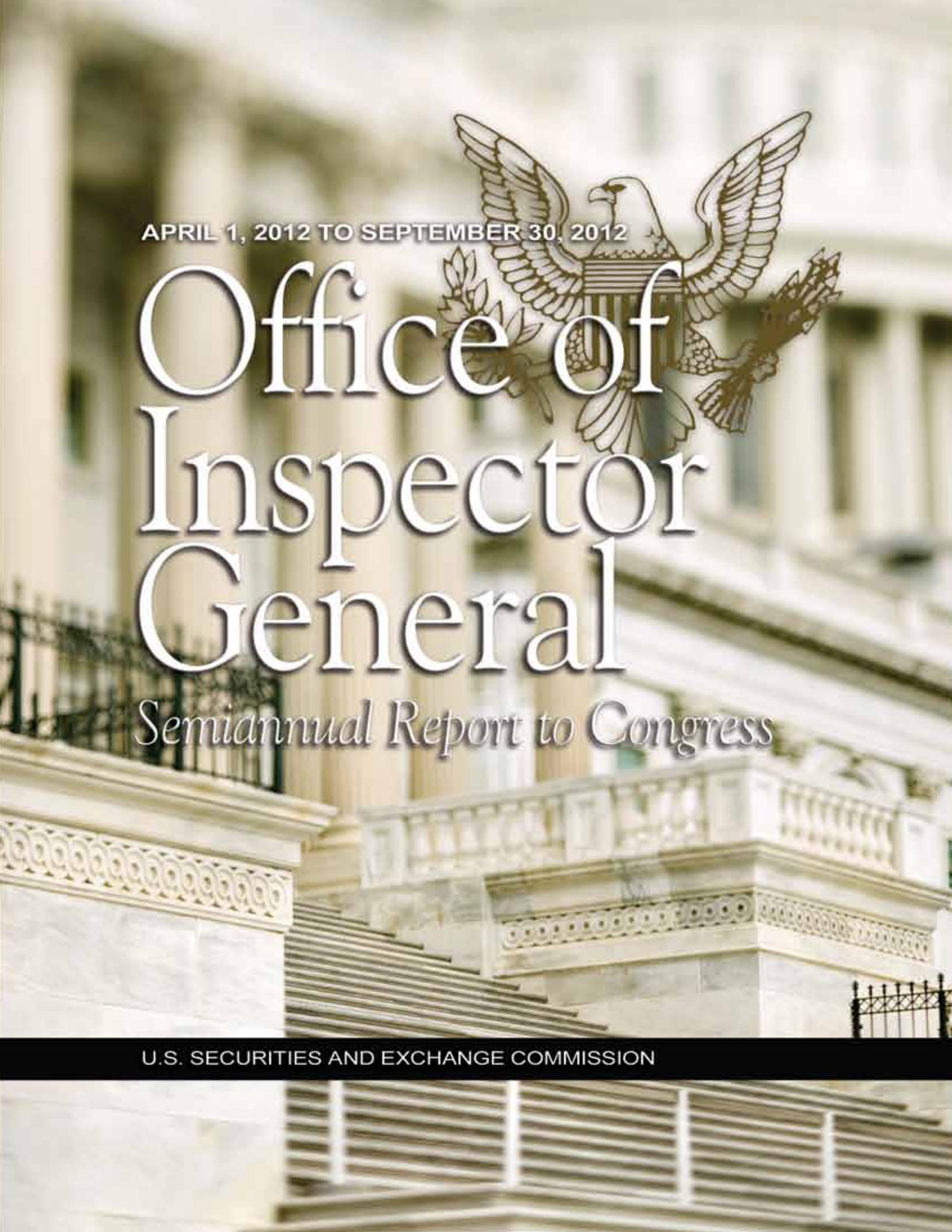

APRIL 1, 2012 TO SEPTEMBER 30, 2012

Office of Inspector General

Semiannual Report to Congress

U.S. SECURITIES AND EXCHANGE COMMISSION

OFFICE OF THE INSPECTOR GENERAL

Semiannual Report to Congress

APRIL 1, 2012–SEPTEMBER 30, 2012

The mission of the Office of Inspector General (OIG) is to promote the integrity, efficiency, and effectiveness of the critical programs and operations of the United States (U.S.) Securities and Exchange Commission (SEC or Commission). This mission is best achieved by having an effective, vigorous, and independent office of seasoned and talented professionals who perform the following functions:

- Conducting independent and objective audits, evaluations, 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 the Commission and Congress fully and currently informed of significant issues and developments.

CONTENTS

Message from the Interim Inspector General

I am pleased to present this Semiannual Report to Congress as Interim Inspector General of the U.S. Securities and Exchange Commission (SEC or Commission). This report describes the work of the SEC Office of Inspector General (OIG) for the period from April 1, 2012, to September 30, 2012. I am concurrently serving as the Inspector General of the Federal Deposit Insurance Corporation. On May 30, 2012, I was designated Interim Inspector General of the SEC until such time as the Commission hires a permanent Inspector General.

The audits, reviews, and investigations described in this report illustrate the commitment of the SEC OIG to promoting the efficiency and effectiveness of the SEC, as well as the impact the Office has had on SEC programs and operations.

At the time of my designation as Interim Inspector General, the SEC OIG faced a number of challenges, including those presented by a complaint alleging misconduct by current and former SEC OIG management. This complaint, which had been reported in the press, called into question the integrity of three reports issued by or to be issued by the SEC OIG. Almost immediately upon my designation as Interim Inspector General, I coordinated with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) to identify another OIG to independently investigate the allegations involving the SEC OIG.

At my request, in early June 2012, the United States Postal Service (USPS) OIG commenced a comprehensive and independent investigation into the allegations of misconduct by current and former SEC OIG management. In late September 2012, the USPS OIG completed its investigation and issued a report. I am now reviewing the evidence in the report to determine the disposition of the three reports issued, or to be issued, by the SEC OIG. I expect to complete my review by November 2012.

The SEC OIG still faces significant challenges, including those presented by depleted staffing levels. Several key staff members departed during the reporting period, including the Deputy Inspector General and a senior auditor. We will be working closely with the SEC's Office of Human Resources to fill these and other critical positions as quickly as possible.

Additionally, since my designation as the SEC Interim Inspector General, I have reviewed the Office's organizational structure and operational processes and have begun to implement certain changes and improvements. For example, under my direction, the Office of Audits has reorganized to add two supervisory auditor positions and plans to move towards a team approach to auditing. I have also undertaken measures designed to improve communications and coordination between the Office of Audits and Office of Investigations. For example, we arranged to have the CIGIE Training Institute conduct an audit overview training session for the SEC OIG's investigators. Additionally, I have sought to develop a more unified and coordinated approach to guide and foster the SEC OIG's relationship with Congress. To that end, I designated an OIG attorney to serve as the SEC OIG's primary legislative contact and be responsible for tracking legislative developments and coordinating the Office's responses to Congressional requests.

Notwithstanding the challenges faced by the SEC OIG during this semiannual reporting period, the SEC OIG staff has remained committed to achieving the Office's mission and promoting the efficiency and effectiveness of the SEC's programs and operations. During this reporting period, the Office of Audits issued reports on agency operations related to the SEC's continuity of operations program (COOP) and records management practices. These reports found that while the agency had taken steps to enhance both its COOP and records management programs, significant improvements were still needed in these areas. For example, our COOP report made a total of 38 recommendations designed to strengthen the SEC's COOP and ensure that the SEC can continue to perform its critical mission functions during an emergency, and SEC management concurred with all of these recommendations. Based upon our report, we have identified COOP as a management challenge facing the SEC.

The Office of Audits also issued a report on the SEC's Office of International Affairs (OIA) internal operations and travel oversight. This report found that OIA's operational units had effective policies, procedures, and controls, but that improvements were needed to strengthen OIA's oversight of international travel by SEC staff. Further, during the reporting period, the Office of Audits worked closely with SEC management to close 69 recommendations arising out of OIG reports.

The SEC OIG's Office of Investigations completed numerous investigations and inquiries during the reporting period and issued seven reports of investigation or inquiry. Specifically, we issued reports related to the misuse of resources and violations of information technology security policies within the Division of Trading and Markets, security violations by a Division of Enforcement contractor, and falsification and misuse of computer resources by a Headquarters employee. We also issued reports concerning the unauthorized disclosure of nonpublic information relating to an SEC enforcement matter and draft regulations being promulgated by the SEC and other federal financial regulatory agencies pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). Our investigative reports resulted in three referrals to the agency for consideration of appropriate administrative action based on the OIG's findings, two referrals to the OIG's Office of Audits for consideration of audit follow-up work, and several specific recommendations for improvement in agency policies and procedures.

Also during the past year, the SEC OIG has continued to operate the OIG SEC Employee Suggestion Program, which was initiated in September 2010 under the Dodd-Frank Act. This program continued to be active and effective during fiscal year 2012, as indicated in our annual report on this program, which is included at Appendix B. During the past

year, we received and reviewed a total of 53 suggestions and allegations, with several suggestions leading to tangible improvements in the SEC's programs and operations and, in some instances, cost savings.

In closing, we will continue to strive to improve the efficiency and effectiveness of the SEC OIG through organizational and procedural changes and by growing our staff resources. We will also continue to work collaboratively with SEC management to assist the agency in addressing the challenges it faces as identified in this report, which include procurement and contracting, information security, COOP, and financial management. This report truly reflects our dual responsibility to report independently to the Commission and Congress, and I reaffirm the SEC OIG's commitment to the Commission and Congress as we carry out the OIG mission.

I appreciate the significant support the Office has received from Congress, the SEC Chairman and Commissioners, and the SEC's management team and employees, as well as the inspector general community. I also wish to acknowledge the service and leadership provided by the former Deputy Inspector General. Finally, I would like to express my gratitude to all the SEC OIG staff, who have continued to demonstrate their dedication and commitment to the work and mission of the SEC OIG during this period of transition for the Office.

Jon T. Rymer
Interim 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. The SEC's 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 Commission's performance through effective alignment and management of human resources, information, and financial capital.

SEC staff monitor and regulate a securities industry comprising more than 35,000 registrants, including approximately 9,500 public companies, 11,800 investment advisers, about 4,200 mutual funds, and about 5,400 broker-dealers, as well as national securities exchanges and self-regulatory organizations, 450 transfer agents, 16 national securities exchanges, 8 clearing agencies, and 9 credit rating agencies. Additionally, the agency has oversight responsibility for the Public Company Accounting Oversight Board (PCAOB), the Financial Industry Regulatory Authority (FINRA), the Municipal Securities Rulemaking Board (MSRB), and the Securities Investor Protection Corporation (SIPC). While about 2,000 smaller investment advisers transitioned to state regulation under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), the SEC is gained responsibility for directly overseeing approximately 1,500 larger private fund advisers, including hedge funds.

In order to accomplish its mission most effectively and efficiently, the SEC is organized into 5 main divisions (Corporation Finance; Enforcement; Investment Management; Trading and Markets; and Risk, Strategy, and Financial Innovation) and 20 functional offices. The Commission's headquarters is in Washington, D.C., and there are 11 regional offices located throughout the country. As of September 30, 2012, the SEC employed 3,792 full-time equivalents (FTEs), consisting of 3,752 permanent and 40 temporary FTEs.

OIG STAFFING

On May 30, 2012, the Commission named an interim inspector general to serve while a search for a permanent inspector general is completed.

During the semiannual reporting period, the deputy inspector general, the writer-editor, an auditor, and a contract paralegal departed the OIG to pursue

other opportunities. The OIG bids farewell to these dedicated staff members.

Also during the reporting period, the OIG restructured its Office of Audits to create two new auditor-in-charge positions and add a new junior auditor position. The OIG plans to fill these important positions during the next reporting period. In addition, the OIG appointed a current OIG staff attorney as Congressional and Public Affairs Counsel.

Congressional Testimony, Requests, and Briefings

During this semiannual reporting period, the OIG continued to keep Congress fully and currently informed of the OIG's investigations, audits, and other activities through testimony, written reports, meetings, and telephonic communications.

On April 17, 2012, the former Inspector General testified before the TARP, Financial Services, and Bailouts of Public and Private Programs Subcommittee of the U.S. House of Representatives Committee on Oversight and Government Reform concerning the cost-benefit analyses performed by the SEC in connection with rulemakings under the Dodd-Frank Act. The primary focus of the former Inspector General's testimony was a report the OIG had issued during the previous semiannual reporting period concerning the OIG's "Follow-up Review of Cost-Benefit Analyses in Selected Dodd-Frank Act Rulemakings." This report, as well as an earlier OIG report on the topic, was prepared in response to a request from several members of the U.S. Senate Committee on Banking, Housing, and Urban Affairs. In his testimony, the former Inspector General summarized the findings and conclusions reached during the OIG's review. In addition, the former Inspector General described the six recommendations made in the report for improvements to the SEC's practices relating to cost-benefit analyses. Finally, the former Inspector General noted that the SEC had taken steps to implement the report's recommendations.

Subsequently, on July 24, 2012, the Interim Inspector General received a request from the Committee on Oversight and Government Reform for the OIG to perform additional work with respect to the cost-benefit analyses associated with certain SEC rulemakings. Specifically, the request noted that on March 16, 2012, the SEC had circulated a memorandum entitled, "Current Guidance on Economic Analysis in SEC Rulemakings" (Current Guidance), and that SEC Chairman Mary Schapiro had assured the Subcommittee on TARP, Financial Services, and Bailouts of Public and Private Programs that the Current Guidance would govern all agency rulemaking. The Committee on Oversight and Government Reform requested that the OIG evaluate the implementation of the Current Guidance in newly-proposed and final Commission rules, as well as the degree to which the principles and policies of the Current Guidance are incorporated into the economic analyses of rulemakings of the self-regulatory organizations (SRO) under the SEC's jurisdiction. The Committee also welcomed the OIG's recommendations for further improvements to the cost-benefit analyses associated with SEC and SRO rulemakings. On August 2, 2012, the Interim Inspector General responded to the Committee's request and stated that the OIG had commenced the

process to retain a contractor to conduct a review of the SEC's implementation of the Current Guidance and its incorporation into SRO rulemaking.

The OIG also responded to several other Congressional requests during the reporting period. For example, on July 11, 2012, the Interim Inspector General responded to a June 27, 2012, request from U.S. Senators Richard G. Lugar and Benjamin L. Cardin. The Senators had requested that the OIG evaluate the status of the SEC's implementation of the Cardin-Lugar Amendment, which was included as Section 1504 of the Dodd-Frank Act and required reporting of payments made to governments for the extraction of oil, natural gas, and minerals by companies that must file disclosures with the SEC. The Interim Inspector General informed the Senators that the OIG had confirmed that the Commission was scheduled to vote on a final rule implementing Section 1504 on August 22, 2012. Thereafter, the Commission adopted the rules mandated by Section 1504.

In addition, on July 20, 2012, the Interim Inspector General responded to a July 16, 2012, request from the Chairman of the Subcommittee on Energy and Environment of the U.S. House of Representatives Committee on Science, Space, and Technology that the OIG conduct an inquiry into the SEC's communications with the Department of Energy (DOE) regarding a DOE grantee. In his response, the Interim Inspector General apprised the Subcommittee Chairman of pertinent communications of which the OIG was aware.

The Interim Inspector General also responded on August 24, 2012, to an August 3, 2012, letter from the Chairman of the U.S. House of Representatives Committee on Oversight and Government Reform, which requested responses to three questions relating to the specific methods used by the SEC OIG to communicate with Congress. In response to the Chairman's questions, the Interim Inspector General stated that he was not aware of any "seven-day letters" issued by the SEC OIG under Section 5(d) of the Inspector General Act, which requires an Inspector General to report particularly serious or flagrant problems to Congress through the agency head. The Interim Inspector General further informed the Chairman that he was not aware of any serious or flagrant problems at the SEC that were not reported to Congress. The Interim Inspector General also emphasized the importance he places on maintaining an active dialogue with Congress and described in detail the various methods used by the SEC OIG to communicate with Congress in a timely, complete, and high-quality manner. Finally, the Interim Inspector General described measures he had undertaken since his May 30, 2012 appointment, to develop a unified and coordinated approach to guide and foster the SEC OIG's relationship with Congress.

In addition to providing responses to the requests discussed above, the Interim Inspector General briefed various Congressional committee and subcommittee staff. Shortly after his appointment, the Interim Inspector General met separately with staff of the U.S. Senate Committee on the Judiciary and the U.S. House of Representatives Committee on Oversight and Government Reform to discuss a number of issues relating to the SEC OIG and its oversight work.

The Inspector General'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 the SEC faces. To identify management challenges we routinely review past and ongoing audit, investigation, and evaluation work to identify material weaknesses, significant deficiencies, and vulnerabilities. This statement has been compiled based on the work we have completed over the past year, our general knowledge of the SEC's operations, and feedback we received from the agency and the Government Accountability Office's (GAO) financial statement auditors.

PROCUREMENT AND CONTRACTING

Since fiscal year 2008, OIG has identified the SEC's procurement and contracting function as a management challenge. While we are pleased at the continued progress and improvements the Office of Acquisitions (OA) has made in this area, overall, procurement and contracting continues to be a management challenge.

Specifically, work conducted by OIG's Office of Investigations during the fiscal year, revealed there were deficiencies in the SEC's administration of a personal services contract. On March 29, 2012, OIG issued a report of investigation into an allegation that the SEC had entered into an improper personal services contract. The investigation found evidence that an SEC contract may have been improperly administered because some contract personnel were subject to the continuous supervision and control of SEC employees.

According to the Federal Acquisition Regulation (FAR), a personal services contract is characterized by the employer-employee relationship that is created between the Government and the contractor's personnel. The Government is normally required to obtain its employees by direct hire under competitive appointment or other procedures that are required by the civil service laws. Obtaining personal services by contract, rather than by direct hire, circumvents these laws, absent specific Congressional authorization.[1]

OIG's investigation recommended the agency obtain an opinion from the Comptroller General on whether the SEC was employing unauthorized personal services. However, we subsequently advised SEC management that issuing a new regulation on personal services contracts would be a sufficient

[1] FAR § 37.104(a).

response to the investigation's findings and a Comptroller General's opinion would not be needed. While OA continues to make improvements in the procurement and contracting area, further progress is needed to ensure the SEC complies fully with the FAR provisions relating to personal services contracts.

INFORMATION SECURITY

Though the Office of Information Technology (OIT) made significant improvements during the fiscal year, information security continues to be a management challenge for the SEC. This was further confirmed in the vulnerabilities that were identified in the system and network logs in the OIG's *Assessment of SEC Systems and Network Logs*, Report No. 500, issued March 16, 2012, and based on new weaknesses covering information security controls that GAO identified in its fiscal year 2011 audit of the SEC's financial statements report.

In *Assessment of SEC Systems and Network Logs*, Report No. 500, the OIG determined OIT should identify capacity requirements for all servers, ensure sufficient capacity is available for the storage of audit records, configure auditing to reduce the likelihood that capacity will be exceeded, and implement a mechanism to alert and notify appropriate offices and divisions when log storage capacity is reached.

The report also found many SEC servers did not log auditable events because their logging capacity had been exceeded. Further, the report found that there was no mechanism available to alert OIT's Servers and Storage Branch or OIT's Security Branch when servers reached their capacity and stopped performing logging functions. Most notably, the report revealed that decommissioned servers were still actively connected to the SEC's Enterprise networks and were still accessible.

Compliance with the Federal Information Security Management Act (FISMA) continues to be a management challenge for the SEC due to repeat findings for the current and past fiscal years that have not been addressed. When taken as a whole, the combination of these deficiencies result in a management challenge that must be addressed to ensure the SEC's full compliance with all FISMA requirements and the SEC's information technology (IT) framework is secured.

Specifically, in the *2011 Annual FISMA Executive Summary Report*, Report No. 501, issued February 2, 2012, we concluded SEC risk management policy did not adhere to the requirements for a comprehensive governance structure and organization-wide risk management strategy, and OIT's risk management did not address risk from a mission and business perspective as described in National Institute of Standards and Technology (NIST) SP 800-37, Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.

Secondly, the SEC has not fully implemented baseline configurations and configuration compliance scanning within the information system environment. Baseline configurations have not been defined and configuration scanning is not conducted for networking devices. Without baseline or compliance scanning for networking devices, settings could be altered without the network administrator's knowledge. As a result, improperly configured devices could present an increased security risk to the SEC's systems.

In the *2011 Annual FISMA Executive Summary Report*, OIT concurred with the OIG's recommendation that the office complete its 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, but it still has not implemented a technical solution to link the multi-factor authentication solutions to SEC's PIV card. Thus, the SEC is not in compli-

ance with the requirements established in Homeland Security Presidential Directive 12, which opens the agency up to a higher risk for fraud, tampering, counterfeiting, etc.

Finally, the SEC's tailored set of baseline security controls are not explicitly defined in the System Security Plan or other security documents for each system. Though OIT identifies a generic set of baseline security controls, the selection process is based on the security categorization of the system and is not in accordance with NIST SP 800-37, Rev 1. Additionally, OIT has not developed formal procedures that provide instructions for tailoring baseline security controls in compliance with NIST SP 800-53, Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009. As a result of not implementing formal tailored control sets, a generic control set based only on security categorization could result in understating or overstating the security requirements for each system and critical controls may not be identified for systems if the tailoring process is not followed.

The areas discussed above remain challenges that were identified in the past and have not yet been completely mitigated. The OIG will continue its oversight of IT management and monitor progress in these areas.

GAO reported in its fiscal year 2011 audit of the SEC's financial statements that the SEC made progress in strengthening its internal controls over its financial information systems. However, despite this progress, they identified new weaknesses in information security controls regarding

- incomplete implementation of SEC's information security program, and
- inadequate review of service auditors' reports that jeopardized the confidentiality and integrity of SEC's financial information.

CONTINUITY OF OPERATIONS PROGRAM

Federal agencies are required to have a viable Continuity of Operations Program (COOP) in place to ensure the agency can continue to perform its critical mission functions during an emergency. An agency's COOP plan focuses on restoring the organization's mission essential functions at an alternate site and performing these functions for up to 30 days before returning to normal operations.

The OIG has identified SEC's COOP as a management challenge. In the *Review of the SEC's Continuity of Operations Program*, Report No. 502, issued on April 23, 2012, we identified areas needing improvement to ensure a comprehensive, cohesive, and up-to-date COOP that complies with federal guidance. Many of the report's recommendations involve OIT's interaction with program offices and divisions agency-wide, to include the SEC's regional offices. These improvements were broadly separated into two groups:

(1) procedural problems, and
(2) IT equipment-related problems.

With regard to procedural improvements, the report found that supplemental plans for divisions, offices, and regional offices are not being updated or properly maintained. In addition, many of the plans that are in place contain unrealistic estimates of required recovery time. Further, the report found that several regional offices' Disaster Recovery Plans (DRP) had not been tested annually, and two regional offices did not include recovery phase testing in their most recent disaster recovery test plans. Finally, we found that while some OIT personnel regularly participate in DRP exercises, many essential personnel do not participate in these exercises and have not received appropriate role-based training for their part in the DRP and COOP activities.

Regarding IT equipment issues, our review identified instances where information feeds and power

distribution throughout the SEC's network could fail if a disruption were to occur. In addition, equipment at the SEC's devolution sites is out-of-date and cannot be used with SEC's network, due to unresolved security issues. We also found that remote access capabilities would be enhanced if remote access to desktop applications could function when the user's desktop computer is turned off or does not have power.

Among the report's 38 recommendations were that DRPs are tested thoroughly each year, and the SEC should revise its system recovery time objectives to include specific and realistic timeframes. Further, the report recommended that the SEC should take procedural steps such as categorizing essential personnel and ensure alternate worksites are readily accessible.

FINANCIAL MANAGEMENT

The GAO's fiscal year 2011 audit of the SEC's financial statements[2] found that they were fairly presented in all material respects, in conformity with U.S. generally accepted accounting principles; and though internal controls could be improved, the SEC maintained in all material respects, effective internal controls over financial reporting. Though GAO found no reportable noncompliance with the laws and regulations they tested, they identified four significant deficiencies in SEC's internal controls. The significant deficiencies identified during fiscal year 2011 included deficiencies in controls over

- information systems,
- financial reporting and accounting processes,
- budgetary resources, and
- registrant deposits and filing fees.

During the current fiscal year the SEC transitioned its core financial system to the Department of Transportation's Enterprise Service Center, Federal Shared Service Provider (FSSP). Based on the four significant deficiencies GAO identified in SEC's internal controls and the inherent risks that are associated with transitioning the SEC's core financial system to a FSSP, financial management remains a management challenge.

GAO found that the SEC continued to carry out its financial reporting during fiscal year 2011 using spreadsheets, databases, and data processing practices that relied on significant manual analysis, reconciliation, and work-arounds that were used to assist in calculating amounts in the general ledger transaction postings. Such manual processes are resource intensive and prone to error and, coupled with the significant amount of data involved, there is an increased risk of materially misstated account balances in the general ledger.

GAO reported that consistent with prior audits they continued to find deficiencies in SEC's recording of new obligations and monitoring of open obligations. These deficiencies resulted in misstatements in SEC's accounting records which could affect the reliability of information that is reported in its Statement of Budgetary Resources.

GAO also noted that the SEC made improvements in verifying current filing fee transactions more timely. However, they found continuing deficiencies in the SEC's controls over registrant deposits and filing fees that collectively represented a significant deficiency for fiscal year 2011. Specifically, the SEC has not effectively addressed previously reported deficiencies in its process to enable timely recognition of filing fee revenue. Because of this continuing control deficiency, the SEC is not always recognizing filing fee revenue in the correct accounting period and, therefore, its registrant deposit liability could be misstated and not be corrected in a timely manner. Contributing to the SEC's deficiencies in this area is that it has yet to finalize and implement a formal process for ongoing monitoring of filing fee transactions.

[2] Includes SEC's general purpose and Investor Protection Fund (IPF) financial statements.

Advice and Assistance Provided to the Agency

During this semiannual reporting period, the OIG provided advice and assistance to SEC management on issues that were brought to the OIG's attention through various means. This advice and assistance was conveyed through written communications, as well as in meetings and conversations with agency officials. The advice and assistance provided included suggestions for improvement in agency programs and operations that were received through the OIG SEC Employee Suggestion Program, which was established pursuant to Section 966 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

Specifically, the OIG received a suggestion through the OIG SEC Employee Suggestion Program regarding subscription costs associated with hard copy sets of Commerce Clearing House (CCH) securities law books and corresponding regular hard copy updates. Staff from the SEC's Branch of Library Services informed the OIG that CCH is available online through CCH IntelliConnect at no additional cost to the agency, but that many employees still receive hard copy sets and the corresponding paper updates. According to the Branch of Library Services, the Commission currently spends over $300,000 per year for hard copy subscriptions. After reviewing and analyzing the suggestion received, the OIG learned that, while the Commission has taken certain initiatives to decrease the number of hard copy CCH purchases, additional steps could be taken to reduce the costs associated with hard copy CCHs. The OIG forwarded the suggestion to the Branch of Library Services and suggested that it consider providing additional information to SEC staff regarding the availability of this resource online. The OIG further suggested that the Branch of Library Services provide information regarding the price discrepancy between the hard copy and online CCH versions and offer training on the online resource to encourage more employees to utilize CCH IntelliConnect. It is expected that these measures will result in a reduction in the number of hard copy CCHs utilized and, therefore, cost savings for the SEC.

Another suggestion received through the OIG SEC Employee Suggestion Program related to employees' ability to book conference rooms online. The OIG was informed that in certain regional offices, conference rooms are booked manually and require assistance from support staff. The OIG spoke with staff from the SEC's OIT and learned that, while all SEC offices currently have the capability to book conference rooms electronically, online scheduling of conference rooms is only available upon specific request from the OIT service desk or local office information technology staff. At the time the OIG received the suggestion, the Philadelphia, New

York, Salt Lake, Chicago, and Denver Regional Offices did not appear to use online conference room scheduling. After reviewing and analyzing the suggestion received, the OIG forwarded it to OIT for consideration. The OIG suggested that OIT provide additional information regarding the online scheduling feature throughout the agency and also consider reminding employees of the benefits of online scheduling. Subsequently, the New York Regional Office began implementing the online scheduling function. It is expected that the remaining regional offices will also begin to use this feature, which will result in a more streamlined, efficient approach to scheduling conference rooms, thereby improving employee efficiency.

Also during the reporting period, the Office of Audits provided the agency with written comments it should consider before finalizing draft SEC Operating Procedure 10-24, *Management and Administration of Service Contracts*. In addition, the Office of Audits provided the agency with minor comments and edits it should consider before finalizing revised SEC Regulation 30-2, *Audit Follow-up and Resolution*.

Finally, the Counsel to the Inspector General worked closely with the SEC's Office of Equal Employment Opportunity (EEO) to develop and offer training to all SEC staff pursuant to the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act). This Act mandates that federal agencies provide training to its employees at least every two years regarding their rights, remedies, and responsibilities under antidiscrimination EEO laws and the whistleblower protection laws. The Counsel to the Inspector General provided assistance to the EEO Office in developing the portion of online No FEAR Act training related to the Whistleblower Protection Act, and this online training was made available to SEC employees beginning in July 2012. In addition, the Counsel to the Inspector General provided instruction concerning the antiretaliation provisions of the Whistleblower Protection Act and the Inspector General Act during two live training sessions offered to SEC employees in September 2012.

Coordination with Other Offices of Inspector General

During this semiannual reporting period, the SEC OIG coordinated its activities with those of other OIGs, as required by Section 4(a)(4) of the Inspector General Act of 1978, as amended. Specifically, the SEC Interim Inspector General attended meetings of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and serves as the Chairman of the CIGIE Audit Committee. The Counsel to the Inspector General participated in the activities of the Council of Counsels to the Inspectors General, an informal organization of OIG attorneys throughout the federal government who meet monthly and coordinate and share information. The SEC OIG also responded to requests for information from CIGIE during the reporting period that related to cyber and information technology security related reviews and subpoena disclosures. Further, the SEC OIG forwarded matters discovered during two separate Office investigations to other OIGs for potential investigation.

In addition, the SEC Acting and Interim Inspectors General participated in the meetings and activities of the Council of Inspectors General on Financial Oversight (CIGFO), which was created by Section 989E of the Dodd-Frank Act. The CIGFO is chaired by the Inspector General of the Department of Treasury and is also comprised of the Inspectors General 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 the SEC and the Special Inspector General for the Troubled Asset Relief Program. Under the Dodd-Frank Act, the CIGFO is required to meet at least quarterly to facilitate the sharing of information with a focus on the concerns that may apply to the broader financial sector and ways to improve financial oversight. The CIGFO is also required to submit an annual report to the Financial Stability Oversight Council and the Congress, which must include a section that highlights the concerns and recommendations of each CIGFO inspector general and a summary of the general CIGFO observations. The CIGFO's 2012 Annual Report was issued in July 2012 and included a section discussing the SEC OIG's mission, recent oversight work, and other planned oversight work. The CIGFO 2012 Annual Report is available at http://www.treasury.gov/about/organizational-structure/ig/Documents/CIGFO%20Document/508_CIGFO%20Annual%20Report.pdf.

In addition to working on the CIGFO Annual Report, the SEC OIG participated in a CIGFO working group that was established in December 2011. The working group included staff from seven CIGFO members' offices. The working group conducted a joint audit of the Financial Stability Oversight Council's (FSOC) controls and protocols to determine whether nonpublic information, deliberations, and decisions are properly safeguarded from unauthorized disclosure. FSOC, which was created by Section 111 of the Dodd-Frank Act, is charged with identifying threats to the financial stability of the United States, promoting market discipline, and responding to emerging risks that could impact the stability of the nation's financial system. FSOC consists of 10 voting members and 5 nonvoting members and brings together the expertise of federal financial regulators, state regulators, and an insurance expert appointed by the President with Senate confirmation. The Chairman of the SEC is among the voting FSOC members.

As part of the working group, the SEC OIG conducted an audit of the SEC's management and internal controls over sensitive and proprietary (nonpublic) information that was collected and exchanged with FSOC. The findings from each respective OIG were consolidated into the joint report entitled, *Audit of the Financial Stability Oversight Council's Controls over Non-public Information*, which was issued on June 22, 2012 to the FSOC Chairman. The report is available at http://www.treasury.gov/about/organizational-structure/ig/Documents/CIGFO%20Document/Audit%20of%20the%20Financial%20Stability%20Oversight%20Council's%20Controls%20over%20Non-public%20Information.pdf.

While the report did not make any recommendations, it identified differences in how FSOC and its member agencies mark nonpublic information. In addition, the report identified control differences in how the various agencies handle nonpublic information with respect to oral communication, supplemental prohibition on financial interest, contractor confidentiality and nondisclosure, encryption, and protocol for tracking information exchange.

Audits and Evaluations

OVERVIEW

The OIG is required by the Inspector General Act of 1978, as amended, to conduct audits and evaluations of agency programs, operations, and activities. The Office of Audits focuses its efforts on conducting independent audits and evaluations of the SEC's programs, operations and functions. The Office of Audits also hires independent contractors and subject matter experts to conduct work on its behalf. Specifically, the Office of Audits conducts audits and evaluations to determine whether

- there is compliance with governing laws, regulations, and policies;
- resources are safeguarded and appropriately managed;
- funds are expended properly;
- desired program results are achieved; and
- information provided by the agency to the public and others is reliable.

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

Audits

Audits examine operations and financial transactions to ensure proper management practices are being followed and resources are adequately protected in accordance with governing laws and regulations. Audits are systematic, independent, and documented processes for obtaining evidence. In general, audits are conducted when firm criteria or data exist, sample data is measurable, and testing internal controls is a major objective. Auditors collect, analyze, and verify data by gathering documentation, conducting interviews, and through physical inspections. The Office of Audits conducts audits in accordance with the generally accepted government auditing standards, as set forth in the *Government Auditing Standards*, issued by the Comptroller General of the United States, OIG policy, and guidance issued by the CIGIE.

Evaluations

The Office of Audits conducts evaluations of SEC programs and activities. Evaluations consist of projects that often cover broad areas and are typically designed to produce timely and useful information associated with current or anticipated problems.

Evaluations are generally conducted when a project's objectives are based on specialty or highly technical areas, criteria or data is not firm, or the

information must be reported in a short period of time. Evaluations are conducted in accordance with OIG policy and governing CIGIE guidance.

Audit Follow-Up and Resolution

During this semiannual reporting period, SEC divisions and offices provided the OIG with documentation to support their implementation of recommendations that were identified in reports we issued to management. Specifically, the OIG closed 68 recommendations related to 14 Office of Audits reports during this semiannual reporting period.

AUDITS AND EVALUATIONS CONDUCTED

Review of the SEC's Continuity of Operations Program (Report No. 502)

BACKGROUND

A continuity of operations program (COOP), including a business continuity plan (BCP) and disaster recovery plan (DRP), is essential to an organization maintaining its critical operations when unforeseen disruptions or interruptions occur that may affect the organization's normal operations. All federal agencies are required to have viable programs and plans in place to ensure they are able to continue to perform critical functions during an emergency. An agency's COOP plan focuses on restoring the organization's mission-essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations.

In November 2011, the SEC OIG contracted the professional services of TWM Associates, Inc. (TWM) to conduct a review of the SEC's COOP. TWM's primary objectives were to determine if the SEC (1) had a viable COOP, BCP, and DRP that sufficiently supported its operations at its headquarters, operations center, and 11 regional offices; and (2) was adequately prepared to perform essential functions during business continuity or disaster recovery events resulting from human/natural disasters, national emergencies, or technological events which could impact the Commission's ability to continue mission-critical and essential functions. The sub-objectives for the review were to:

- evaluate the SEC's pandemic plan to ensure it was formal, documented, well-communicated, had been tested at regular intervals, and met the objectives of the National Strategy for Pandemic Influenza: Implementation;
- assess the Commission's implementation and testing of its pandemic plan;
- determine the Commission's plans for protecting its employees and contractors during a pandemic occurrence; and
- evaluate the Commission's plans for sustaining essential functions during high rates of employee absenteeism.

RESULTS

As detailed in the report, TWM found that while the SEC did have a COOP function and plan (including relocation sites and testing) in place, the program needed to be improved. In particular, the SEC's COOP policies, procedures, and documents were: (1) outdated or incomplete, (2) not comprehensive, and (3) not being followed in some respects.

TWM also found SEC recovery time objectives were inconsistent with the Federal Information Security Management Act's (FISMA) system categorization for availability and system functionality. The review also identified deficiencies with the DRPs for individual systems, and found that the SEC did not prepare BCPs or Information System Contingency Plans for its information systems. Additionally, the review identified instances in which information feeds and power distribution could fail if a disruption were to occur. Further, TWM found that current data restoration processes were insufficient and improvements were needed in the processes for recovering data.

TWM also found that remote access capabilities needed to be enhanced to allow remote access to desktop applications. The review found that several DRPs had not been tested annually, regional offices have not tested their alternate site restoration capability, and the pandemic plan has not been tested since 2007. In addition, the review found that alternate work locations for eight regional offices have not been specified in COOP supplements or DRPs and the alternate work locations may not be available during an event.

TWM further found the SEC's plans of action and milestones did not include certain issues found or recommendations for improvement made during COOP or DRP testing. The review also found that while the SEC conducts COOP and disaster recovery exercises, the testing included a high concentration of personnel at headquarters and many essential personnel were not included. Lastly, the review identified that the SEC did not have current memoranda of agreement, memoranda of understanding, or service level agreements for alternate worksites. TWM found these documents were either outdated or not included in the Commission's COOP or DRP.

RECOMMENDATIONS

The OIG issued its report on April 23, 2012, and made 38 recommendations that were designed to strengthen the SEC's COOP.

The OIG recommended, among other things, the Office of Freedom of Information Act, Records Management, and Security (OFRMS) and OIT, in conjunction with SEC divisions and offices, update, revise, and finalize all COOP documents, including COOP plans and supplements, DRPs, BCPs, business impact analyses, and pandemic plans and supplements. The OIG further recommended OFRMS and OIT ensure these documents are complete, include necessary elements, and properly define the SEC's essential functions.

In addition, the OIG recommended OIT determine which aspects of DRP and BCP testing should be conducted annually and ensure this testing includes the recovery phase and reconstitution phase. The OIG also recommended OFRMS revise the SEC's system recovery time objectives to specify more realistic timeframes. Further, the OIG recommended the SEC take appropriate procedural steps to categorize essential personnel according to necessary functions and ensure alternate worksites are readily accessible.

OFRMS and OIT concurred with all recommendations in the report that were addressed to their respective offices. The offices provided OIG with corrective action plans that were fully responsive to each recommendation. However, recommendations remain open until documentation is provided that demonstrates the recommendations were implemented. The report is available on the OIG's website at http://www.sec-oig.gov/Reports/AuditsInspections/2012/502.pdf.

SEC's Records Management Practices (Report No. 505)

BACKGROUND

The Office of Records Management Services (ORMS) is responsible for coordinating, overseeing, and implementing the SEC's records management program at its headquarters, operations center, and 11 regional office locations. ORMS and the Office of Security Services (OSS) are direct reporting units to the Office of Support Operations (OSO). OSS has oversight of SEC's vital records program, while ORMS oversees the SEC's overall records management program through points-of-contact (POC) in most divisions and offices. The POCs provide oversight of their individual records management program and practices. ORMS' responsibilities include providing reference services for Commission staff, other federal, state, and local entities and members of the public that are essential

for the SEC to achieve its mission. Additionally, ORMS coordinates with the SEC's Office of Investor Education and Advocacy and Public Reference Room concerning records reference requests from the public. Further, ORMS assists the Office of Freedom of Information Act (FOIA) Services, in responding to requests for nonpublic records under FOIA.

The objectives of our audit were to examine whether ORMS:

- established a viable records management program that ensures permanent SEC records are appropriately maintained and preserved in accordance with applicable federal statutes and regulations; and
- adhered to applicable federal statutes and regulations regarding the retention, disposal, transfer, and recovery of SEC records.

RESULTS

The audit found that the SEC did not have an active staff assistance program and ORMS or its predecessors did not conduct periodic agency-wide staff assistance visits. Although ORMS provided assistance to offices and divisions to identify their records and had scheduled records for disposition, it had not conducted staff assistance visits of all 36 SEC divisions and offices. Therefore, confusion existed among POCs regarding their records management responsibilities.

In addition, the audit revealed that although ORMS readily answered agency staff questions about records matters, provided basic records management training during the SEC's new employee orientation, and provided training to staff in the regional offices, ORMS did not provide records management training to staff agency-wide. The OIG determined that this has caused confusion among employees.

Our review of a sample number of records requests found that some ORMS staff did not follow the office's standard operating policy in processing requests and several requests were not completed within ORMS' seven business days goal for non-urgent records requests.

The audit also identified offices that did not have records retention schedules and other offices whose records retention schedules were outdated. Additionally, we found ORMS had not met with all SEC offices to determine if they had records.

The OIG determined that many divisions and offices did not have proper records management procedures to ensure that active records are properly and economically maintained and used on a regular basis. Further, the audit found that inactive records were not regularly disposed.

Several POCs informed the OIG they did not know when their records should be disposed of and did not do so annually. Additionally, the OIG found ORMS had not reviewed the contents of 256 boxes that its contractor identified in a November 2010 report that was issued to ORMS. These boxes contained records that must be reviewed and scheduled for disposition. ORMS informed the OIG that, as of September 2012, it had reviewed 98 of the 256 boxes and coordinated with the Federal Records Center (FRC) to review the remaining boxes.

The audit also found that ORMS had not performed a timely review of SEC records that were eligible for destruction. As a result, there was an approximate 10-year backlog of records that were eligible for destruction but had not been destroyed. Although ORMS maintains hard copies of disposal forms the FRC provided for records review, approval, and destruction, the office did not maintain a list of Commission records the FRC identified as eligible for destruction.

Further, we determined that some offices and divisions did not have records management POCs. We also found that SEC's records management directives did not require offices or divisions to have records management POCs. As a result, some SEC employees did not understand their records management responsibilities. Also, the federal regulations and SEC policies covering records management were not being followed properly.

At the time of our audit, OSS had oversight of SEC's vital records program and was working with ORMS to evaluate the program, but had not defined the SEC's vital records and did not review or update the Commission's vital records at least annually. As a result, the SEC's listing of vital records was incomplete and outdated. Further, the SEC had not definitively established how it will protect and retrieve vital records in an emergency. Due to changes in responsibilities for vital records management, confusion existed regarding the SEC's compliance with the National Archives and Records Administration's (NARA) guidance on vital records. Thus, the SEC did not comply with certain vital records management regulations.

Lastly, our audit found the SEC's records management administrative regulations and vital records handbook were outdated. The administrative regulations contained terminology, processes, and forms that were no longer current, and the vital records handbook included a form the SEC never used.

RECOMMENDATIONS

On September 30, 2012, the OIG issued a final report containing 12 recommendations that were designed to ensure the SEC's records are properly managed and to strengthen the SEC's records management program.

Specifically, the OIG recommended ORMS periodically conduct agency-wide staff assistance visits of the SEC's records management programs in accordance with SECR 7-1, *Securities and Exchange Commission's Records Management Program*. In addition, OIG recommended ORMS develop a records management training program and offer training sessions on records management to all SEC employees. We also recommended ORMS develop robust internal controls that provide oversight of its records requests processes. Further, we recommended that ORMS work with offices and divisions agency-wide to ensure they have current management procedures that enable them to properly manage their records in accordance with applicable federal regulations and the SEC's administrative regulations.

Additionally, the OIG recommended ORMS develop a definitive action and milestones plan to review the records backlog maintained at the FRC and determine how the records will be treated. We also recommended ORMS develop an action plan to address the 10-year backlog of records the FRC has identified as being eligible for destruction.

Further, the OIG recommended ORMS require all divisions and offices to designate a POC for records management matters, and periodically verify the POC listing. We also recommended OSS, in coordination with ORMS, develop a vital records program that includes processes and procedures, and establish and maintain the SEC's vital records in accordance with applicable federal regulations and NARA's guidance on vital records management.

We also recommended ORMS update its administrative regulations covering records management and train SEC employees on the new regulations. Lastly, we recommended OSS and ORMS coordinate review of the SEC's Vital Records Handbook and determine if it will be revised or rescinded.

Management concurred with all of the report's recommendations. Each recommendation will remain open until documentation is provided to OIG that demonstrates the recommendations were implemented. This report is available on OIG's website at: http://www.sec-oig.gov/Reports/AuditsInspections/2012/505a.pdf.

The Office of International Affairs Internal Operations and Travel Oversight (Report No. 508)

BACKGROUND

The mission of the Office of International Affairs (OIA) is to promote investor protection and cross-border securities transactions by: (1) advancing international regulatory and enforcement cooperation, (2) promoting the adoption of high regulatory standards worldwide, and (3) formulating technical assistance programs to strengthen the regulatory infrastructure in global securities markets.

OIA also serves as the focal point for the SEC staff's official international travel. OIA reviews staff's proposed foreign travel, as presented in the SEC's Foreign Travel Memorandum (FTM) and supporting documents, which travelers provide to OIA. OIA then submits these documents to the Office of the Chief Operating Officer (OCOO) for final review and approval. Further, OIA coordinates SEC staff's needed country clearances with the U.S. Department of State and foreign governments, and determines if there are any visa requirements. In addition, OIA provides input to the "International Travel" section of the SEC's intranet, which provides foreign travel guidance to SEC staff.

The overall objective of the OIG's audit was to assess the effectiveness and efficiency of OIA's internal operations and identify areas for improvement to reduce or eliminate fraud, waste, and abuse. The specific audit objectives were to assess whether OIA:

- had viable policies, procedures, and controls for its program activities;
- effectively tracked and processed requests for technical assistance and enforcement assistance in a timely manner;
- had developed a program that ensures SEC employees' international travel is appropriately processed through OIA;
- adequately communicated the SEC's international travel process and related procedures to employees; and
- appropriately conducted and reported its staff's international travel in accordance with applicable federal regulations and internal policies and procedures.

RESULTS

The OIG found OIA's operating units had viable policies, procedures, and controls, and OIA effectively tracked and processed technical and enforcement assistance requests. However, OIA had not documented its international travel coordination and review procedures. In addition, our testing of FTMs, the primary review document for international travel, found that:

- FTMs were not always submitted to OIA two weeks prior to the start of travel, as is required by SEC policy;
- Some FTMs did not have one or more required supporting documents; and
- Some FTMs were approved by the former Executive Director on or after the traveler's departure date, and the former Executive Director did not approve a few FTMs.

The audit also found that while OIA obtained country clearances for SEC international travelers, it maintained the documents in its file and did not provide them to the travelers.

Further, our review of supporting documentation for three separate international trips taken by SEC in 2009 and 2010, did not sufficiently document the benefits to be derived from these trips. However, OIA management provided the OIG with additional documentation to justify the benefits of these trips.

Our review of a sample number of international expense reports found compliance with federal travel regulations and SEC travel policies needed improvement. Specifically, we determined that 61 percent of expense reports in our sample were not submitted by travelers within five working days after the trips' completion, as required. The audit also found compliance issues related to business class travel, taxis, airport parking, hotel per diem, meals and incidental expenses, and the recording of compensatory time for travel. Finally, we determined the "International Travel" section on the SEC's intranet had outdated information that needed updating.

RECOMMENDATIONS

Based on the results of the audit, the OIG issued the final report on September 30, 2012. The report contained 10 recommendations that were developed to strengthen OIA's internal operations and to assist OIA and the OCOO in effectively executing their international travel-related responsibilities.

Specifically, the OIG recommended OIA develop and implement written procedures for its travel coordination and review activities. In addition, we recommended OIA strengthen its travel administrative activities. In this regard, OIA and OCOO should periodically inform SEC staff of the requirement to prepare FTMs at least two weeks before the travel date and to provide supporting documents with the FTM to OIA. Further, we recommended the FTM be revised to include a justification for approved travel and copies of approved country clearances be provided to international travelers.

Additionally, we recommended OIA establish procedures and provide training to its staff on the proper application of federal travel regulations and SEC travel policies related to planning international trips, preparing expense reports, and computing and recording compensatory time for travel. We also recommended OIA ensure its timekeeper records compensatory time for travel in the pay period the hours are earned.

Finally, we recommended OIA and OCOO review guidance on the SEC intranet related to international travel processes and procedures and regularly update this information.

OIA and OCOO concurred with the recommendations addressed to their respective offices. Each recommendation will remain open until OIG is provided documentation that supports the recommendations were implemented. The report is available on the OIG's website at http://www.sec-oig.gov/Reports/AuditsInspections/2012/508.pdf.

PENDING AUDITS AND EVALUATIONS

SEC's Whistleblower Program

During this reporting period, the OIG began a statutorily mandated study to evaluate the SEC's whistleblower program, which was established pursuant to the Dodd-Frank Act. The audit will determine (1) if the final rules implementing the SEC's whistleblower program clearly defined the program and make it user friendly; (2) if the program is promoted on the SEC's website and has been widely publicized; (3) whether the Commission is prompt in responding to whistleblowers and other interested parties; (4) whether reward levels are adequate to entice whistleblowers to provide information or too high thereby encouraging illegitimate whistleblower claims; and (5) how current policies, procedures, and provisions of the Dodd-

Frank Act impact the effectiveness of the SEC's whistleblower program.

Fieldwork is currently ongoing, and we expect to issue a final report in January 2013.

Support, Expert, and Consulting Services Contracts at the SEC

We contracted with an independent public accountant to conduct an audit of the SEC's contract for support, expert, and consulting services. The primary objective of the audit is to determine whether the Office of Acquisitions (OA) awarded contracts for services that were inherently governmental or has contracts that are being administered as personal services contracts, in violation of the Federal Acquisition Regulation. Further, the audit will determine if OA has (1) internal controls and policy to prevent contractors from performing inherently governmental functions, (2) policy that prohibits services contracts from being administered as personal services contracts; (3) monitoring guidance to ensure the contract terms are carried out in compliance with governing federal laws, regulations, and SEC internal policy; and (4) internal controls to ensure the SEC is properly charged for services rendered under the terms of the contracts. Where appropriate, the audit will identify best practices and possible cost savings.

The contractor will complete the audit and issue a final report during the next semiannual reporting period.

Evaluation of the SEC's Systems Certification and Accreditation Process

The OIG hired a contractor to perform an independent review of the OIT's certification and accreditation (C&A) process. The evaluation's objectives are to determine (1) if the SEC's systems are appropriately certified and accredited in accordance with governing guidelines and industry best practices; (2) if the C&A process for critical applications is effective in identifying and mitigating risks in a timely manner; and (3) the adequacy of OIT's internal controls and compliance with internal information security policies and procedures and industry best practices, standards, and guidelines.

In addition, the evaluation will determine whether OIT's C&A process is consistent with the National Institute of Standards and Technology's (NIST) six-step risk management framework guidance, *Guide for Applying the Risk Management Framework to Federal Information Systems (NIST 800-37*, Rev 1). Where appropriate, the evaluation will identify areas that can be strengthened and best practices.

The contractor will complete its work and issue a final report during the next semiannual reporting period.

Hiring Practices for Senior Level Positions at the SEC

The OIG has continued to receive complaints and allegations regarding the SEC's failure to follow established policies and procedures in connection with hiring or promoting staff to senior-level positions. As a result, the OIG is conducting an audit of the SEC's civil service hiring practices. During the reporting period, we extended the scope of the audit and revised the objectives to better assess systemic issues related to the SEC's hiring and promotion practices for senior level staff positions.

The objectives of the audit are to examine whether OHR (1) adheres to applicable federal statutes and regulations and has adequate policies and procedures covering senior level vacancies in the competi-

tive service, excepted service, and for senior officers; (2) ensures the SEC's hiring and promotion practices are carried out in a fair and consistent manner and in accordance with applicable federal statutes, regulations and OHR policy requirements; (3) communicates its hiring authority, decisions, and changes to the appropriate personnel; (4) ensures hiring and promotion decisions are documented in accordance with applicable federal statutes and regulations; and (5) takes action in accordance with applicable federal statutes and regulations and OHR policy pertaining to improper hirings or promotions.

The audit's fieldwork is nearing completion and several tentative findings have been drafted. We expect to issue a final audit report by the end of next semiannual reporting period.

Filing Fee Refund Requests

The OIG commenced an audit of the Office of Financial Management's (OFM) filing fee refund request procedures during this reporting period. We contracted an independent public accounting firm to conduct this audit. The objectives of the audit are to assess (1) the adequacy of OFM's written policies and standard operating procedures covering its oversight of the filing fee program; (2) whether program staff are adequately trained and have the requisite skills needed carry out their duties; (3) if the system being used to track filing fee refund requests is appropriate; and (4) whether backlogs and dormant accounts are properly administered and managed.

Where possible, the contractor will also identify best practices and determine whether there are cost saving opportunities. The contractor will complete the audit and issue a final report during the next reporting period.

The SEC's Controls Over Sensitive and Proprietary Information Collected and Exchanged With the Financial Stability Oversight Council

During the reporting period, as part of the CIGFO working group, the Office of Audits worked on a joint audit with other CIGFO members' staff to examine the respective agencies' management and internal controls over sensitive and proprietary (nonpublic) information that was collected and exchanged with the FSOC. CIGFO was established to (1) facilitate information sharing among inspectors general, (2) provide a forum for discussing work as it relates to the broader financial sector, and (3) evaluate the FSOC's effectiveness and internal operations. A joint report entitled, *Audit of the Financial Stability Oversight Council's Controls over Non-public Information*, was issued to the FSOC Chairman on June 22, 2012. The report did not make any recommendations.

As a follow-up to the joint audit, OIG conducted an audit of the SEC's controls for handling and safeguarding nonpublic information from unauthorized disclosure. The audit's objective was to examine the controls and protocols employed by the SEC to ensure that the nonpublic information, including deliberations, and decisions, of the FSOC, the Department of Treasury's Office of Financial Research, and the FSOC member agencies is properly safeguarded from unauthorized disclosure.

During the semiannual reporting period, fieldwork was completed and a report was drafted. The final audit report will be issued in the next semiannual reporting period.

Fiscal Year 2012 Federal Information Security Management Act (FISMA) Assessment

The OIG hired a contractor with IT expertise to perform an independent review of the SEC's IT security programs and practices. The contractor will determine the extent to which the SEC's OIT meets the Department of Homeland Security (DHS) and NIST requirements covering configuration management, contingency planning, continuous monitoring management, contractor systems, identity and access management, incident response and reporting, plan of action and milestones, remote access management, risk management, security capital planning, and security training.

Additionally, the contractor will evaluate OIT's: data and boundary protections; continuous monitoring asset, configurations, and vulnerability management; enterprise security architecture; incident management; network security protocols; and system inventory and quality of the inventory.

The contractor will further provide responses to DHS's fiscal year 2012 questions related to the SEC's information security program. The contractor will also issue a final FISMA report prior to the completion of the next semiannual reporting period.

Investigations

OVERVIEW

The OIG's Office of Investigations responds to allegations of violations of statutes, rules, and regulations and other misconduct by SEC staff and contractors. The misconduct investigated ranges from criminal wrongdoing and fraud to violations of SEC rules and policies and the Standards of Ethical Conduct for Employees of the Executive Branch.

The Office of Investigations conducts thorough and independent investigations into allegations received in accordance with CIGIE Quality Standards for Investigations and the OIG Investigations Manual. The Investigations Manual contains the procedures by which the OIG conducts its investigations and preliminary inquiries and implements CIGIE Quality Standards. The Investigations Manual sets forth specific guidance on, among other things, OIG investigative authorities and policies, investigator qualifications, independence requirements, procedures for conducting investigations and preliminary inquiries, coordination with the U.S. Department of Justice (DOJ), and issuing reports of investigation.

The OIG receives complaints through the OIG Complaint Hotline, an office electronic mailbox, mail, facsimile, and telephone. The OIG Complaint Hotline consists of both telephone and web-based complaint mechanisms. Complaints may be made anonymously by calling the Hotline, which is staffed and answered 24 hours a day, 7 days a week. Complaints may also be made to the Hotline through an online complaint form, which is accessible through the OIG's website. In addition to being a mechanism for receiving complaints, the OIG's website provides the public with an overview of the work of the Office of Investigations, as well as links to some investigative memoranda and reports issued by the Office of Investigations. The OIG also receives allegations from SEC employees of waste, abuse, misconduct, or mismanagement within the Commission through the OIG SEC Employee Suggestion Program, which was established pursuant to Section 966 of the Dodd-Frank Act.

The OIG reviews and analyzes all complaints received to determine the appropriate course of action. In instances where it is determined that something less than a full investigation is appropriate, the OIG may conduct a preliminary inquiry into the allegation. If the information obtained during the inquiry indicates that a full investigation is warranted, the Office of Investigations will commence an investigation of the allegation. When an investigation is opened, the primary OIG investigator assigned to the case prepares a comprehensive plan of investigation that describes the focus and

scope of the investigation, as well as the specific investigative steps to be performed during the investigation. The OIG investigator interviews the complainant whenever feasible, and the OIG investigator may give assurances of confidentiality to potential witnesses who have expressed a reluctance to come forward.

Where allegations of criminal conduct are involved, the Office of Investigations notifies and works with DOJ and the Federal Bureau of Investigation (FBI), as appropriate. The OIG also obtains necessary investigative assistance from OIT, including the prompt retrieval of employee e-mails and forensic analysis of computer hard drives. The OIG investigative staff also consults as necessary with the Commission's Ethics Counsel to coordinate activities.

Upon completion of an investigation, the OIG investigator prepares a comprehensive report of investigation that sets forth the evidence obtained during the investigation. Investigative matters are referred to SEC management and DOJ as appropriate. The OIG does not publicly release its reports of investigation because they contain nonpublic information. The Commission decides whether an OIG investigative report should be publicly released, in response to a Freedom of Information Act request or otherwise.

In many investigative reports provided to SEC management, the OIG makes specific findings and recommendations for consideration of administrative action by management The OIG requests that management report to the OIG what, if any, administrative actions have been taken in response to the OIG's recommendations within 45 days of the issuance of the report. The OIG follows up as appropriate with management to determine the status of administrative action taken in matters referred by the OIG. The OIG may also make recommendations for improvements in policies, procedures, and internal controls in its investigative reports and closed 18 such investigative recommendations during the reporting period.

INVESTIGATIONS AND INQUIRIES CONDUCTED

Investigation Into Misuse of Resources and Violations of Information Technology Security Policies Within the Division of Trading and Markets (Report No. OIG-557)

During the semiannual reporting period, the OIG completed its investigation of an anonymous complaint alleging mismanagement of a computer security lab in the Division of Trading and Markets. The anonymous complaint alleged that lab staff inappropriately allocated and spent significant budget dollars to purchase computer equipment for the lab without justification or planning; used unencrypted laptops during inspections, in violation of SEC information technology security policies; and inappropriately used SEC funds for training without filing appropriate training forms. The anonymous complaint alleged unprofessional behavior, ineffective management, and misuse of unrestricted Internet access.

To investigate the allegations in the complaint, the OIG obtained and reviewed the e-mail records for eight current and former SEC employees who worked in the lab. The OIG also reviewed numerous documents pertaining to the lab and took on-the-record testimony of twelve current and former SEC employees with knowledge of the facts or circumstances surrounding the lab's operations, functions, or acquisitions.

The OIG investigation found that since 2006, lab staff spent over $1 million dollars on computer equipment and software with little oversight or planning and that a significant portion of the equipment and software purchased was unneeded

or never used in the program. The OIG found that although the lab's budget was vetted by a project review board and the actual equipment and software purchases were submitted through OIT, neither the review board nor OIT knew enough about the lab, its mission, or the items it was purchasing to adequately judge whether the money was being effectively spent. Further, the OIG found that the lab continued to spend money on technology despite not having the staff to implement the technology it was buying. In addition, the OIG discovered that some equipment was taken home by lab employees and used primarily for personal purposes.

The OIG also found that some of the lab's equipment was purchased based on misrepresentations made by lab staff in contracting documents. During testimony, two lab staff admitted misrepresenting in contracting documents that the lab needed a certain brand of computer because the entities the staff inspected were commonly using that brand and that computer tablets were needed for a specific method of testing. However, the OIG found that brand of computers identified in the contracting documents was not commonly used at the entities the staff inspected and that the tablets could not in fact be used for the purpose stated in the contracting documents.

In addition, the OIG discovered that lab staff members were taking unencrypted laptops and laptops without virus protection on inspections. Because the laptops used by the lab staff were not configured by OIT, the lab staff members were responsible for installing and maintaining encryption and antivirus software on those laptops. However, several laptops had no such protection and the lab had no internal policies regarding installing or maintaining encryption and virus protection on the lab equipment, despite an SEC-wide requirement that all portable media, including laptops, contain encryption. Moreover, the OIG found that even the few laptops identified as having encryption and virus protection may not have had that protection installed until late 2011.

Although no lab laptop was reported lost or stolen, the unprotected laptops could have been compromised. The OIG found evidence that the unprotected laptops were left unattended in hotel rooms and in offices outside the SEC and that the laptops were connected to public wireless networks at hotels. The OIG also found that the laptops and the data they contained were placed at risk when they were connected to an unfiltered, unmonitored Internet connection in the lab, which was used to access Internet sites otherwise prohibited by SEC policy, such as personal e-mail sites. The staff also used the lab Internet to download freeware onto the unprotected laptops in violation of SEC policy. Additionally, lab staff, including a manager, brought in personal computers, which were connected to the lab network, thereby potentially infecting that network with viruses and malware.

Further, the OIG found that the lab staff's multiple violations of SEC information technology security policies occurred despite the SEC having spent hundreds of thousands of dollars training the lab staff. The lab staff had perhaps the largest per person training budget at the SEC, spending, with little oversight, an average of $20,000 on training per person per year. Lab staff could choose from a variety of classes offered by prepaid training vendors and sign up for those classes without filling out training forms usually required for other SEC staff. Lab staff members were also not required to sign continued service agreements in connection with their training. Therefore, they were able to leave the SEC any time after building up their resumes with tens of thousands of dollars in training paid for by the SEC.

Overall, the OIG found that lab management did very little to monitor what was happening in the lab. Managers could not physically access the lab

with their badges for several years, did not know what equipment the lab purchased or what it was used for, and did not track or monitor the training that lab staff received. Management also did not put in place policies and procedures to protect the data lab staff collected or take any steps to ensure that lab staff members abided SEC OIT policies.

Because of the nature of the issues the OIG discovered in its investigation and in an effort to protect the information contained in the lab and on lab equipment, the OIG informed SEC management about the issues uncovered in the investigation before the OIG had issued its report of investigation in this matter. As a consequence, before the report was issued, SEC management commenced certain actions to address the problems and deficiencies the OIG investigation identified. Among other things, the SEC contracted with an outside forensics team to conduct testing and related work on selected laptops that had been used by the lab staff. In addition, management implemented several policy changes, including requiring that staff use only laptops with management's pre-approved security configurations. SEC management also placed two employees on paid, non-duty status pending completion of the OIG investigation. Both employees resigned shortly before the report was issued.

The OIG issued its report of investigation to management on August 30, 2012, for consideration of appropriate administrative action with respect to the individuals responsible for the problems and deficiencies who remained employed by the SEC. The OIG also recommended that (1) OIT exercise authority over the lab to ensure its equipment was properly secured and protected; (2) the lab's future equipment purchases be properly monitored by another SEC office; and (3) lab staff be required to complete appropriate training forms and the SEC clarify its policy on continued services agreements. In addition, the report was provided to the OIG Office of Audits for consideration of conducting follow-up audits of the lab and, more broadly, of the purchase of information technology equipment throughout the SEC to ensure that proper controls are in place to prevent waste and potential data breaches in the future.

Subsequent to the issuance of the OIG's report, the outside vendor the SEC retained to perform forensic analysis on select lab laptops issued its report, which indicated that forensic analysis was performed on eight laptops and no evidence of a compromise was found. The OIG plans to perform further review of this matter as necessary.

Physical Altercation and Security Violations by a Division of Enforcement Contractor (Report No. OIG-572)

The OIG opened this investigation immediately after learning from a confidential source that an unauthorized entry and a physical altercation occurred within the SEC headquarters facility. The confidential source informed the OIG that a male, later identified as a Division of Enforcement contractor, circumvented security protocol by inappropriately granting his girlfriend access to SEC space and had a physical altercation with the woman on SEC premises. The confidential source stated that the SEC Office of Security Services (OSS) and the SEC's contract security force were made aware of the altercation after security officers who are employed by the SEC headquarters building landlord—not the SEC—witnessed the incident. The confidential source also alleged that the incident was facilitated in part by inadequate security measures.

The OIG conducted an investigation of this matter and substantiated the allegations that both an unauthorized entry and a physical altercation occurred in the SEC's headquarters on the night in question. During the course of this investigation, the OIG took sworn testimony from and interviewed multiple individuals with knowledge of facts

relevant to the investigation. The OIG also obtained and reviewed SEC video footage of the reported unauthorized entry and physical altercation, as well as relevant documents, including security incident reports, an SEC personnel security file, criminal history reports and other public records. Additionally, the OIG searched approximately 64,000 e-mails for 9 current and former SEC employees and contractors relevant to this matter. Further, the OIG visited the SEC's Security Command Center to review the camera monitoring function and notified the Washington Metropolitan Police Department of the incident.

The OIG investigation determined that the SEC's OSS was notified of the physical altercation and unauthorized access through building management security, rather than through the SEC's contract security force. The OIG investigation also found that an SEC security camera was trained on the area where the altercation occurred and there was an audible alarm sounding continuously from an SEC turnstile, which was triggered when the unidentified woman exited the turnstile without an SEC badge. However, the SEC's contract security force officers did not respond to the scene during the incident, but did eventually turn off the sounding alarm. The OIG's investigation also revealed that the SEC contractor involved in the altercation and unauthorized entry was allowed to leave the facility that evening and returned to work the following day, but was then removed from the facility.

The OIG investigation further found that the SEC contractor had numerous prior criminal convictions, but was nonetheless was granted a waiver for investigation requirements to enter on duty, issued a contractor badge, and received full access to SEC headquarters and information technology systems for several years. The contractor was only removed from the SEC contract the day after the physical altercation occurred. Further, the OIG learned from OSS that other contractors employed at the SEC may have criminal records. Subsequent to the incident in question, OSS management began a review of these contractors' access to SEC facilities and systems.

The OIG issued its report of investigation to management on August 17, 2012, describing the findings of the investigation in detail. As a result of these findings, the OIG Office of Investigation referred the identified personnel security and physical security deficiencies to the OIG's Office of Audits for consideration of appropriate audits. The OIG also referred the matter to management for purposes of taking appropriate corrective action to remedy the findings contained in the report of investigation.

Fraud, Falsification, and Misuse of Computer Resources by Headquarters Employees (Report No. OIG-563)

During the semiannual reporting period, the OIG completed its investigation into fraud, falsification, and misuse of computer resources involving two headquarters employees. The investigation was conducted jointly with the District of Columbia OIG and the U.S. Office of Personnel Management OIG.

As noted in our semiannual report for the period ending March 31, 2012, the first employee had pled guilty in District of Columbia Superior Court to one count of first degree felony fraud. In April 2012, the employee was sentenced to 365 days in jail with all but 20 days suspended and five years of probation, and was ordered to pay restitution in the amount of approximately $30,000.

The OIG's investigation of the second employee's conduct uncovered evidence of various acts of falsification and misuse of government computer resources by the employee. Specifically, the investigation uncovered evidence that the employee had submitted false claims for expenses of approximately $14,500 to the federal flexible spending

account program during a five-year period, and had obtained reimbursement for those false claims. As a results of this fraudulent conduct, the employee received a tax benefit to which she was not entitled (of approximately 30 percent of the fraudulent claims) and potentially avoided forfeiture of contribution amounts that she had not spent on qualifying health care or dependent care expenses.

The investigation also found evidence that the employee had submitted fictitious college registration statements in order to obtain scholarship funds from a nonprofit charitable organization comprised of former agency employees. These scholarship monies were to be used toward tuition payments for an undergraduate degree program; however, the employee admitted that she was not attending classes at the time and used the money to pay household expenses. Finally, the investigation found evidence that the employee had misused her SEC e-mail account in connection with the falsification of her personal credit union statements, which she used to obtain short-term loans.

On August 31, 2012, the OIG issued a detailed report of investigation to management, discussing its findings with respect to the second employee's misconduct. The OIG referred the matter for consideration of appropriate administrative action against the employee, and such action was pending as of the end of the reporting period. In addition, the OIG referred the second employee to the United States Attorney's Office of the District of Columbia, which declined prosecution in favor of administrative action. The OIG also referred evidence concerning the employee's student loans to the Department of Education OIG.

Unauthorized Disclosure of Nonpublic Information Concerning an Enforcement Matter (Report No. OIG-575)

During the semiannual reporting period, the OIG opened an investigation into a complaint alleging that nonpublic SEC information had been disclosed to a reporter concerning the Commission's consideration of an action recommended by Enforcement against a corporation. A news article had been published electronically shortly before the Commission considered this Enforcement recommendation, which identified the corporation by name and described the nature of the charges against the corporation that were reportedly to be considered by the Commission that day. Commission regulations expressly prohibit SEC employees from disclosing nonpublic information unless specifically authorized to do so.

The OIG investigated whether a leak in fact occurred and whether there was evidence that the source of the leak was an SEC employee. During the investigation, the OIG obtained and searched over 135,000 e-mails of 28 current or former SEC employees. The OIG also conducted interviews of the complainant and 26 current SEC employees. In addition, the OIG obtained and reviewed documents that were related to the Enforcement investigation and Commission action concerning the corporation, as well as SEC Blackberry telephone records and news media articles concerning the SEC's action against the corporation.

The OIG investigation confirmed that information concerning the SEC's consideration of proceedings against the corporation was improperly disclosed outside the Commission. However, based upon the evidence obtained during the investigation, the OIG was unable to conclude which specific individual or individuals improperly disclosed this information, or whether the disclosure was made by someone employed outside the SEC. On September 27, 2012,

the OIG issued a report of investigation in this matter to management for informational purposes. The OIG's report described its findings in detail and encouraged management to continue to advise employees, through training, correspondence, and other means, of the prohibition on disclosing non-public information without authorization.

Allegations of Theft and/or Improper Handling of SEC Blackberries (Report No. OIG-566)

The OIG concluded its investigation based upon a referral from the SEC's OIT regarding information that it had received from its wireless services provider concerning potentially improper orders of BlackBerries on the SEC's account. Specifically, the wireless services provider notified the SEC that certain orders of BlackBerry devices placed on the SEC's account were being shipped to what appeared to be a residential address, which, upon review, was determined to belong to an SEC contractor.

To investigate the alleged theft or improper handling of these SEC Blackberries, the OIG took the sworn testimony of the SEC contractor in question. During his testimony, the contractor admitted that he had ordered the BlackBerry devices and had them shipped to his home address, but stated that he had brought all the devices into the office and deployed them to the agency. The OIG also conducted interviews of relevant OIT personnel, who informed the OIG that these BlackBerries were not in the SEC's possession. The OIT personnel also informed the OIG that the SEC contractor did not have the authority to order these devices on behalf of the SEC. In addition, the OIG consulted the wireless services provider, which informed the OIG that at least some of these BlackBerry devices ordered by the contractor and shipped to his home are active on a non-SEC account. Accordingly, the OIG concluded that these BlackBerries were sold or otherwise conveyed to non-SEC users, but based on the available evidence, the OIG was unable to determine that the contractor was responsible for that sale or conveyance.

After learning of the BlackBerry orders in question, the SEC requested that the contractor be removed from the relevant OIT contract and terminated his access to SEC facilities. Shortly thereafter, his employment with the contractor was terminated. Moreover, during our investigation, we learned that OIT has instituted new procedures for ordering BlackBerries on behalf of the SEC.

In light of the fact that the contractor is no longer working at the SEC, and that OIT has developed new property control procedures, the OIG concluded that the likelihood of additional harm to the agency had been greatly reduced. The OIG issued a report of investigation to management on September 18, 2012. The OIG's report described in detail the evidence obtained during the investigation and recommended that OIT formalize and document its new procedures in writing to avoid recurrence of this situation.

Allegation of Leak of Draft Interagency Rule (PI 12-01)

The OIG completed its inquiry into the public disclosure of a confidential draft document prepared in connection with the so-called "Volcker Rule." Under the Dodd-Frank Act, the SEC, along with four other financial and bank regulatory agencies, was tasked with coordinating and issuing certain rules, including the Volcker Rule, which would implement the Dodd-Frank Act's prohibition of, among other things, proprietary trading by banking entities. The SEC has worked with the four other agencies on the rulemaking process. On October 5, 2011, a banking industry newspaper published on its website an article stating that it had obtained a draft document outlining key details of the Volcker Rule and containing a link to a 205-page PDF file

purporting to be that draft document. The OIG opened its inquiry into the public disclosure of that draft document on October 13, 2011, after being contacted by the Senate Banking Committee.

The OIG's inquiry focused on determining whether there was any evidence that the draft document was disclosed by anyone within the SEC and, if so, by whom. During its inquiry, the OIG obtained and searched e-mails of 48 current and former SEC employees who had some involvement in the rule-making process during the relevant time period. The OIG also took the sworn testimony of 42 current SEC employees.

The OIG inquiry did not identify any source within the SEC who provided a copy of the draft document to the industry newspaper or any other entity or person outside the SEC or the coordinating agencies working on the rule. Additionally, the OIG was unable to identify any draft within the SEC files it reviewed that corresponded exactly to the version of the draft document published by the newspaper. As a result, on July 27, 2012, the OIG issued a memorandum report describing the results of its inquiry to management for informational purposes.

Allegations of Misuse of Official Time and Violation of Time and Attendance Rules (PI 12-16)

The OIG conducted a preliminary inquiry into an anonymous complaint alleging that a regional office senior counsel regularly arrived for work late and also left the office during core business hours without taking leave for these absences. A subsequent anonymous complaint alleged that this senior counsel was a board member of a local school organization and exhibited unethical behavior in the workplace. During the inquiry, the OIG also considered whether the senior counsel used official time and SEC resources to improperly support fund-raising efforts and whether the personal solicitations made on a school's behalf were permissible.

During this inquiry, the OIG reviewed relevant time and attendance and regional office security log records. Additionally, the OIG examined the senior counsel's remote computer access to the SEC network and obtained and searched the senior counsel's e-mails for pertinent time periods. In addition, the OIG took the testimony of the senior counsel's supervisor and attempted to take the testimony of the senior counsel, who terminated the interview.

The OIG inquiry found evidence that the regional office senior counsel violated the Standards of Ethical Conduct for Employees of the Executive Branch by using official time and resources to support various school fundraisers. The OIG also found that the amount of work time the senior counsel spent on school fundraisers was excessive and may have diminished his work productivity. Further, the OIG determined that among the companies the senior counsel solicited for school fundraisers were publicly traded companies, which are "prohibited sources" for solicitation by SEC employees. The OIG also found that the senior counsel improperly used his SEC title (in addition to his SEC e-mail account) in personal solicitations on behalf of the schools for which he was fundraising. Finally, the OIG substantiated the allegation that the employee frequently arrived at work late, and also found that the employee's supervisor was aware of this issue and had brought it to the senior counsel's attention.

As a result of the OIG's findings, the OIG issued a memorandum report to management on August 2, 2012, and referred the matter for consideration of administrative action against the employee. The OIG also obtained a declination of criminal prosecution in the matter, and administrative action by management was pending at the end of the reporting period.

Review of Legislation and Regulations

During the semiannual reporting period, the OIG reviewed legislation and proposed and final rules and regulations relating to the SEC's programs and operations, pursuant to Section 4(a)(2) of the Inspector General Act, as amended.

In particular, the OIG reviewed the requirements and history of Section 1504 of the Dodd-Frank Act, which mandated reporting of payments made to governments for the extraction of oil, natural gas, and minerals by companies that must file disclosures with the SEC, as well as the status of the SEC's related rulemaking. The OIG's review was performed in response to a request from U.S. Senators Richard Lugar and Benjamin Cardin, the sponsors of the amendment that became Section 1504, that the OIG evaluate the status of the SEC's implementation of Section 1504.

The OIG also reviewed statutes, rules, and regulations, and their impact on Commission programs and operations, within the context of reviews, audits, and investigations conducted during the reporting period. For example, in the OIG's review of the SEC's COOP (Report No. 502, issued April 23, 2012), the OIG reviewed the SEC OIT policies and procedures relating to business continuity management, business impact analysis, and disaster recovery planning. The OIG determined that these policies were outdated and recommended that the all of the agency's COOP policies and procedures be revised and updated. Similarly, during its audit of the SEC's record management practices (Report No. 505, issued September 30, 2012), the OIG reviewed the SEC administrative regulations pertaining to records management and found that they had not been updated for several years, with one regulation dating back to May 1991. The OIG recommended that the Office of Support Operations ensure that these regulations are revised.

During an investigation completed during the reporting period into the misuse of resources and violations of information technology security policies (Report No. OIG-557, issued August 30, 2012), the OIG reviewed the requirements of the SEC's training and development policy in effect at the time of the conduct described in the OIG's report. In particular, the OIG reviewed the paragraph of the policy related to continued service agreements for training and recommended clarification of this policy. The former training and development policy has been superseded by a new administrative regulation on continued service agreements for education and training.

Also during the reporting period, the OIG reviewed a draft administrative regulation on the manage-

ment and administration of service contracts and a related draft operating procedure and checklist. The OIG provided comments on the draft documents based upon information acquired during an investigation the OIG had conducted during the previous semiannual reporting period into an allegation of an improper personal services contract (Report OIG-569, issued March 29, 2012).

Finally, in coordination with the Legislation Committee of the CIGIE and other OIGs, the SEC OIG reviewed and tracked various legislation that would impact OIGs, including H.R. 4404, "Sunshine on Government Act of 2012," and S. 300, "Government Charge Card Abuse Prevention Act."

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 Office of Inspector General agrees with all significant management decisions regarding audit recommendations.

INSTANCES WHERE INFORMATION WAS REFUSED

During this reporting period, there were no instances where information was refused.

TABLES

Table 1. List of Reports: Audit and Evaluations

Report Number	Title	Date Issued
502	Review of the SEC's Continuity of Operations Program	4/23/12
505	SEC's Records Management Practices	9/30/12
508	The Office of International Affairs Internal Operations and Travel Oversight	9/30/12

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

Recommendations Open 180 days or more

Report Number and Title	Issue Date	Summary of Recommendations
439—Student Loan Program	3/27/2008	In consultation with the National Treasury Employees Union, develop a detailed distribution plan.
474—Assessment of the SEC's Bounty Program	3/29/2010	Develop a communication plan to address outreach to both the public and SEC personnel regarding the SEC bounty program, which includes efforts to make information available on the SEC's intranet, enhance information available on the SEC's public website, and provide training to employees who are most likely to deal with whistleblower cases.
		Examine ways in which the Commission can increase communications with whistleblowers by notifying them of the status of their bounty requests without releasing nonpublic or confidential information during the course of an investigation or examination.
		Require that a bounty file (hard copy or electronic) be created for each bounty application, which should contain at a minimum the bounty application, any correspondence with the whistleblower, documentation of how the whistleblower's information was utilized, and documentation regarding significant decisions made with regard to the whistleblower's complaint.
		Incorporate best practices from the Department of Justice (DOJ) and the Internal Revenue Service (IRS) into the SEC bounty program with respect to bounty applications, analysis of whistleblower information, tracking of whistleblower complaints, recordkeeping practices, and continual assessment of the whistleblower program.
		Set a timeframe to finalize new policies and procedures for the SEC bounty program that incorporate the best practices from DOJ and IRS, as well as any legislative changes to the program.
480—Review of the SEC's Section 13(f) Reporting Requirements	9/27/2010	Update Form 13F to a more structured format, such as Extensible Markup Language, to make it easier for users and researchers to extract and analyze Section 13(f) data.
482—Oversight of and Compliance with Conditions and Representations Related to Exemptive Orders and No-Action Letters	6/29/2011	Develop processes, including written policies and procedures, regarding reviewing for compliance with conditions and representations in exemptive orders and no-action letters issued to regulated entities on a risk basis.

Table 3. Reports with Recommendations, continued

Recommendations Open 180 days or more

Report Number and Title	Issue Date	Summary of Recommendations
		In plans for implementing Section 965 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, develop procedures to coordinate examinations with those conducted by the Office of Compliance Inspections and Examinations and, as appropriate, include provisions for reviewing for compliance with the conditions in exemptive orders and representations made in no-action letters on a risk basis.
		In connection with monitoring efforts, include compliance with the conditions and representations in significant exemptive orders and/or no-action letters issued to regulated entities as risk considerations.
485—Assessment of the SEC's Privacy Program	9/29/2010	Evaluate risk assessment processes for scoring risk to ensure that the Office of Information Technology adequately weighs all appropriate factors, including the identification of risk levels by vendors.
		Implement an agency-wide policy regarding shared folder structure and access rights, ensuring that only the employees involved with a particular case have access to that data. If an employee backs up additional information to the shared resources, only the employee and his or her supervisor should have access.
		Ensure personal storage tab (PST) files are saved to a protected folder.
489—2010 Annual FISMA Executive Summary Report	3/3/2011	Complete a logical access integration of the Homeland Security Presidential Directive 12 card no later than December 2011, as reported to the Office of Management and Budget on December 31, 2010.
491—Review of Alternative Work Arrangements, Overtime Compensation, and COOP-Related Activities at the SEC	9/28/2011	In developing the new Human Capital Directive, work with the National Treasury Employees Union to determine whether additional alternative work schedules, such as the gliding, variable day, variable week, three-day workweek, and Maxiflex options described in the Office of Personnel Management Handbook on Alternative Work Schedules, should be adopted as options for SEC employees.

Table 3. Reports with Recommendations, continued

Recommendations Open 180 days or more

Report Number and Title	Issue Date	Summary of Recommendations
		Negotiate revisions to the language in the collective bargaining agreement between the Commission and the National Treasury Employees Union with respect to the use of credit hours by employees working conforming schedules, ensuring that the revised language conforms with applicable law.
		Perform server stress tests that incorporate a variety of applications used with remote access.
492—Audit of SEC's Employee Recognition Program and Recruitment, Relocation, and Retention Incentives	8/2/2011	Develop and implement a mechanism to reward employees for superior or meritorious performance within their job responsibilities through lump-sum performance awards.
493—OCIE Regional Offices' Referrals to Enforcement	3/30/2011	Continue efforts to establish a complete interface between the Super Tracking and Review System or its equivalent, the Hub, and the Tips, Complaints, and Referrals system.
497—Assessment of SEC's Continuous Monitoring Program	8/11/2011	Ensure that security controls configurations that are applied in the production environment are identical with those applied in the testing environment.
		Develop and implement written procedures to ensure consistency in the Commission's production and testing environments. These procedures should detail the software and hardware components in both environments and specify the actions required to maintain consistent environments.
		Complete and finalize written server and storage log management policies and procedures that fully document the roles and responsibilities for log capture, management, retention, and separation of duties.
		Analyze the level of criticality of the Commission data and the needs and wants of its customers, and establish an appropriate backup retention period based on the results of the analysis and that meets the requirements of the Commission.
		Ensure that tapes are handled appropriately.
500—Assessment of SEC's System and Network Logs	3/16/2011	Identify capacity requirements for all servers, ensure sufficient capacity is available for the storage of audit records, configure auditing to reduce the likelihood that capacity will be exceeded, and implement a mechanism to alert and notify appropriate Commission office/divisions when log storage capacity is reached.

Table 3. Reports with Recommendations, continued

Recommendations Open 180 days or more

Report Number and Title	Issue Date	Summary of Recommendations
		Review and update all logging policies and procedures consistent with the policy's review interval requirements and retain evidence of its reviews and any updates to the policy.
501—2011 Annual FISMA Executive Summary Report	2/2/2012	Develop and implement a detailed plan to review and update OIT security policies and procedures and to create OIT security policies and procedures for areas that lack formal policy and procedures.
		Develop a comprehensive risk management strategy in accordance with National Institute of Standards and Technology's (NIST) *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, which will ensure that management of system-related security risks is consistent with the Commission's mission/business objectives and overall risk strategy.
		Update risk management policy to include language regarding developing a comprehensive governance structure and ensure that management of system-related security risks is consistent with the Commission's mission/business objectives and overall risk strategy.
		Develop and implement a formal risk management procedure that identifies an acceptable process for evaluating system risk consistent with the Commission's mission or business objectives and overall risk strategy.
		Develop and implement formal policy that addresses tailoring baseline security controls sets.
		Determine whether to perform the tailoring process at the organization level for all information systems (either as the required tailored baseline or as the starting point for system-specific tailoring) at the individual information system level, or by using a combination of organization-level and system-specific approaches.
		Tailor a baseline security controls set (with rationale) for applicable systems in accordance with NIST's *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, and NIST's Recommended Security Controls for Federal Information Systems and Organizations*.
		Review and document the current standard baseline configuration, including identification of approved deviations and exceptions to the standard.

Table 3. Reports with Recommendations, continued

Recommendations Open 180 days or more

Report Number and Title	Issue Date	Summary of Recommendations
		Conduct compliance scans of information technology devices, according to the organizationally defined frequency in the policy and procedures, to ensure that all devices are configured as required by OIT's configuration management policy and procedures.
		Update policy and include language indicating that deviations from baseline configurations that are identified and documented as a result of the configuration compliance scans are properly remediated in a timely manner.
		Complete the implementation of the technical solution for linking multi-factor authentication to Personal Identity Verification cards for system authentication and require use of the cards as a second authentication factor by December 2012.
PI-09-05—SEC Access Card Readers in Regional Offices	2/22/2010	Ensure, on a Commission-wide basis, that all regional offices are capable of capturing and recording building entry and exit information of Commission employees.
ROI-505—Failure to Timely Investigate Allegations of Financial Fraud	2/26/2010	Ensure as part of changes to complaint handling system that databases used to refer complaints are updated to accurately reflect status of investigations and identity of staff.
ROI-544—Failure to Complete Background Investigation Clearance Before Giving Access to SEC Buildings and Computer Systems	1/20/2011	Take immediate measures to determine whether every OIT employee and contractor has been properly cleared by a background investigation and issued an official SEC badge.
ROI-551—Allegations of Unauthorized Disclosures of Nonpublic Information During SEC Investigations	3/30/2011	Employ technology that will enable the agency to maintain records of phone calls made from and received by SEC telephones.
ROI-560—Investigation of Conflict of Interest Arising from Former General Counsel's Participation in Madoff-Related Matters*	9/16/2011	Reconsider position that net equity for Madoff customer claims be calculated in constant dollars by conducting a re-vote, and advise the bankruptcy court of the results.

*Shortly after the close of the semiannual reporting period, the Commission conducted a re-vote. The Commission is in the process of advising the bankruptcy court of the results of the re-vote.

Table 4. Summary of Investigative Activity

Cases	Number
Cases Open as of 3/31/2012	10
Cases Opened during 4/1/2012 - 9/30/2012	4
Cases Closed during 4/1/2012 - 9/30/2012	8
Total Open Cases as of 9/30/2012	6
Referrals to Department of Justice for Prosecution	3
Prosecutions	0
Convictions	0
Referrals to OIG Office of Audits	2
Referrals to Agency for Administrative Action	4

Preliminary Inquiries	Number
Inquiries Open as of 3/31/2012	58
Inquiries Opened during 4/1/2012 - 9/30/2012	14
Inquiries Closed during 4/1/2012 - 9/30/2012	31
Total Open Inquiries as of 9/30/2012	41
Referrals to Department of Justice for Prosecution	1
Referrals to Agency for Administrative Action	1

Disciplinary Actions (including referrals made in prior periods)	Number
Removals (Including Resignations and Retirements)	5
Suspensions	3
Reprimands	0
Warnings/Other Actions	3

Table 5. Summary of Complaint Activity

Complaints Received During the Period	Number
Complaints Pending Disposition at Beginning of Period	1
Hotline Complaints Received	172
Other Complaints Received	110
Total Complaints Received	282
Complaints on which a Decision was Made	270
Complaints Awaiting Disposition at End of Period	13

Dispositions of Complaints During the Period	Number
Complaints Resulting in Investigations	3
Complaints Resulting in Inquiries	13
Complaints Referred to OIG Office of Audits	1
Complaints Referred to Other Agency Components	153
Complaints Referred to Other Agencies	10
Complaints Included in Ongoing Investigations or Inquiries	6
Response Sent/Additional Information Requested	44
No Action Needed	42

Table 6. References to Reporting Requirements of the Inspector General Act

The Inspector General Act of 1978, as amended, specifies reporting requirements for semiannual reports to Congress. The requirements are listed below and indexed to the applicable pages.

Section	Inspector General Act Reporting Requirement	Pages
4(a)(2)	Review of Legislation and Regulations	35–36
5(a)(1)	Significant Problems, Abuses, and Deficiencies	9–12; 18–23; 28–34
5(a)(2)	Recommendations for Corrective Action	18–23; 28–34
5(a)(3)	Prior Recommendations Not Yet Implemented	40–44
5(a)(4)	Matters Referred to Prosecutive Authorities	45
5(a)(5)	Summary of Instances Where Information Was Unreasonably Refused or Not Provided	37
5(a)(6)	List of OIG Audit and Evaluation Reports Issued During the Period	39
5(a)(7)	Summary of Significant Reports Issued During the Period	18–23; 28–34
5(a)(8)	Statistical Table on Management Decisions with Respect to Questioned Costs	39
5(a)(9)	Statistical Table on Management Decisions on Recommendations That Funds Be Put to Better Use	39
5(a)(10)	Summary of Each Audit, Inspection or Evaluation Report Over Six Months Old for Which No Management Decision has been Made	37
5(a)(11)	Significant Revised Management Decisions	37
5(a)(12)	Significant Management Decisions with Which the Inspector General Disagreed	37
5(a)(14)	Appendix of Peer Reviews Conducted by Another OIG	49

APPENDIX A. Peer Reviews of OIG Operations

PEER REVIEW OF THE SEC OIG'S AUDIT OPERATIONS

In accordance with the CIGIE quality control and assurance standards, an OIG's audit functions are assessed by an external OIG audit team approximately every three years. 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 is suitably designed to provide the OIG with a reasonable assurance of conforming with applicable professional standards.

On August 23, 2012, LSC OIG issued its report, concluding that the SEC OIG complied with the system of quality control and that it 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. Federal audit organizations can receive a rating of "pass," "pass with deficiencies," or "fail." The SEC OIG received a "pass" rating, and no recommendations were made. Further, there are no outstanding recommendations from previous peer reviews of our audit organization.

A copy of the peer review report was provided to the SEC Chairman and Commissioners. The peer review report is located on OIG's website at: www.sec-oig.gov/Reports/Semiannual/2012/OIG_SAR_Spring2012.pdf

PEER REVIEW OF THE SEC OIG'S INVESTIGATIVE OPERATIONS

During the semiannual reporting period, the SEC OIG did not have an external peer review of its investigative operations. Peer reviews of Designated Federal Entity OIGs, such as the SEC OIG, are conducted on a voluntary basis. The most recent peer review of the SEC OIG's investigative operations was conducted by the U.S. Equal Employment Opportunity Commission (EEOC) OIG. The EEOC OIG issued its report on the SEC OIG's investigative operations in July 2007. This report concluded that the SEC OIG's system of quality for the investigative function conformed to the professional standards established by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (now CIGIE).

The OIG plans to submit a request to CIGIE's Investigations Committee for an investigative operations peer review during fiscal year 2013.

APPENDIX B. Annual Report on the OIG SEC Employee Suggestion Hotline—Issued Pursuant to Section 966 of the Dodd-Frank Act

INTRODUCTION AND BACKGROUND

The OIG established the OIG SEC Employee Suggestion Program in accordance with Section 966 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). Under Section 966 of the Dodd-Frank Act, the Securities Exchange Act of 1934 (15 U.S.C. § 78a et seq.) (Exchange Act) was amended to include a new Section 4D (15 U.S.C. § 78d-4), which required the Inspector General to establish a suggestion program for employees of the Commission. The OIG established its Employee Suggestion Program on September 27, 2010.

In accordance with Section 4D(d) of the Exchange Act, SEC OIG has prepared this second annual report containing a description of suggestions and allegations received, recommendations made or action taken by the OIG, and action taken by the Commission in response to suggestions or allegations from October 1, 2011, through September 30, 2012.

Through this program, the OIG receives suggestions from Commission employees for improvements in work efficiency, effectiveness, productivity, and the use of the resources of the Commission, as well as allegations by employees of the Commission of waste, abuse, misconduct, or mismanagement within the Commission. The OIG receives suggestions or allegations under this program through an e-mail mailbox and telephone hotline established to facilitate the making of suggestions or allegations.

The program operates pursuant to formal policies and procedures, which were adopted on March 30, 2011, and encompass both the receipt and handling of employee suggestions and allegations, as well as recognition of employees whose suggestions or disclosures to the OIG may result or have resulted in cost savings to or efficiencies within the Commission. The OIG held the first OIG SEC Employee Suggestion Program awards ceremony in December 2011, during which several SEC employees who had made suggestions resulting in agency cost savings were honored.

SUMMARY OF EMPLOYEE SUGGESTIONS AND ALLEGATIONS RECEIVED

Between October 1, 2011 and September 30, 2012, the OIG received and analyzed 53 suggestions or allegations. Set forth below are details regarding:

(1) The nature, number, and potential benefits of any suggestions received.
(2) The nature, number, and seriousness of any allegations received.
(3) Any recommendations made or actions taken *by the OIG* in response to substantiated allegations received.
(4) Any action taken *by the Commission* in response to suggestions or allegations received.

Nature and Potential Benefits of Suggestions	Number
Increase efficiency or productivity	12
Increase effectiveness	15
Increase the use of resources or decrease costs	14

Nature and Seriousness of Allegations[1]	Number
Mismanagement and/or discrimination	2
Waste of Commission resources	7
Misconduct by an employee	3

Nature and Potential Benefits of Suggestions	Number
Memorandum to or communication with the Commission requesting action be taken	14
Referred to OIG Office of Investigations	3
Referred to OIG Office of Audits	1
OIG Office of Investigations opened preliminary inquiry	2
Researched issue, but no further action by the Commission was necessary	22

Action Taken by the Commission[2]	Number
SEC management took specific action to address the suggestion	4
The Commission decided to secure new technology in response to the suggestion	1
SEC management is considering suggestion in context of existing procedures	2

[1] Suggestions and/or allegations may fall into more than one category and, as such, the numbers below may be greater than the total number of suggestions/allegations received.

[2] This table represents the Commission's response to suggestions and allegations that were referred to the Commission for consideration and for which a response was received during the reporting period.

EXAMPLES OF SUGGESTIONS RECEIVED

EDGAR Electronic Refund Requests

The OIG received a suggestion from an employee regarding fee-bearing filings made through the SEC's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system and the process by which EDGAR users request refunds of excess filing fees paid. At the time the suggestion was received, users were required to submit refund requests by mail or facsimile. The employee suggested that an online refund request form or process be developed to make the refund process more efficient for filers and SEC staff who process the refunds.

After reviewing and analyzing the suggestion received, the OIG forwarded it to the Office of Financial Management, which concurred with the suggestion. In July 2012, the EDGAR system was upgraded to support the electronic submission of requests for refunds of excess fees paid. In August 2012, the SEC adopted revisions to the EDGAR

Filer Manual to reflect the updates made to the EDGAR system.

Hard Copy CCHs

An employee suggested that cost savings could be achieved if the Commission decreased its number of subscriptions to hard copy Commerce Clearing House (CCH) securities law books and their corresponding regular hard copy updates and instead encouraged the use of CCH's online service, CCH IntelliConnect. The Commission pays an annual fee per hard copy of the CCH securities law volumes, but pays a regular annual subscription fee for the online version that is not dependent on the number of users. Currently, the Commission spends over $300,000 per year for hard copy subscriptions.

The OIG determined that, while the Commission has taken certain initiatives to decrease the number of hard copy CCH purchases, additional steps could be taken to reduce the costs associated with hard copy CCHs. The OIG forwarded the suggestion to the SEC's Branch of Library Services and suggested that it consider taking steps to ensure that additional information regarding the availability of this resource online be communicated to the staff on a regular basis. The OIG also recommended that the Branch of Library Services provide information to staff regarding the price discrepancy between the hard copy and online CCH versions, and offer training on the online resource to encourage more employees to use it. As of September 30, 2012, SEC management was still considering its response to this suggestion.

Employee Directories

The OIG received suggestions concerning the creation of an agency-wide employee directory or organizational chart that would include staff photos, titles, and other relevant information which, according to the employee, would facilitate organizational understanding for both new and long-term employees. The employee making the suggestions further stated that the creation of an expertise database to catalogue information regarding employees' previous work experience would allow colleagues to become more familiar with other employees throughout the Commission and facilitate knowledge sharing and organizational understanding.

The Division of Enforcement maintains a facebook and directory that includes certain staff information, such as photograph, phone number, e-mail address, office location, position, and start date. We discussed the suggestions we received with a representative of the SEC's SharePoint Executive Steering Committee, who stated that the SEC is currently considering expanding the facebook/directory feature to other offices and divisions. Further, according to the Steering Committee representative, the Committee believes that the inclusion of an expertise database could improve efficiency and effectiveness by facilitating knowledge sharing and there is wide support throughout the Commission for such a feature. The representative added that the Committee was already in the process of considering and/or taking steps to implement this suggestion.

Paper and Supply Waste

The OIG received several suggestions relating to paper and supply waste and ways in which such waste could be decreased or eliminated. One of these suggestions related to the use of specialized "Tech Wipes," which are specifically designed to be used for aerospace, electronics, and laboratories, but, according to the employee, are instead used by many employees as paper towels. The OIG forwarded this suggestion to the SEC's Facilities Branch, which stated that these wipes were purchased for and had specific uses, but agreed to limit the distribution, thereby decreasing their unnecessary or unintended use.

Another suggestion we received related to the printing of certificates through the Commission's Lead, Learn, and Perform (LEAP) training management system. According to this suggestion, the course completion certificates printed through LEAP were formatted to use three sheets of paper, with the third page being blank. The employee suggested that the certificate be reformatted to use only one sheet of paper and, therefore, decrease waste. The OIG contacted the Office of Human Resources, which indicated that it recognized the issue and then worked with the software vendor to eliminate the unnecessary pages for printed certificates.

EXAMPLES OF ALLEGATIONS RECEIVED

Replacement of Physical Security Systems in Regional Offices

The OIG received an allegation regarding the Commission's replacement of physical security systems in the regional offices. Specifically, the employee alleged that the decision to replace card readers and cameras in the regional offices was based on the fact that there were issues with such readers and cameras in SEC headquarters in Washington, D.C. According to the employee, the replacements in the regional offices were unnecessary and a waste of Commission resources.

The OIG discussed this allegation with the SEC's Office of Security Services and learned that Commission-wide changes to "access control systems," which included video cameras, alarm systems, and card readers, were required to improve security and become compliant with Homeland Security Presidential Directive 12 (HSPD-12). HSPD-12 provides for a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and federal contractors. According to the Office of Security Services, the Commission's previous security services were outdated and were not in compliance with HSPD-12, and the new systems were cost-effective and went through a substantial review process before implementation. The OIG determined that there appeared to be adequate justification for the replacement and/or upgrade of security services on an agency-wide basis.

Referrals to the Office of Investigations

The OIG received four allegations that resulted in referrals to the OIG's Office of Investigations. Allegations related to retaliation against an employee, as well as mismanagement and discrimination by a supervisor, were referred for inclusion in ongoing preliminary inquiries. In addition, the Office of Investigations opened preliminary inquiries based on the receipt of an allegation of potential misconduct by contractors and allegations of mismanagement, preferential treatment of contractors, and theft.

CONCLUSION

The OIG is pleased with the Employee Suggestion Program effectiveness. We received favorable responses from the SEC on several suggestions we submitted to them for consideration. Many suggestions resulted in positive changes that will improve SEC employee's efficiency and effectiveness and increase the use of SEC's resources, as well as decrease waste.

The OIG anticipates additional favorable responses to suggestions that the SEC is currently reviewing. We continue to encourage SEC employees to submit suggestions to OIG.

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 HOTLINE	www.sec-oig.gov/ooi/hotline.html	
FAX	202.772.9265	
MAIL	Office of Inspector General U.S. Securities and Exchange Commission 100 F Street, NE Washington, DC 20549	
EMAIL	oig@sec.gov	

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

Additional copies of this report may be obtained by contacting the
Office of Inspector General at 202.551.6061
The report is also available on the Inspector General's website at www.sec-oig.gov.

U.S. SECURITIES AND EXCHANGE COMMISSION
100 F STREET, NE | WASHINGTON, DC 20549