dodd-Frank Act, CIGFO meets at least once every 3 months. At the CIGFO meetings, members share information about their ongoing work, with a focus on concerns that may apply to the broader financial sector and ways to improve financial oversight.

Further, the SEC OIG's Office of Audits participated in a CIGFO working group that assessed the extent to which the operations of the Financial Stability Oversight Council were consistent with the expectations outlined in its transparency policy. The final report was issued on July 1, 2014, and can be accessed through CIGFO's website. In addition, the Office of Audits participated in a CIGFO working group that is assessing the Financial Stability Oversight Council's response to recommendations for continued oversight of interest rate risk. The working group expects to issue a final report summarizing its findings in April 2015.

The SEC IG attended meetings of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and continued to serve as the Chairman of the CIGIE Investigations Committee. The mission of the Investigations Committee is to advise the IG community on issues involving criminal investigations and criminal investigations personnel and to establish criminal investigative guidelines.

In addition, the Office of Audits continued to participate in various CIGIE activities. For example, a representative of the Office of Audits was a member of a working group that revised the *Guide for*

Conducting External Peer Reviews of the Audit Organizations of Federal Offices of Inspector General. Office of Audits staff also participated in activities of the CIGIE Federal Audit Executive Council (FAEC), including attending training that FAEC provided.

Lastly, OIG staff participated in the activities of the Council of Counsels to the Inspectors General, the CIGIE Records Management Working Group, and the CIGIE External Affairs Liaisons' Group.



AUDITS AND EVALUATIONS

OVERVIEW

The **OIG** Office of Audits conducts, coordinates, and supervises independent audits and evaluations of the agency's programs and operations at the SEC's headquarters and 11 regional offices. The Office of Audits also hires, as needed, contractors and subject matter experts, who provide technical expertise in specific areas, to perform work on the **OIG's** behalf. In addition, the Office of Audits monitors the SEC's progress in taking corrective actions on recommendations in **OIG** audit and evaluation reports.

Each year, the Office of Audits prepares an annual audit plan. The plan includes work that the Office selects for audit or evaluation on the basis of risk and materiality, known or perceived vulnerabilities and inefficiencies, resource availability, and information received from Congress, internal SEC staff, GAO, and the public.

The Office conducts audits in compliance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States. **OIG** evaluations follow applicable CIGIE Quality Standards for Inspection and Evaluation and GAGAS. At the completion of an audit or evaluation, the **OIG** issues an independent report in which it identifies deficiencies and makes

recommendations to correct those deficiencies or increase efficiencies in an SEC program.

To improve the efficiency and quality of our audits and evaluations, the Office of Audits began using a team approach to auditing. Further, in July 2014, the Office of Audits implemented an audit management software system to increase auditor productivity and facilitate supervisory review.

COMPLETED AUDITS AND EVALUATIONS

[Review of the SEC's Practices for Sanitizing Digital Information System Media \(Report No. 521\)](#)

The SEC generates and collects commercially valuable, market-sensitive, proprietary, and other nonpublic information. To safeguard against unauthorized disclosure of this information, the SEC requires that digital information system media (media), including computer hard drives, compact discs, digital video discs, and data tapes used to process and store information, be sanitized before disposal. Effective sanitization minimizes the risk of unauthorized release of information that is potentially damaging to the agency, its employees and contractors, and those entities that the SEC

regulates. To determine whether the SEC effectively sanitized surplus media before its disposal, the OIG hired a contractor to evaluate the agency's media sanitization practices.

During this review, we identified needed improvements in the agency's sanitization and disposal practices. Specifically, we found that the SEC did not always (1) securely store media awaiting sanitization, particularly surplus hard drives; (2) encrypt laptop computer hard drives; (3) inventory or track hard drives during the sanitization process; and (4) sanitize failed disks that were part of the agency's data center redundant storage arrays before returning those disks to a vendor. We also determined that SEC employees did not always witness the third-party destruction of media or obtain accurate or complete certificates of destruction.

The OIG issued a final report to the agency on May 30, 2014. We made eight recommendations for corrective action. The recommendations addressed surplus media storage, laptop encryption, inventory and tracking of surplus hard drives, sanitization of failed hard disks used in disk arrays, certificates of destruction, media sanitization policies and procedures, and implementation of verification activities. Management concurred with all of the recommendations and two recommendations were closed before the end of the reporting period. The remaining recommendations were pending but will be closed upon completion and verification of corrective action.

Also during our review, we found on the SEC's enterprisewide network drives large amounts of sensitive, nonpublic information that was available to all employees and contractors with access to the network. Upon notification, management restricted access to the drives, pending further review by OIT. Subsequently, OIT confirmed that it took the drive off line and sanitized it and that the drive is no longer in use.

A summary of the OIG's report is available on its website at www.sec.gov/oig/reportspubs/521.pdf.

Audit of the SEC's Physical Security Program (Report No. 523)

GAO has designated Federal real property management as a government high-risk area due, in part, to the continued challenge of protecting Federal facilities. The SEC's OSS is responsible for the physical security and safety of SEC staff and facilities at the SEC's 11 regional offices, 2 data centers, and headquarters in Washington, D.C. In 2011 and 2012, the OIG investigated physical security violations and recommended a review of the SEC's physical security program. As a result, the OIG retained a contractor to assess the SEC's policies, procedures, and controls for safeguarding personnel and property and preventing unauthorized access to its facilities.

The objectives of the audit were to assess (1) OSS' compliance with Federal physical security standards and the SEC's policies and procedures; (2) the effectiveness of OSS' physical security policies and procedures; and (3) the adequacy of OSS' procedures and practices to oversee the physical security of the SEC's facilities.

To conduct the audit, we visited the SEC's headquarters, three of its regional offices, and its two data centers; we also obtained information from personnel at the remaining SEC locations. From our observations and the information we obtained, we determined that improvements were needed in the SEC's physical security controls. Specifically, we identified vulnerabilities relating to the agency's facility risk assessment and facility security plans; control of SEC-issued badges; some access-controlled doors; and monitoring of the SEC's physical access control and intrusion detection systems. We also found that the SEC's security system contractor did not always notify OSS of alarm conditions and that an SEC facility lacked sufficient security measures to prevent

unauthorized, undetected, and undocumented access to key IT assets.

During the audit, management took action to address some of the conditions we observed. However, we found that the conditions noted occurred because OSS did not adequately manage and administer the SEC's physical security program in several respects. The overall results of our audit indicated that actions are required to establish a comprehensive physical security program and that doing so will reduce the risk to SEC personnel, facilities, and property.

We issued our final report on August 1, 2014, and made nine recommendations for corrective action. The recommendations addressed policies and procedures; risk assessments; facility security plans; issuance of badges; access-controlled doors; contractor performance; data center monitoring and controls; and security specialist training. Management concurred with eight of the recommendations and partially concurred with one recommendation. The recommendations will be closed upon completion and verification of corrective action but were pending at the close of this reporting period.

Controls Over the SEC's Inventory of Laptop Computers (Report No. 524)

Laptop computers (laptops) are portable and easy to conceal and often contain sensitive information. Consequently, they are at risk of loss and theft and must be properly safeguarded and accounted for. To support the agency's mission, SEC employees and contractors use laptops, some of which process and store commercially valuable, market-sensitive, proprietary, and other nonpublic information. Recent OIG investigative and review work identified weaknesses in the SEC's laptop inventory records and encryption controls. The OIG conducted this audit to evaluate the effectiveness of the agency's IT inventory program and its controls over laptops. During the audit, we reviewed a statistical sample of 244 laptops assigned to the SEC's headquarters and

3 of its regional offices. We also reviewed a judgmental sample of an additional 244 laptops assigned to those offices, for a total of 488 laptops reviewed. We determined that the SEC had addressed prior OIG recommendations about laptop accountability and had controls for safeguarding laptops throughout their lifecycles. However, we identified needed improvements.

Specifically, we found that the SEC's IT inventory contained incorrect information for a significant number of laptops. For example, the inventory had an incorrect location for 82 of the 488 laptops we reviewed and incorrect user information for 105 of those 488 laptops. In addition, 24 laptops could not be accounted for, and 4 laptops in the custody of users were not included in the inventory. Further, the SEC's procedures for sharing information about lost or stolen laptops were inadequate.

We noted that these weaknesses existed because SEC personnel did not always understand their roles and responsibilities, and related policies and procedures were inadequate, had not been properly communicated, and were not consistently followed. We also found that the SEC may be unaware of lost or stolen laptops and that, if such laptops are not protected by encryption software (which we reported as a finding in our May 2014 *Review of the SEC's Practices for Sanitizing Digital Information System Media*, Report No. 521), the SEC is at risk for the unauthorized release of sensitive, nonpublic information. Finally, we identified a lack of segregation of duties and compensating controls in the SEC's IT inventory management system, which creates opportunities for misappropriation of laptops without management's knowledge.

The OIG issued its final report on September 22, 2014. We noted that OIT is undertaking an agency-wide IT inventory, which includes laptops, and plans to replace its inventory management system. However, we found that additional actions are needed to improve the agency's controls over laptops. We

made four recommendations for corrective action that address policies and procedures for maintaining inventories of laptops; coordination between OIT organizations; notifications about unaccounted-for laptops; and a review of IT inventory management system user accountability. Management concurred with all of our recommendations. The recommendations will be closed upon completion and verification of corrective action, but were pending at the close of this reporting period.

The OIG's report is available on its website at www.sec.gov/oig/reportspubs/524.pdf

Analysis of the SEC's Compliance with Conference Approval and Reporting Requirements for Fiscal Year 2014

Section 742(c) of Title VII, Division E, of the Consolidated Appropriations Act, 2014 (P.L. 113-76) requires Federal agencies to report to their IGs conferences that cost more than \$20,000, within 15 days after the date of the conference. The OIG analyzed whether the SEC complied with this reporting requirement, as well as agency policy for approving conferences that meet certain cost thresholds, for FY 2014.

To perform this review, the OIG met with personnel from the Office of Financial Management (OFM) and analyzed supporting documents for the 19 conferences that were reported to the OIG as of September 30, 2014. The OIG found that, for the 19 conferences reported to the OIG, the SEC reported all required information within 15 days of the conference date. The OIG also found that approvals for each of the 19 reported conferences complied with OFM's approval requirements.

In FY 2015, the OIG plans to further analyze the SEC's FY 2014 conference expenditures and assess the agency's compliance with additional statutory reporting requirements for conferences costing more than \$100,000. We will also determine whether the

SEC complied with Federal and agency requirements for planning and conducting conferences to ensure conference-related spending was legal, reasonable, and necessary.

The OIG's memorandum describing its analysis is available on its website at www.sec.gov/about/offices/oig/inspector_general_reppubs_other.shtml.

ONGOING AUDITS AND EVALUATIONS

Audit of the SEC Office of the Ethics Counsel's Oversight of Employee Security Holdings

The *Supplemental Standards of Ethical Conduct for Members and Employees of the Securities and Exchange Commission* (supplemental ethics regulations), which the SEC adopted in August 2010 with the Office of Government Ethics' concurrence, prohibit SEC members and employees from knowingly purchasing or holding securities of entities that the SEC directly regulates and also restricts their personal securities trading. During this semiannual reporting period, the OIG's Office of Investigations notified the Office of Audits that during investigations of SEC employees' possession of, or failure to divest, prohibited holdings, the Office of Investigations discovered potential problems that might warrant an audit of the SEC Office of the Ethics Counsel's (OEC) processes.

In response, the OIG initiated an audit of OEC's oversight of employee security holdings. The overall objective is to evaluate OEC's efforts to ensure that SEC members and employees comply with the supplemental ethics regulations that prohibit certain securities holdings and restrict trading. Specifically, the audit will determine whether OEC has adequate controls to prevent, detect, and correct SEC members' and employees' noncompliance with the applicable provisions of the supplemental ethics regulations.

We expect to issue a report summarizing our findings during the next semiannual reporting period.

Audit of the Representation of Minorities and Women in the SEC's Workforce

The OIG initiated an audit of workforce diversity at the SEC in response to a request received from several members of the U.S. House of Representatives Committee on Financial Services during the previous semiannual reporting period. The Committee members sent similar requests to the IGs of five other Federal financial regulators.

Section 342 of the Dodd-Frank Act required Federal agencies that oversee the financial services industry, including the SEC, to establish an OMWI. The SEC formally established its OMWI in July 2011. To accomplish its mission of enhancing diversity and inclusion in the SEC's workforce, OMWI works closely with the SEC's OHR and Office of Equal Employment Opportunity (OEEO).

To determine the SEC's workforce diversity, the SEC OIG is assessing the operations, policies, and procedures at the SEC's OHR, OMWI, and OEEO related to the representation of minorities and women in the SEC workforce from FY 2011 through FY 2013.

The overall objectives of the audit are to assess the SEC's efforts to (1) increase the representation of minorities and women at the SEC; (2) create a workplace free of systemic discrimination of minorities and women; and (3) provide equal opportunity for minorities and women to obtain senior management positions. We developed these objectives in coordination with the OIGs from the five other Federal financial regulators that received requests from the

Committee members. We will also seek to identify factors that may impact the SEC's ability to increase the representation of minorities and women at the SEC generally, and in senior management positions particularly.

We expect to issue a report summarizing our findings during the next semiannual reporting period.

Federal Information Security Management Act: Fiscal Year 2014 Evaluation

FISMA provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets. FISMA also requires IGs to annually assess the effectiveness of agency information security programs and practices and report the results to OMB.

The OIG has hired a contractor to perform the FY 2014 FISMA evaluation on the OIG's behalf. The overall objective of the FY 2014 FISMA evaluation is to assess the SEC's information systems and provide the OIG with input for the SEC's response to the *FY 2014 Inspector General Federal Information System Security Management Act Reporting Metrics*, which contains standardized questions that all executive agencies are required to answer. As required by FISMA, the evaluation will include a review of the SEC's information security posture based on guidance issued by OMB, the Department of Homeland Security, and the National Institute of Standards and Technology.

The contractor will summarize its findings and recommendations in a report, which we will issue in the next semiannual reporting period.



INVESTIGATIONS

OVERVIEW

The OIG Office of Investigations investigates allegations of criminal, civil, and administrative violations relating to SEC programs and operations by SEC employees, contractors, and outside entities. These investigations may result in criminal prosecutions, fines, civil penalties, administrative sanctions, and personnel actions.

The Office of Investigations adheres to the CIGIE Quality Standards for Investigations and applicable U.S. Attorney General guidelines. The Office of Investigations continues to enhance its systems and processes to meet the demands of the OIG and to provide high quality investigative work products.

Investigations require extensive collaboration with separate SEC OIG component offices, other SEC divisions and offices, and outside agencies, as well as coordination with DOJ and state prosecutors. Through these efforts, the Office of Investigations is able to thoroughly identify vulnerabilities, deficiencies, and wrongdoing that could negatively impact the SEC's programs and operations.

The Office of Investigations manages the OIG Hotline, which is available 24 hours a day, 7 days a week, to receive and process tips and complaints about fraud, waste, or abuse related to SEC pro-

grams and operations. The Hotline allows individuals to report their allegations to the OIG directly and confidentially.

In June 2014, the Attorney General authorized the Office of Investigations to exercise law enforcement authority in accordance with Section 6(e) of the Inspector General Act of 1978, as amended, and the Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority. This authority allows the OIG's special agents to exercise law enforcement powers and enhances our ability to conduct criminal investigations.

STATUS OF PREVIOUSLY REPORTED INVESTIGATIONS

Violation of SEC Supplemental Ethics Rules by a Staff Accountant

(Case No. 14-0070-I; previously OIG-585)

As discussed in our previous Semiannual Report, an OIG investigation determined that an SEC staff accountant held certain securities that SEC employees were prohibited from owning under the SEC's supplemental ethics regulations and failed to report those holdings on government financial disclosure forms. The OIG referred the matter to the United States Attorney's Office (USAO) for

possible prosecution and reported its interim findings to SEC management. Thereafter, the staff accountant resigned from the SEC, and the USAO declined prosecution in February 2014.

During this semiannual reporting period, the OIG issued a final report of investigation to SEC management and closed the investigation.

False Statements Related to Prohibited Financial Holdings (Case No. 14-0071-I; previously OIG-598)

Also as described in our previous Semiannual Report, an OIG investigation found evidence that an SEC staff accountant falsely certified that his security holdings complied with the SEC's supplemental ethics regulations and falsely claimed that he had divested certain prohibited holdings. The OIG referred the matter to the USAO, which accepted the case for prosecution.

The USAO filed a criminal complaint against the staff accountant, charging him with three counts of making false statements to the SEC about his ownership of prohibited securities. The staff accountant was arrested in November 2013.

In April 2014, the USAO entered into a deferred prosecution agreement with the staff accountant. If the staff accountant complied with all terms and conditions for 6 months after signing the agreement, the USAO would not prosecute the staff accountant for the offenses in the complaint. The agreement also required the staff accountant to cooperate fully with the USAO, as well as the SEC, and to resign from the SEC within 3 days of signing the agreement. The staff accountant subsequently resigned from the SEC. The OIG issued a report of investigation to agency management and closed the investigation.

Departing SEC Employee's Attempt to Remove Nonpublic Information from the SEC (Case No. 14-0012-I; previously OIG-600)

As reported in our previous Semiannual Report, the OIG investigated allegations that a departing SEC employee may have stolen sensitive documents. Specifically, the OIG learned that nonpublic information was identified in materials that were being shipped from the SEC to the employee's new employer.

In March 2014, the OIG issued an Investigative Memorandum to SEC management, identifying how the SEC could improve its employee exit process. In this Memorandum, the OIG recommended that the agency revise its policies and procedures to require the divisions and offices of departing employees to review the documents that employees plan to remove from the SEC, determine which documents departing employees are authorized to remove, and document this determination. The OIG further recommended that management communicate to employees the revised exit procedures and their obligation to ensure nonpublic information is not improperly disclosed.

The agency implemented the recommendations during this semiannual reporting period. Specifically, management instituted a revised records clearance form that requires a departing employee and his or her supervisor to attest that they have reviewed the documents the employee plans to remove from the SEC and, to their knowledge; no government records are being removed. Management also communicated its records clearance procedure to all employees; added language to pertinent training materials; and notified employees of their responsibility to comply with laws, rules, and regulations prohibiting the unauthorized disclosure of nonpublic information. As a result, the OIG concurred with closure of the recommendations.

Unauthorized Disclosure of Nonpublic Information from Executive Session Commission Meeting

(Case No. 14-0013-I; previously OIG-601)

Our previous Semiannual Report described the results of the OIG's investigation into concerns about the unauthorized disclosure of nonpublic information from an Executive Session of a "closed" (non-public) Commission meeting. The OIG was unable to determine which specific individual or individuals had improperly disclosed information from the closed Commission meeting. However, the OIG found that an SEC employee may have confirmed certain nonpublic information to a news reporter. Additionally, the OIG learned during its investigation that an SEC employee and a Commissioner had transmitted certain Commission-related information using their personal, nonsecure email.

In March 2014, the OIG provided the results of its investigation to the agency for appropriate action. In response to the OIG's report, management notified the OIG that the SEC employee who may have confirmed certain nonpublic information to a news reporter had resigned from the SEC. Management further notified the OIG that it had determined that no further action was necessary with respect to the other individuals named in the report.

COMPLETED INVESTIGATIONS

SEC Senior Officer's Acceptance of Direct Payment for International Travel

(Case No. 14-0009-I)

The OIG investigated allegations that an SEC Senior Officer (SO) accepted direct reimbursement of travel expenses, which constituted a monetary gift, from an international organization that sponsored a conference where the SO presented an academic paper on financial research. SEC administrative regulations expressly prohibit an SEC employee from directly receiving reimbursement from the

sponsor of a meeting outside of the SEC, and ethics standards prohibit the receipt of gifts from prohibited sources or because of an employee's official position.

The OIG found that the SO had received reimbursement for the travel from the organization hosting the event, through an electronic funds transfer to the SO's personal bank account. However, the OIG determined that the sponsoring organization did not receive clear instructions from the SEC's OFM on how to submit an international electronic funds transfer to reimburse the SEC for the SO's travel. As a result, the sponsoring organization submitted payment directly to the SO in an attempt to remedy the situation. After the SO received a notice from OFM about the payment several months later, the SO reimbursed OFM for the full amount.

Further, the OIG identified possible vulnerabilities in the procedures used to reimburse the SEC for host-paid travel. We referred these issues to the OIG Office of Audits for review. In May 2014, the OIG reported its findings to management for informational purposes only, as the SO had resigned from the SEC.

Allegations of Time and Attendance Fraud by SEC Managers

(Case No. 14-0017-I)

The OIG investigated allegations that certain SEC regional office managers engaged in time and attendance fraud for over a year. The complaint was similar to ones the OIG had received in the past, and previous investigations by the OIG and the SEC's OHR did not substantiate the allegations.

Based on its review of available records, including turnstile records and video surveillance, the OIG determined that the allegations of time and attendance fraud by the managers were unfounded. The OIG provided its findings to management for informational purposes and closed the investigation.

Fraudulent SEC Internet Domains (Case No. 14-0182-I)

The OIG opened an investigation into allegations that an unknown Internet domain subscriber had created several fraudulent SEC Internet domains to further a suspected Internal Revenue Service (IRS)-related investment scam. These Internet domains were *olia-sec.us*, *sec-oig.us*, *sec-oia.us*, and *oca-sec.us*.

During its investigation, the OIG subpoenaed, obtained, and reviewed relevant documents from the Internet domain registrars for the fraudulent domains. The OIG also searched various Internet databases and reviewed information from numerous websites.

The OIG investigation did not identify the Internet domain subscriber who had created the fraudulent domains. However, the OIG coordinated with the IRS and confirmed that the fraudulent domains were no longer registered or active with the domain host company and, therefore, closed the investigation.

Unauthorized Transmission of Personally Identifiable Information by an SEC Employee (Case No. 14-0516-I)

The OIG initiated an investigation after being informed that an SEC headquarters employee sent an email to his personal Internet email account that attached a spreadsheet containing personally identifiable information (PII) of SEC employees.

During the investigation, the OIG discovered that the employee had also sent approximately 40 work-related and sensitive emails to his personal Internet email account over a 2-year period. The OIG did not find evidence that the employee disseminated the PII to unauthorized persons or used the documents for unauthorized purposes. Further, as a result of this incident, the agency provided the potentially affected SEC employees with credit monitoring for 1 year.

In September 2014, the OIG provided the results of its investigation to SEC management for any action deemed appropriate, and management's decision was pending at the end of the reporting period.

Allegation of Misconduct by an SEC Manager (Case No. 14-0543-I)

The OIG investigated an allegation that an SEC manager requested that a former subordinate employee retract a complaint the employee had previously made against the manager. The complaint had been included, along with other complaints, in an official reprimand of the manager.

During its investigation, the OIG interviewed the manager, who confirmed that she contacted the employee on two separate occasions and requested that she retract the complaint. The manager also admitted that she requested retraction of the complaint around the same time the employee sought reassignment to the manager's office and that she advocated on the employee's behalf. However, the OIG did not develop evidence that the manager requested the retraction in exchange for facilitating the employee's return to the manager's office. Moreover, the employee denied that she felt pressure from the manager to retract her complaint and, even though the employee did not retract her complaint, the manager ultimately selected the employee for a position in the manager's office.

In September 2014, the OIG provided the results of its investigation to SEC management for any action deemed appropriate, and management's decision was pending at the end of the reporting period.

Unauthorized Transmission of Nonpublic Information by an SEC Attorney (Case No. 14-0552-I)

The OIG opened an investigation after learning that an SEC regional office attorney transmitted a spreadsheet containing PII, as well as other non-

public information, to his personal Internet email account.

During its investigation, the OIG found that PII was stored in hidden columns of the spreadsheet. The OIG also determined that, over an approximate 1½ year period, the attorney transmitted about 30 nonpublic or SEC-sensitive unencrypted documents to this Internet email account. The OIG did not

find evidence that the employee disseminated PII or any nonpublic documents to unauthorized personnel or transmitted the documents for unauthorized purposes.

In September 2014, the OIG provided the results of its investigation to SEC management for any action deemed appropriate, and management's decision was pending at the end of the reporting period.



REVIEW OF LEGISLATION AND REGULATIONS

During this semiannual reporting period, the OIG reviewed and monitored the following legislation and regulations:

P.L. 113-76 Consolidated Appropriations Act, 2014 (Section 742, enacted January 18, 2014) (requiring Federal agencies to report conference costs and other conference data to Inspectors General);

P.L. 113-101 Digital Accountability and Transparency Act of 2014 (enacted May 9, 2014) (amending the Federal Funding Accountability and Transparency Act of 2006 to, among other things: (1) make specific classes of Federal agency spending data publicly available with more specificity than was previously reported; (2) require agencies to report this data on USASpending.gov; and (3) streamline agency reporting requirements);

H.R. 4934 Regulatory Agency Demilitarization Act (introduced June 23, 2014) (seeking to, among other things, prohibit certain Federal agencies from using or purchasing certain firearms);

H.R. 4937 Protection Against Wasteful Spending Act of 2014 (introduced June 23, 2014) (seeking to require, for fiscal years 2014–2020, federal agency heads to implement report recommendations made by an IG regarding wasteful and excessive spending

not later than four years after the submission of the report, unless the recommendation would be illegal under existing law);

H.R. 5170 Federal Records Accountability Act of 2014 (introduced July 23, 2014) (seeking to institute strict penalties, up to and including removal, for Federal employees found to have willfully and unlawfully concealed, removed, falsified or destroyed any government record; and also to prohibit an officer or an employee of a Federal agency from creating or sending a federal record using a non-official messaging system unless certain precautions are taken);

H.R. 5492 Inspector General Empowerment Act of 2014 (introduced September 16, 2014) (seeking to amend the Inspector General Act of 1978 to strengthen the independence of IGs); and

79 FR 30661 Privacy Act of 1974: Systems of Records/Notice to Establish a New System of Records and to Revise Two Existing Systems of Records (effective July 7, 2014) (among other things, revising the existing system of records implemented by the SEC OIG in accordance with “Office of Inspector General Investigative Files (SEC-43),” last published in Federal Register Volume 71, Number 105 on June 1, 2006.



MANAGEMENT DECISIONS

STATUS OF RECOMMENDATIONS WITH NO MANAGEMENT DECISIONS

Management decisions have been made on all audit reports issued before the beginning of this reporting period.

REVISED MANAGEMENT DECISIONS

No management decisions were revised during the period.

AGREEMENT WITH SIGNIFICANT MANAGEMENT DECISIONS

The OIG agrees with all significant management decisions regarding audit recommendations.

INSTANCES WHERE THE AGENCY REFUSED OR FAILED TO PROVIDE INFORMATION TO THE OIG

During this reporting period, there were no instances where the agency unreasonably refused or failed to provide information to the OIG.



TABLES

Table 1. List of Reports: Audits and Evaluations

Report Number	Title	Date Issued
521	Review of the SEC's Practices for Sanitizing Digital Information System Media	5/30/2014
523	Audit of the SEC's Physical Security Program	8/01/2014
524	Controls Over the SEC's Inventory of Laptop Computers	9/22/2014
Memorandum	Analysis of the SEC's Compliance with Conference Approval and Reporting Requirements for Fiscal Year 2014	9/30/2014

Table 2. Reports Issued with Costs Questioned or Funds Put to Better Use (Including Disallowed Costs)

	No. of Reports	Value
A. Reports issued prior to this period		
For which no management decision had been made on any issue at the commencement of the reporting period	0	\$0
For which some decisions had been made on some issues at the commencement of the reporting period	0	\$0
B. Reports issued during this period	0	\$0
Total of Categories A and B	0	\$0
C. For which final management decisions were made during this period	0	\$0
D. For which no management decisions were made during this period	0	\$0
E. For which management decisions were made on some issues during this period	0	\$0
Total of Categories C, D, and E	0	\$0

Table 3. Reports With Recommendations on Which Corrective Action Has Not Been Completed

During this semiannual reporting period, SEC management provided the OIG with documentation to support the implementation of OIG recommendations. In response, the OIG closed 22 recommendations related to 8 Office of Audits and Office of Investigations reports. The following table lists recommendations open 180 days or more.

Report Number and Title	Rec. No.	Issue Date	Recommendation Summary
489 - 2010 Annual FISMA Executive Summary Report	5	3/3/2011	Complete the logical access integration of the Homeland Security Presidential Directive 12 card no later than December 2011, as reported to the OMB on December 31, 2010.
501 - 2011 Annual FISMA Executive Summary Report	13	2/2/2012	Complete the implementation of the technical solution for linking multi-factor authentication to Personal Identity Verification (PIV) cards for system authentication and require use of the PIV cards as a second authentication factor by December 2012.
522 - Federal Information Security Management Act: Fiscal Year 2013 Evaluation	1	3/31/2014	Identify, evaluate, and document security controls for an externally-hosted system.
522 - Federal Information Security Management Act: Fiscal Year 2013 Evaluation	2	3/31/2014	Develop and implement formal, written procedures for conducting security assessments for externally-hosted and contractor systems.
522 - Federal Information Security Management Act: Fiscal Year 2013 Evaluation	3	3/31/2014	Require privileged users of an externally-hosted system to use multi-factor authentication for remote access and ensure multi-factor authentication is required for remote access to all other externally-hosted systems with privileged user accounts.
522 - Federal Information Security Management Act: Fiscal Year 2013 Evaluation	4	3/31/2014	Review certain user accounts to determine whether users still require access.

Table 3. Continued

During this semiannual reporting period, SEC management provided the OIG with documentation to support the implementation of OIG recommendations. In response, the OIG closed 22 recommendations related to 8 Office of Audits and Office of Investigations reports. The following table lists recommendations open 180 days or more.

Report Number and Title	Rec. No.	Issue Date	Recommendation Summary
522 - Federal Information Security Management Act: Fiscal Year 2013 Evaluation	5	3/31/104	Implement a centralized management tool that can automatically generate a list of user accounts.
522 - Federal Information Security Management Act: Fiscal Year 2013 Evaluation	6	3/31/2014	Periodically review and reconcile user accounts for a particular system, remove all accounts that do not require access, and then recertify the user accounts for the system.
522 - Federal Information Security Management Act: Fiscal Year 2013 Evaluation	8	3/31/2014	Conduct regularly scheduled scans of the SEC's workstations and laptops to identify unapproved software and take remedial action, such as removing software or obtaining approval for the software from the change control board.

Table 4. Summary of Investigative Activity for the Reporting Period of April 1, 2014 to September 30, 2014

Investigative Caseload	Number
Cases Open at Beginning of Period	23
Cases Opened During Period	25
Cases Completed During Period	3
Cases Closed During Period	8
Total Open Cases at End of Period	37

Criminal and Civil Investigative Activities	Number
Referrals for Prosecution	9
Accepted	2
Pending	1
Declined	6
Indictments/Informations	0
Arrests	0

Administrative Investigative Activities	Number
Removals, Retirements, and Resignations	8
Suspensions	0
Reprimands/Warnings/Other Actions	0

Complaints Received	Number
Hotline Complaints	121
Other Complaints	295
Total Complaints During Period	416

Table 5. References to Reporting Requirements of the Inspector General Act

Section	Inspector General Act Reporting Requirement	Pages
4(a)(2)	Review of Legislation and Regulations	24
5(a)(1)	Significant Problems, Abuses, and Deficiencies	6-11, 14-23
5(a)(2)	Recommendations for Corrective Action	14-17, 20
5(a)(3)	Prior Recommendations Not Yet Implemented	28-29
5(a)(4)	Matters Referred to Prosecutive Authorities	19-20, 30
5(a)(5)	Summary of Instances Where the Agency Unreasonably Refused or Failed to Provide Information to the OIG	25
5(a)(6)	List of OIG Audit and Evaluation Reports Issued During the Period	27
5(a)(7)	Summary of Significant Reports Issued During the Period	14-23
5(a)(8)	Statistical Table on Management Decisions with Respect to Questioned Costs	27
5(a)(9)	Statistical Table on Management Decisions on Recommendations That Funds Be Put to Better Use	27
5(a)(10)	Summary of Each Audit, Inspection or Evaluation Report Over Six Months Old for Which No Management Decision has been Made	25
5(a)(11)	Significant Revised Management Decisions	25
5(a)(12)	Significant Management Decisions with Which the Inspector General Disagreed	25
5(a)(14)(B)	Date of the Last Peer Review Conducted by Another OIG	32

APPENDIX A

PEER REVIEWS OF OIG OPERATIONS

PEER REVIEW OF THE SEC OIG'S AUDIT OPERATIONS

In accordance with GAGAS and CIGIE quality control and assurance standards, an OIG audit team assesses another OIG's audit functions approximately every 3 years. The most recent external peer review of the SEC OIG's audit operations was conducted in FY 2012.

The Legal Services Corporation (LSC) OIG conducted an assessment of the Office of Audit's system of quality control for the period ending March 31, 2012. The review focused on whether the SEC OIG established and complied with a system of quality control that was suitably designed to provide the SEC OIG with reasonable assurance of conforming with applicable professional standards.

On August 23, 2012, the LSC OIG issued its report, concluding that the SEC OIG complied with its system of quality control and that the system was suitably designed to provide the SEC OIG with reasonable assurance of performing and reporting in conformity with applicable government auditing standards in all material respects. Based on its review, the LSC OIG gave the SEC OIG a peer review rating of "pass." (Federal audit organizations can receive a rating of "pass," "pass with deficiencies," or "fail.") The LSC OIG did not make any recommendations. Further, there are no outstanding recommendations from previous peer reviews of the SEC OIG's audit organization.

The peer review report is available on the SEC OIG website at www.sec.gov/about/offices/oig/reports/reppubs/other/finalpeerreviewreport-sec.pdf.

The next external peer review of the Office of Audit's system of quality control is scheduled for Spring 2015.

PEER REVIEW OF THE SEC OIG'S INVESTIGATIVE OPERATIONS

During the semiannual reporting period, the Federal Housing Finance Agency (FHFA) OIG conducted an external peer review of the SEC OIG's investigative operations. The FHFA OIG's review was conducted in conformity with the Quality Standards for Investigations and the Quality Assessment Review Guidelines established by CIGIE and the Attorney General Guidelines for Offices of Inspectors General with Statutory Law Enforcement Authority.

The FHFA OIG issued its report on the SEC OIG's investigative operations in August 2014. In its report, the FHFA OIG noted that the SEC OIG was granted statutory law enforcement authority on June 10, 2014, and that the Attorney General Guidelines were not applicable prior to that time. The report stated that the SEC OIG has achieved significant progress in strengthening and developing its policies and procedures since receiving statutory law enforcement authority and that the FHFA OIG observed solid implementation of these improved policies and procedures throughout the SEC OIG's investigative operations. The FHFA OIG concluded that the SEC OIG is in compliance with the Attorney General Guidelines for the period during which they were applicable.

APPENDIX B

OIG SEC EMPLOYEE SUGGESTION PROGRAM ANNUAL REPORT

OVERVIEW

The OIG established the OIG SEC Employee Suggestion Program in September 2010, pursuant to Section 966 of the Dodd-Frank Act. Section 966 required the IG to establish a suggestion program for SEC employees. In accordance with the Dodd-Frank Act, the SEC OIG has prepared this fourth annual report containing a description of suggestions and allegations received, recommendations made or action taken by the OIG, and action taken by the SEC in response to suggestions or allegations from October 1, 2013 to September 30, 2014.

Through the SEC OIG Employee Suggestion Program, the OIG receives suggestions from agency employees concerning improvements in the SEC's work efficiency, effectiveness, and productivity, and

use of its resources. The OIG also receives allegations by employees of waste, abuse, misconduct, or mismanagement within the SEC through this program. To facilitate employees' participation in the program, the OIG created an electronic mailbox and telephone hotline for employees to submit their suggestions or allegations to the OIG. The OIG has established formal policies and procedures for the receipt and handling of employee suggestions and allegations under the program.

SUMMARY OF EMPLOYEE SUGGESTIONS AND ALLEGATIONS

Between October 1, 2013, and September 30, 2014, the OIG received and analyzed 22 suggestions or allegations, details of which are shown below:

Nature and Potential Benefits of Suggestion*	Number
Increase efficiency or productivity	8
Increase effectiveness	6
Increase the use of resources or decrease costs	6

Nature and Seriousness of Allegation*	Number
Mismanagement and/or discrimination	2
Waste of SEC resources	5
Misconduct by an employee	1

Action Taken by the OIG in Response to Suggestion or Allegation	Number
Memorandum to or communication with the SEC about the suggestion or allegation	14
Referred to OIG Office of Investigations	2
Referred to OIG Office of Audits	2
OIG Office of Investigations opened preliminary inquiry	0
Researched issue, but determined no further action was necessary	2
Other	2

Action Taken by SEC Management*	Number
SEC management took specific action to address the suggestion or allegation	2
The SEC decided to secure new technology in response to the suggestion	0
SEC management is considering the suggestion in context of existing procedures	2
SEC management initiated an internal review	2

*Some suggestions or allegations are included under multiple categories.

EXAMPLES OF SUGGESTIONS AND ALLEGATIONS

Print Font Requiring Less Space (ES-0214)

The OIG received a suggestion for potential cost savings from an SEC employee by altering the printing preferences within the SEC, which generates a substantial amount of paperwork with multiple hard copies of documents distributed throughout the organization, especially at SEC headquarters. According to a press article referenced by the employee, Federal agencies could substantially reduce their printing costs by using less ink intensive fonts such as Garamond. The employee suggested that the SEC could greatly reduce its printing expenses by asking all staff to change the font used to produce documents that are submitted to the Commissioners in hard copy.

The OIG forwarded this suggestion, along with a copy of a journal article supporting the suggested font change, to the SEC's Office of the Secretary (OS) to consider whether the suggestion could

be implemented. In response, OS stated that it is working with OIT to modernize its various technology systems to improve efficiency, reduce reliance on paper, and support a more electronic environment. OS also noted that the article we provided raised interesting points about print size and fonts and that the General Services Administration began a PrintWise program in 2012 that encourages the Federal government to print less and save resources. OS also noted that the SEC's Office of the Chief Operating Officer (OCOO) had already initiated many of the suggestions the PrintWise campaign advocates. The OCOO confirmed that the SEC continues to implement efficiencies in printing and publishing and that, in FY 2015, it will consider additional printing initiatives as resources permit.

Training System Automatic Notification and Calendar Reminders (ES 14-0274; ES 14-0574)

The OIG received a suggestion from an SEC employee that the SEC's online training system, known as LEAP (Lead, Learn and Perform), be set to automatically notify users by email when

they have pending training requirements. The OIG observed that LEAP had a functionality that, if activated, would notify SEC staff by email when a training deadline was approaching. However, the OIG found that the default for this function was set to “Off.”

Additionally, the OIG received a related suggestion about the lack of automatic calendar training reminders. According to the suggestion, when a user signed up for a meeting or training in LEAP, the user received an email confirmation along with an attached appointment for the user’s electronic calendar; however, the “Reminder” field appeared to be automatically toggled to “None.” As a result, a user would not receive a reminder of any training sessions for which he or she had signed up. Conversely, the default calendar notification when users created a meeting on their own was 15 minutes.

Given the numerous training requirements that SEC staff must continually comply with, the OIG believed that enabling the LEAP automatic notification function and changing the calendar notification default to 15 minutes would potentially aid staff in meeting their numerous training requirements. Therefore, the OIG referred both suggestions to the SEC’s OHR to consider whether they could be implemented. In response, OHR reviewed the LEAP system’s functionality and agreed to enable the automated notification feature so employees will receive system-generated emails to remind them of training requirements. OHR also agreed to discuss the feasibility of changing the calendar notification default to 15 minutes with the SEC’s OIT and the system vendor. However, OHR later notified the OIG that the change could not be implemented within the current LEAP environment.

Fees for Local Travel Expense Reimbursement (ES 14-0583)

An SEC employee questioned whether the SEC should be using its current travel system to process local travel expense reimbursements because of

the fees charged. The employee noted that, for one local trip, the service fees for processing the expense reimbursement were almost half the cost of the travel. The OIG also learned that fees for processing a local travel voucher had recently increased in August 2014. In addition, OFM staff informed the OIG that OFM previously explored using a paper reimbursement form for local travel but decided not to do so because the paper forms would still have to be processed for a fee.

The OIG forwarded the information provided by the employee to OFM to reassess whether any cost savings could be achieved by using another method to process local travel expense reimbursements. OFM responded that it examined the question and concluded that processing local travel expense reimbursement outside the SEC’s current travel system would not result in cost savings for the SEC. However, OFM stated that the current fee level was temporary until the SEC migrates to a new travel system. Also, OFM indicated it had issued guidance to travelers to process multiple vouchers at one time to reduce the fees incurred by the agency.

CONCLUSION

The OIG remains pleased with the effectiveness of the OIG SEC Employee Suggestion Program. We have received favorable responses from the agency on suggestions we have submitted for its consideration. Some of these suggestions have resulted, or may result, in positive changes that will improve the agency’s efficiency and effectiveness or conserve the agency’s resources. The OIG included information about the Employee Suggestion Program in the outreach presentations it conducted for SEC employees and looks forward to receiving additional suggestions as a result of those outreach efforts.

OIG CONTACT INFORMATION

Help ensure the integrity of SEC operations. Report to the OIG suspected fraud, waste, or abuse in SEC programs or operations as well as SEC staff or contractor misconduct. Contact the OIG by:

PHONE Hotline 877.442.0854
 Main Office 202.551.6061

WEB-BASED www.sec.gov/about/offices/oig/inspector_general_investigations_hotline.shtml
HOTLINE

FAX 202.772.9265

MAIL Office of Inspector General
 U.S. Securities and Exchange Commission
 100 F Street, NE, Washington, DC 20549-2977

EMAIL oig@sec.gov

Information received is held in confidence upon request. While the OIG encourages complainants to provide information on how they may be contacted for additional information, anonymous complaints are also accepted.



This report is available on the Inspector General's website
www.sec.gov/about/offices/inspector_general.shtml