



Office of Inspector General

# SEMIANNUAL REPORT TO CONGRESS

10.01.19 TO 03.31.20

U.S. SECURITIES AND  
EXCHANGE COMMISSION



OFFICE OF INSPECTOR GENERAL  
SEMIANNUAL REPORT TO CONGRESS

---

OCTOBER 1, 2019 THROUGH MARCH 31, 2020



### OIG MISSION

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 U.S. Securities and Exchange Commission (Agency or SEC). We accomplish this mission by:

- conducting independent and objective audits, evaluations, and other reviews of SEC programs and operations;
- conducting independent and objective investigations of potential criminal, civil, and administrative violations that undermine the ability of the SEC to accomplish its statutory mission;
- preventing and detecting fraud, waste, and abuse in SEC programs and operations;
- identifying vulnerabilities in SEC systems and operations and making recommendations to improve them;
- communicating timely and useful information that facilitates management decision making and the achievement of measurable gains; and
- keeping Congress and the Chairman and Commissioners fully and currently informed of significant issues and developments.

“We continued our efforts to meet our strategic goals of (1) delivering results that promote integrity, efficiency, and effectiveness in the SEC’s programs and operations; (2) advancing an inclusive and dynamic OIG culture that inspires high performance; and (3) improving the effectiveness and efficiency of OIG processes through continuous innovation, collaboration, and communication.”

# CONTENTS

MESSAGE FROM THE INSPECTOR GENERAL . . . . .	1
MANAGEMENT AND ADMINISTRATION . . . . .	5
Agency Overview . . . . .	5
OIG Staffing, Resources, and Administration . . . . .	5
OIG Outreach . . . . .	6
OIG Annual Awards Program . . . . .	6
COORDINATION WITH OTHER AGENCIES . . . . .	7
AUDITS AND EVALUATIONS . . . . .	9
Overview . . . . .	9
Completed Audits and Evaluations . . . . .	9
<i>Audit of the SEC’s Compliance With the Digital Accountability     and Transparency Act for Fiscal Year 2019 (Report No. 557)</i> . . . . .	9
<i>The SEC Can More Strategically and Securely Plan, Manage,     and Implement Cloud Computing Services (Report No. 556)</i> . . . . .	10
<i>Final Management Letter: Evaluation of the U.S. Securities and     Exchange Commission’s Delinquent Filer Program</i> . . . . .	11
<i>Fiscal Year 2019 Independent Evaluation of the SEC’s Implementation     of the Federal Information Security Modernization Act (Report No. 558)</i> . . . . .	12
<i>The SEC’s Office of Broker-Dealer Finances Provides Effective Oversight,     But Opportunities To Improve Efficiency Exist (Report No. 559)</i> . . . . .	13
<i>Controls Over the SEC’s Travel Charge Card Program Could Be Strengthened To     More Fully Comply With Requirements and Maximize Benefits (Report No. 560)</i> . . . . .	14
Other Projects and Reports . . . . .	15
<i>IG’s Letter to OMB on the SEC’s Implementation of Purchase Card     Program Audit Recommendations</i> . . . . .	15
<i>Results of the Inspector General’s Fiscal Year 2019 Purchase Card     Program Risk Assessment</i> . . . . .	16
Ongoing Audits and Evaluations . . . . .	17
<i>Audit of the U.S. Securities and Exchange Commission’s Management     of Mobile Devices and Services</i> . . . . .	17
<i>Evaluation of the U.S. Securities and Exchange Commission’s Fiscal Year 2019     Compliance With the Improper Payments Elimination and Recovery Act of 2010</i> . . . . .	17
<i>Audit of the U.S. Securities and Exchange Commission’s Oversight of     the Infrastructure Support Services Contractor Performance</i> . . . . .	18
<i>Evaluation of the U.S. Securities and Exchange Commission’s Tips, Complaints,     and Referrals Program</i> . . . . .	18

INVESTIGATIONS . . . . .	19
Overview . . . . .	19
Report on Instances of Whistleblower Retaliation . . . . .	19
Status of Previously Reported Investigations . . . . .	20
<i>SEC Contractor Photographs Nonpublic Computer Screen Information</i> . . . . .	20
<i>Allegations of Fraud</i> . . . . .	20
Open and Completed Investigations . . . . .	21
<i>SEC Employee Impersonation and SEC Seal Fraud Scheme</i> . . . . .	21
<i>Unaccountable SEC Special Agent Badges</i> . . . . .	21
<i>SEC Employee Impersonation and SEC Seal Fraud Scheme</i> . . . . .	22
<i>Disclosure of Nonpublic Investigative Information</i> . . . . .	22
<i>Whistleblower Misconduct and False Statements</i> . . . . .	23
<i>SEC Manager Solicited and Accepted Gifts From Contractors</i> . . . . .	24
REVIEW OF LEGISLATION AND REGULATIONS . . . . .	25
MANAGEMENT DECISIONS . . . . .	29
TABLES . . . . .	30
<i>Table 1. List of Reports: Audits and Evaluations</i> . . . . .	30
<i>Table 2. Reports Issued With Questioned Costs or Recommendations That Funds Be Put to Better Use (Including Disallowed Costs)</i> . . . . .	31
<i>Table 3. Reports With Recommendations on Which Corrective Action Has Not Been Completed</i> . . . . .	32
<i>Table 4. Summary of Investigative Activity for the Reporting Period of October 1, 2019, to March 31, 2020</i> . . . . .	37
<i>Table 5. References to Reporting Requirements of the Inspector General Act</i> . . . . .	39
APPENDIX PEER REVIEWS OF OIG OPERATIONS . . . . .	41
Peer Review of the SEC OIG’s Audit Operations . . . . .	41
Peer Review of the SEC OIG’s Investigative Operations . . . . .	41
OIG GENERAL OFFICE CONTACT INFORMATION . . . . .	42

# ABBREVIATIONS

Acquisitions	Office of Acquisitions
Agency/SEC	U.S. Securities and Exchange Commission
Charge Card Act	Government Charge Card Abuse Prevention Act of 2012
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
COVID-19	Coronavirus
CSRA	SRA International Inc.
DATA Act	Digital Accountability and Transparency Act of 2014
DFP	Delinquent Filings Program
Dodd-Frank	Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010
DOJ	Department of Justice
ENF	Division of Enforcement
Exchange Act	Securities Exchange Act of 1934
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
FY19Q1	fiscal year 2019, first quarter
FY19Q1-2	fiscal year 2019, first and second quarters
GAO	Government Accountability Office
GPC	Government Purchase Card
IG	Inspector General
IPERA	Improper Payments Elimination and Recovery Act of 2010
ISS	infrastructure support services
IT	information technology
Kearney	Kearney & Company, P.C.
NSF	National Science Foundation
OA	Office of Audits
OBDF	Office of Broker-Dealer Finances
OI	Office of Investigations
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OSO	Office of Support Operations
OSS	Office of Security Services
PII	personally identifiable information
TCR	tips, complaints, and referrals
TM	Division of Trading and Markets
Treasury	U.S. Department of the Treasury
USAO	U.S. Attorney's Office
U.S.C.	United States Code





## MESSAGE FROM THE INSPECTOR GENERAL



I am pleased to present this Semiannual Report to Congress as Inspector General (IG) of the SEC. This report describes the work of the SEC OIG from October 1, 2019, to March 31, 2020, and reflects our responsibility to report independently to Congress and the Commission. The audits, evaluations, investigations, and other reviews that we describe illustrate the OIG's efforts to promote the efficiency and effectiveness of the SEC and demonstrate the impact that our work has had on the agency's programs and operations.

During this semiannual reporting period, we continued our efforts to meet our strategic goals of (1) delivering results that promote integrity, efficiency, and effectiveness in the SEC's programs and operations; (2) advancing an inclusive and dynamic OIG culture that inspires high performance; and (3) improving the effectiveness and efficiency of OIG processes through continuous innovation, collaboration, and communication.

During this reporting period, the OIG's *Office of Audits (OA)* issued its *Audit of the SEC's Compliance With the Digital Accountability and Transparency Act for Fiscal Year 2019* (Report

No. 557), which includes two recommendations to further improve the SEC's processes related to the Digital Accountability and Transparency Act of 2014 (DATA Act). Next, we issued *The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services* (Report No. 556), which includes three recommendations to improve the SEC's planning, management, and implementation of cloud strategies and the security of the SEC's cloud-based systems. Then, we issued the *Final Management Letter: Evaluation of the U.S. Securities and Exchange Commission's Delinquent Filings Program*, which includes two recommendations to improve efficiency of the

Delinquent Filings Program (DFP). Next, we issued the *Fiscal Year 2019 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014 (Report No. 558)*, which includes nine new recommendations to strengthen the SEC's information security program. Acting on these opportunities for improvement will help minimize the risk of unauthorized disclosure, modification, use, and disruption of the SEC's sensitive, nonpublic information, as well as assist the SEC's information security program reach the next maturity level. Next, we issued *The SEC's Office of Broker-Dealer Finances Provides Effective Oversight, But Opportunities To Improve Efficiency Exist (Report No. 559)*, which includes three recommendations to address areas that can improve the Office of Broker-Dealer Finances' (OBDF) oversight and efficiency. Finally, we issued the *Controls Over the SEC's Travel Charge Card Program Could Be Strengthened To More Fully Comply With Requirements and Maximize Benefits (Report No. 560)*, which includes 15 recommendations to strengthen controls over the Travel Charge Card Program.

OA also worked with SEC management to close 13 recommendations made in 6 OIG reports issued during this and previous semiannual reporting periods.

In addition, the *Office of Investigations (OI)* completed or closed 10 investigations during this reporting period. Our investigations resulted in 11 referrals to the Department of Justice (DOJ), 2 of which were accepted for prosecution, 3 referrals to management for administrative action, 1 conviction, and more than \$2 million in criminal fines, restitution, recoveries, assessments, and forfeitures.

I am also pleased to report that the OIG held its sixth annual OIG awards ceremony in March 2020 to honor service and outstanding achievements by OIG staff during 2019. At this ceremony, I recognized the specific contributions of the award recipients. I would like to express my gratitude to the award recipients, as well as all the OIG staff, for their continued hard work and dedication to the OIG's mission.

In particular, the 2019 SEC OIG Special Joint Team Award went to the team for the All Hands Training Committee. This team embarked on a months-long journey to gather and synthesize training topics from OIG staff, recruit trainers, facilitate logistics, and create an all-around memorable training event. This training is critical to the OIG staff to be able to accomplish its mission in an ever-changing environment relating to oversight of the Commission as it regulates the securities and marketplace activities.

The SEC OIG is in the early stages of incorporating more data analytics into our work products. Through analysis, modeling, and visualization, one can identify anomalies and extract other useful information. The preparation, analysis, and visualization of the insights about the data is an interactive process that involves a continuous agile approach to deliver timely and actionable work products to audits and investigations. The OIG is currently leveraging analytics in some audits to help identify and understand any trend analyses as well as red flags. Our general approach is to build a high level overview of the data, examine anything that looks like an outlier, and then use the data to identify potential issues. We procured several software tools in order to assist with our efforts and have other endeavors planned and underway.

The OIG continued to provide oversight even through the challenges of the Coronavirus (COVID-19), with OIG staff directed to telework at the conclusion of the reporting period. OIG staff continued the OIG's mission and operations. Important oversight work that was essential to the protection of life and property continued. Moreover, at the end of the reporting period, the OIG added a new Counsel to the IG, after the previous Counsel to the IG departed in January 2020 to become an IG himself. Because of the effects of COVID-19, the OIG is managing its workload from a shelter in place environment but is ably progressing on its mandates during this time of uncertainty.

In closing, I remain firmly committed to executing the OIG's mission of promoting the integrity, efficiency, and effectiveness of the SEC's programs and operations and to reporting our findings and recommendations to Congress and the Commission. We will continue to collaborate with SEC management to assist the agency in addressing the challenges it faces in its unique and important mission of protecting investors, maintaining fair, orderly, and efficient markets, and facilitating capital formation. I appreciate the significant support that the OIG has received from Congress and the agency. We look forward to continuing to work closely with the Commission and staff, as well as Congress, to accomplish our mission.



Carl W. Hoecker  
*Inspector General*



EQUAL JUSTICE UNDER LAW





# MANAGEMENT AND ADMINISTRATION

## AGENCY OVERVIEW

**T**he SEC's mission is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation. The SEC strives to promote capital markets that inspire public confidence and provide a diverse array of financial opportunities to retail and institutional investors, entrepreneurs, public companies, and other market participants. Its core values consist of integrity, excellence, accountability, teamwork, fairness, and effectiveness. The SEC's goals are "(1) focus on the long-term interests of our Main Street investors; (2) recognize significant developments and trends in our evolving capital markets and adjusting our efforts to ensure we are effectively allocating our resources; and (3) elevate the SEC's performance by enhancing our analytical capabilities and human capital development."

The SEC is responsible for overseeing the nation's securities markets and certain primary participants, including broker-dealers, investment companies, investment advisers, clearing agencies, transfer agents, credit rating agencies, and securities exchanges, as well as organizations such as the Financial Industry Regulatory Authority, Municipal Securities Rulemaking Board, and the Public Company Accounting Oversight Board. Under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), the agency's

jurisdiction was expanded to include certain participants in the derivatives markets, private fund advisers, and municipal advisors.

The SEC accomplishes its mission through 5 main divisions—Corporation Finance, Enforcement (ENF), Investment Management, Trading and Markets (TM), and Economic and Risk Analysis—and 25 functional offices. The SEC's headquarters are in Washington, DC, and the agency has 11 regional offices located throughout the country. As of March 2020, the SEC employed 4,406 full-time equivalent employees.

## OIG STAFFING, RESOURCES, AND ADMINISTRATION

During this semiannual reporting period, the OIG recruited to fill key vacancies integral to the management, audit, and investigative functions. We hired a supervisory attorney, one auditor, and two investigators. We also continued our efforts to meet our strategic goals of (1) delivering results that promote integrity, efficiency, and effectiveness in the SEC's programs and operations; (2) advancing an inclusive and dynamic OIG culture that inspires high performance; and (3) improving the effectiveness and efficiency of OIG processes through continuous innovation, collaboration, and communication.

## OIG OUTREACH

The IG regularly met with the Commissioners and senior officers from various SEC divisions and offices to foster open communication at all levels between the OIG and the agency. Through these efforts, the OIG kept up to date on significant, current matters that were relevant to the OIG's work. These regular communications also enabled the OIG to obtain agency management's input on what it believes are the areas presenting the greatest risks or challenges, facilitating the OIG's identification and planning for future work. The OIG continually strives to keep apprised of changes to agency programs and operations and keeps SEC management informed of the OIG's activities and concerns raised during its work.

The OIG also continued its efforts to educate SEC employees on the roles and responsibilities of the OIG. The OIG participated in the SEC's new employee orientation sessions and gave an overview of the OIG and its various functions. Additionally, the OIG continued to educate staff on and promote the OIG's SEC Employee Suggestion Program, to encourage suggestions for improvements in the SEC's work efficiency, effectiveness, and productivity, and the use of its resources. The OIG also participated on a panel discussion educating SEC employees on whistleblower retaliation and the role of the OIG with respect to whistleblower retaliation complaints.

OIG continued delivering its fraud awareness briefing program throughout the SEC. These briefings serve to educate SEC employees on the activities of the OIG as well as specific vulnerabilities in the programs they oversee. The briefings also enhance the OIG's "eyes and ears," with the goal of achieving more timely and complete reporting of possible fraud, waste and abuse in SEC programs and operations. Additionally, the OIG continued its collaboration with the SEC's Office of Financial Management and Office of Acquisitions (Acquisitions) to provide a fraud awareness training module during annual training for contracting officials.

Finally, OA supported the February 12, 2020, *Information Systems Audit and Control Association Greater Washington, DC Information Technology Audit in Civilian and Department of Defense Environments Conference*. Specifically, an audit manager gave a presentation on the SEC's challenges, successes, and lessons learned while building the OIG's information technology audit program.

## OIG ANNUAL AWARDS PROGRAM

The OIG held its annual awards ceremony on March 5, 2020, to honor service and outstanding achievements in 2019. The awardees were selected in various categories based on nominations submitted by their peers. The IG and special guests presented the awards at the ceremony.

The Length of Service awardees included:

- Carl W. Hoecker—40 years
- Ismael Serrano—20 years
- Ronald Wormsley—20 years
- Adelle Harris—15 years
- John Dettinger—10 years
- Steven Encomienda—10 years
- Leann Harrier—10 years

The 2019 Outstanding Achievement award recipients included:

- Ronald Wormsley—IG Award;
- Tawana Edwards—Office of Operations and Management Employee of the Year Award;
- Melissa Mulhollen—OA Employee of the Year Award;
- K. Shane Breffitt—OI Employee of the Year Award;
- Adelle Harris, Ronald Wormsley, Roberta Raftovich, and William Beach—Group Superior Accomplishment Award—Special Act or Service;
- Lori Wagner—Individual Superior Accomplishment Award—Special Act or Service; and
- Holley Miller, Bruce McLean, Adelle Harris, and Kelli Brown-Barnes—Special Joint Team Award.



## COORDINATION WITH OTHER AGENCIES

**D**uring this semiannual reporting period, the SEC OIG coordinated its activities with those of other agencies, pursuant to Section 4(a)(4) of the IG Act of 1978, as amended.

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

The SEC IG also attended meetings of the Council of the Inspectors General on Integrity and Efficiency (CIGIE). In addition, the OIG participated on a team to update CIGIE Quality Standards for Digital Forensics, which provide a framework for performing high-quality digital forensics in support of investigations conducted by an OIG. The OIG also participated in the CIGIE Undercover Review Committee, which provided recommendations and approvals on the suitability of undercover operations that involved sensitive circumstances that were carried out in accordance with DOJ guidelines. Additionally, we collaborated with the OIG community to assist DOJ in ensuring full reporting of required criminal history information to the National Instant Criminal Background Check System.

OA continued to participate in activities of various CIGIE Federal Audit Executive Council working groups, including the Audit Peer Review, DATA Act, and Information Technology Committee working groups. In addition, OA staff supported the activities of CIGIE's Inspections and Evaluation Peer Review working group. As necessary, OA

also supported requests for assistance from other OIGs. For example, OA assisted the Federal Deposit Insurance Corporation OIG in gathering information about hiring examiners and managing their workload. Finally, OA staff continued participating in the CIGIE Enterprise Risk Management working group. As part of this effort, the Deputy IG for Audits, Evaluations, and Special Projects chaired one of the working group's sub-groups. In January 2020, CIGIE ratified a document authored by the sub-group titled *Inspectors General Guide to Assessing Enterprise Risk Management*,

which provides guidance for audit and evaluation teams responsible for assessing their agency's Enterprise Risk Management programs.

The Counsel to the IG participated in the Employment Law Working Group of the Council of Counsels to the Inspectors General, and participated in the Small OIG Counsel Working Group. OIG staff also participated in the activities of the Deputy Inspectors General group and the OIG Freedom of Information Act Working Group.



# AUDITS AND EVALUATIONS

## OVERVIEW

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

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

OA conducts audits in compliance with generally accepted government auditing standards issued by the Comptroller General of the United States. OIG evaluations follow CIGIE's *Quality Standards for Inspection and Evaluation*. At the completion of an audit or evaluation, the OIG issues an independent report that identifies deficiencies and makes recommendations, as necessary, to correct those deficiencies or increase efficiencies in an SEC program or operation.

## COMPLETED AUDITS AND EVALUATIONS

### Audit of the SEC's Compliance With the Digital Accountability and Transparency Act for Fiscal Year 2019 (Report No. 557)

The DATA Act enables taxpayers and policymakers to track Federal spending more effectively. The DATA Act directs the Office of Management and Budget (OMB) and Treasury to establish government-wide financial data standards to ensure the reporting of reliable, consistent Federal spending data for public use. The DATA Act also requires the IG of each Federal agency to assess the completeness, accuracy, timeliness, and quality of their component agency's spending data and the agency's implementation and use of the data standards.

In accordance with the DATA Act and guidance (referred to as the IG Guide) promulgated by CIGIE's Federal Audit Executive Council, we conducted an audit of the SEC's compliance with the DATA Act with respect to the SEC's fiscal year (FY) 2019, first quarter (FY19Q1) data submitted to Treasury.

We found that the SEC's Office of Financial Management prepared and submitted the agency's FY19Q1 data in a timely manner and in accordance with the DATA Act. Moreover, the SEC appears to have properly designed and implemented controls that are operating effectively and are providing reasonable assurance that agency data extracted from source systems and agency reporting of transactional information is complete, accurate, and timely. We tested 46 data elements across all 134 detailed transactions included in the SEC's FY19Q1 submission to Treasury's DATA Act Broker. The resulting overall error rates were sufficiently low to conclude that the SEC has "higher" quality data as defined by the IG Guide. (Data quality could be "higher," "moderate," or "lower.")

We further determined that, of the 132 errors identified, only 12 were because of SEC actions. The remaining errors were linked to data extracted or derived from third-party systems. When we removed the errors attributable to third parties, the SEC's error rates for completeness, accuracy, and timeliness fell to 0 percent, 0.22 percent, and 0 percent, respectively.

We also evaluated the SEC's implementation and use of the government-wide financial data standards and determined that the SEC has fully implemented and used the data standards as required. Although we generally found the SEC's controls to be adequate and effective to ensure DATA Act compliance, the SEC can further improve its processes related to the DATA Act by (1) updating aspects of the Office of Financial Management's Reference Guide, and (2) verifying that the program activity codes, program activity names, and data elements in File B are correct before the SEC certifies and publishes File B to Treasury's DATA Act Broker. (Agencies submit to the Broker data in files known as File A, File B, and File C.)

We issued our final report on November 4, 2019, and made two recommendations to address areas for further improvement.

The report is available on our website at <https://www.sec.gov/files/Audit-of-the-SECs-Compliance-with-the-DATA-Act-for-FY-19-Report-No-557.pdf>.

### The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services (Report No. 556)

Beginning in December 2010, OMB—citing cloud computing benefits such as potential cost savings, ease in scalability, and procurement efficiencies—directed Federal agencies to default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. Since that time, GAO has issued multiple cloud computing reports, identifying issues such as the need for some Federal agencies to (1) pursue additional cloud opportunities and costs savings, (2) incorporate key performance practices, and (3) improve security.

We conducted this audit to assess the SEC's management of the planning, implementation, and security of its cloud computing services. Specifically, we sought to (1) assess the SEC's strategy for migrating information technology (IT) services and applications to the cloud, and (2) determine whether key security measures were in place to adequately protect SEC systems that use cloud computing services.

Consistent with Federal guidance, in 2017, the SEC developed a strategy that defined the goals and objectives of the agency's cloud program, and a plan that established cloud-related goals. However, we found that the SEC did not fully implement its cloud strategy; follow a clear, robust strategic plan to evaluate and prioritize IT services and applications for migration to the cloud; or effectively track

related goals. Instead, the agency used an “ad hoc” or “as-needed” approach to implementing cloud computing. This occurred because the SEC did not coordinate or collaborate on cloud strategies at an enterprise level. As a result, the SEC has not fully realized the potential performance and economic benefits attributed to cloud computing services.

In addition, we assessed the SEC’s key security measures for protecting agency systems that use cloud computing services. Although the SEC’s Office of Information Technology (OIT) developed an IT security program and other supporting security policies and procedures governing the agency’s systems, processes for protecting the SEC’s cloud-based systems need improvement. Specifically, we found that the SEC’s system security plans for its cloud-based systems in operation as of March 20, 2019, were missing cloud-specific security controls and enhancements; and that security assessment reports for the systems were incomplete.

These conditions occurred because OIT had not developed policies and procedures specific to cloud system security, or adequate processes to ensure compliance with Federal Risk and Authorization Management Program baseline controls and enhancements for which the agency is responsible. As a result, the SEC’s processes did not adequately ensure compliance, assess risk, identify issues, or mitigate vulnerabilities specific to the agency’s cloud-based systems.

We also identified four other matters of interest that did not warrant recommendations; however, we discussed the matters with agency management for their consideration. These matters involved security categories, reporting of cloud services, incident response processes, and inclusion of security requirements in cloud service contracts.

We noted that an open recommendation from prior OIG work should address the matter regarding the SEC’s cloud service contracts, and we encourage management to implement the previously agreed-to corrective action.

We issued our final report on November 7, 2019, and made three recommendations to improve the SEC’s planning, management, and implementation of cloud strategies, and the security of its cloud-based systems.

Because this report contains sensitive information, we are releasing a redacted version on our website at <https://www.sec.gov/files/SEC-Can-More-Strategically-and-Securely-Plan-Manage-and-Implement-Cloud-Computing-Service.pdf>.

#### Final Management Letter: Evaluation of the U.S. Securities and Exchange Commission’s Delinquent Filer Program

DFP’s mission is to encourage reporting companies delinquent in filing periodic reports to become and stay current with the reporting requirements of the Securities Exchange Act of 1934 (Exchange Act) and to take action against those who do not. According to ENF officials, since 2004, DFP has generated about 5,000 revocation orders and 2,200 trading suspensions related to delinquent filers. Moreover, ENF’s DFP employees worked through a backlog of about 2,000 delinquent filers and produce about 7 to 15 percent of all Commission actions each year.

To determine whether DFP’s processes and internal controls were operating effectively, we conducted interviews; reviewed applicable laws, rules, regulations, and policies and procedures; and examined supporting documents for a sample of delinquent filers. We also surveyed

ENF employees newly assigned to DFP. Generally, we found that DFP had adequate processes for identifying, tracking, and notifying delinquent filers and recommending related revocation orders and/or trading suspensions in accordance with applicable laws, rules, and regulations. Based on our testing, we also concluded that DFP adhered to its policies and procedures and maintained adequate documents to support its recommendations to the Commission. Finally, those employees who responded to our survey generally believed that they have received sufficient training and written guidance to fulfill their new DFP responsibilities. As a result, it appears that DFP is well-positioned to continue pursuing its mission.

Nonetheless, two issues came to our attention that warrant management action. First, among other potential changes, the Division of Corporation Finance is assessing its ability to take a more active role in identifying companies that become delinquent or are likely to be delinquent, which could precede, overlap, and possibly impact the work conducted by ENF and the Division of Corporation Finance's Office of Enforcement Liaison. Second, delegating certain authority related to the Exchange Act could improve the efficiency of DFP.

We issued our final management letter on December 17, 2019, and made two recommendations to improve DFP.

Because this evaluation contains sensitive information, we are releasing a redacted version on our website at <https://www.sec.gov/files/Final-Mgmt-Ltr-Eval-of-the-SECs-Delinquent-Filings-Program.pdf>.

### Fiscal Year 2019 Independent Evaluation of the SEC's Implementation of the Federal Information Security Modernization Act (Report No. 558)

The SEC OIG contracted with Kearney & Company, P.C. (Kearney) to conduct an independent evaluation of the SEC's information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires all Federal agencies to develop, document, and implement an agency-wide information security program to protect its information and information systems, including those provided or managed by another agency, contractor, or other source. Additionally, FISMA requires Federal agencies or a contracted independent external auditor to conduct an annual independent evaluation of its information security program and practices, as well as an assessment of its compliance with the requirements of FISMA.

Kearney conducted this independent evaluation of the SEC's information security program and practices in support of the SEC OIG in accordance with CIGIE's *Quality Standards for Inspection and Evaluation*. Kearney's evaluation included inquiries, observations, and inspection of SEC documents and records, as well as direct testing of controls.

Kearney reported that since FY 2018, the SEC's OIT had improved aspects of its information security program. Among other actions taken, OIT made progress in implementing information security policies and procedures to address security risks at the organizational level, creating an entity-wide Identity and Access Management strategy, enhancing its security awareness and training processes, continuing its efforts to enhance its continuous monitoring program, and improving its incident response capabilities.

Although the SEC has strengthened its program since the last FISMA evaluation, Kearney noted that the agency's information security program did not meet the FY 2019 IG FISMA Reporting Metrics' definition of "effective," which requires the simple majority of domains to be rated as Level 4: Managed and Measurable. Although the agency's program, as a whole, did not reach the level of an effective information security program, the SEC has shown significant improvements at the domain levels. The report, issued on December 18, 2019, includes nine new recommendations to strengthen the SEC's information security program.

Because this report contains sensitive information, we are releasing a redacted version on our website at <https://www.sec.gov/files/FY-2019-Independent-Evaluation-SEC-Implementation-of-the-FISMA-of-2014-Report-No-558.pdf>.

#### The SEC's Office of Broker-Dealer Finances Provides Effective Oversight, But Opportunities To Improve Efficiency Exist (Report No. 559)

The SEC prescribes broker-dealer net capital and risk assessment reporting requirements through various rules overseen by the TM's OBDF. The largest broker-dealer firms can apply for and use an alternative net capital calculation for computing capital, if approved. Additionally, over-the-counter derivatives dealers can apply for and use value-at-risk and other statistical models to calculate capital once approved. OBDF monitors approved firms' monthly, quarterly, and annual filings and meets regularly with the firms' senior risk management staff. As of January 2020, there were five approved alternative net capital broker-dealer firms and three approved over-the-counter derivatives dealers. There were also 280 broker-dealers subject to risk assessment and material affiliate requirements.

We conducted this evaluation to assess the efficiency and effectiveness of TM's OBDF. Specifically, we sought to determine whether OBDF (1) provides effective oversight of broker-dealer compliance with capital and risk reporting requirements, in accordance with applicable rules and guidance, and (2) ensures efficient use of government resources to help achieve organizational goals and objectives.

We found that OBDF effectively monitors broker-dealer compliance with net capital and risk assessment rules and reporting requirements. Specifically, OBDF's sub-offices support its mission, and each sub-office has written policies and procedures with detailed processes that align with the organization's oversight requirements. Based on our review and testing of each sub-office's key processes and controls for oversight activities, we found that OBDF's processes were effective for overseeing broker-dealer net capital and risk reporting.

However, clarifications are needed in OBDF's Office of Broker-Dealer Inspections sub-office to reflect current practices and requirements. Specifically, certain updates to the Office of Broker-Dealer Inspections' written policies and procedures could strengthen controls over the inspection program, thereby improving efficiency.

Finally, we obtained reasonable assurance of OBDF's efficient use of government resources, and we did not identify waste. However, we were unable to link OBDF's programs and resources to its goals and objectives because of the lack of a unified, office-wide strategy. Also, OBDF did not make use of strategic planning, and did not have a formal succession plan. TM has drafted a strategic plan that includes goals for OBDF but, according

to the TM Managing Executive, the final plan has been delayed because of the extensive rulemaking agenda. We reviewed TM's draft strategic plan and we discussed OBDF's strategic and succession planning with OBDF senior management who confirmed that, while there have been planning discussions, formal plans have not been established.

We issued our final report on February 26, 2020, and made three recommendations to address areas that can improve OBDF's oversight and efficiency, including recommendations to update its inspection policies and finalize needed rule updates and strategic plans.

Because this report contains sensitive information, we are releasing a redacted version on our website at <https://www.sec.gov/files/SECs-Office-of-Broker-Dealer-Finances-Provides-Effective-Oversight-but-opportunities.pdf>.

#### Controls Over the SEC's Travel Charge Card Program Could Be Strengthened To More Fully Comply With Requirements and Maximize Benefits (Report No. 560)

In FY 2018 and FY 2019 quarters 1-2 (FY19Q1-2), the SEC spent almost \$12 million on work-related temporary duty travel and transportation. About 72 percent of this amount (or more than \$8.6 million) was paid using a government travel charge card. Although annual government travel charge card expenses are immaterial to the SEC's financial statements, compliance with laws and regulations and efficient and effective stewardship of resources are important Federal internal control objectives.

The Travel and Transportation Reform Act of 1998 requires Federal employees to use their government travel charge cards for all payments of expenses for official government travel. Travel charge cards provide benefits to the agency such as improved

oversight of government spending, tax exemptions, and refunds based on sales volume. However, travel charge cards are susceptible to misuse, fraud, waste, and abuse. To prevent abuse of government charge cards, Congress enacted the Government Charge Card Abuse Prevention Act of 2012 (Charge Card Act), which requires, among other things, agencies to establish and maintain specific internal control activities. We conducted this audit to assess the SEC's controls over its travel charge card program during FY 2018 and FY19Q1-2, and to determine whether the agency complied with applicable laws, regulations, policies, and procedures.

The SEC established and maintained many of the internal control activities required by the Charge Card Act, or relied on alternate controls that were generally effective for addressing certain risks associated with government travel charge card programs. The SEC has controls in place related to recordkeeping, training, and establishing effective systems, techniques, and technologies to prevent or identify improper travel card purchases. However, the agency did not implement all travel card-related internal control objectives required by the Travel and Transportation Reform Act of 1998, the Charge Card Act, and the Federal Travel Regulation, or fully comply with certain standard minimum requirements established by OMB. Moreover, although some controls established in SEC policy conformed to higher-level requirements, the controls were either ineffectively designed or implemented. Specifically, we found that the SEC did not:

- Clearly and consistently, require employees to establish Individually Billed Accounts and use their government travel charge cards as the method of payment for all official travel expenses. As a result, we estimate that, in FY 2018, the SEC lost about \$3,200 in refunds associated with lodging expenses alone and accepted additional financial risk.

- Ensure that employees and authorizing officials minimized costs to the agency by (1) adequately supporting requests for premium-class air travel expenses claimed under the 14-hour rule; (2) providing justifications and support for claimed travel expenses; and (3) pursuing exemptions to state taxes, where available. We identified \$109,882 in unsupported travel costs and estimate that the SEC could have put \$121,573 to better use had the agency pursued available tax exemptions.
- Monitor sales refunds for accuracy and to ensure they were received. SEC officials were unaware that they had not received the agency's first quarter FY 2018 refund, totaling \$9,900.
- Enforce requirements for conducting alternative creditworthiness assessments before issuing or renewing restricted travel charge cards.
- Issue travel charge card payments directly to the travel card-issuing bank, as required, until July 2019.
- Immediately cancel all separated employees' Individually Billed Accounts.
- Ensure that employees timely submitted travel vouchers or paid account balances.

Finally, we identified an opportunity for potential cost savings through Tax Advantage Travel Card Accounts, available under the General Services Administration SmartPay 3 contract. If SEC employees had been able to use these accounts in FY 2018 and FY19Q1-2, the agency would have potentially avoided paying about \$406,760 in state lodging and rental car taxes.

We issued our final report on March 30, 2020, and made 15 recommendations, including that the SEC update out-of-date or conflicting policies, increase outreach efforts to make travelers and authorizing officials aware of their responsibilities and obligations, and consider cost savings opportunities.

The report is available on our website at <https://www.sec.gov/files/Controls-Over-the-SECs-Travel-Charge-Card-Program-Could-Be-Strengthened-Report-No-560.pdf>.

## OTHER PROJECTS AND REPORTS

### IG's Letter to OMB on the SEC's Implementation of Purchase Card Program Audit Recommendations

The Charge Card Act, Public Law 112-194, requires that IGs report to the Director of OMB on the implementation of recommendations made to the head of an executive agency to address findings of any analysis or audit of purchase card and convenience check transactions or programs. OMB's implementing guidance requires IGs to report to the Director of OMB 120 days after the end of each FY on agency progress in implementing such recommendations.

On December 19, 2019, the OIG reported to OMB that the OIG did not issue any reports regarding the SEC's government purchase card (GPC) program during FY 2019. Furthermore, before the end of FY 2019, the OIG closed all purchase card-related recommendations, which were to ensure cardholders comply with established requirements when using a GPC to purchase information and data sources and print materials.

The OIG's letter report is available on our website at <https://www.sec.gov/files/SEC-OIG-FY-2019-Ltr-to-OMB-on-Purchase-Card-Related-Audit-Recommendations.pdf>.

## Results of the Inspector General's Fiscal Year 2019 Purchase Card Program Risk Assessment

The Charge Card Act, as implemented by OMB Circular No. A-123, Appendix B, requires OIGs to conduct periodic assessments of agency purchase card or convenience check programs to identify and analyze the risks of illegal, improper, or erroneous purchases and payments. The risk assessments are used to determine the scope, frequency, and number of audits of purchase card or convenience check transactions.

On March 31, 2020, the OIG reported to the SEC Chairman on the results of its FY 2019 risk assessment of the SEC's GPC program. To conduct the risk assessment, we assessed agency compliance with the Charge Card Act's requirements and evaluated the SEC's GPC program against an established enterprise risk management framework. We also interviewed Acquisitions staff and reviewed applicable documents. Additionally, we considered the results of our periodic review of purchase card transactions. In FY 2019, the SEC GPC program had about 100 cardholders who made 2,991 transactions for a total of \$2,270,443. We used a data analytic software program to risk-rank transactions and, based on risk scoring, we selected a judgmental sample of 55 transactions to compare to supporting documentation.

We found that the SEC has set program objectives, identified risks to the GPC program, and established controls and monitoring protocols to address those risks. We agreed with the SEC's assessment of how its controls and monitoring protocols affect the likelihood the risks could occur and the impact those risks would have on the GPC program. Given the objectives and size of the GPC program and its materiality to the SEC, we found that the SEC's risk response appeared reasonable and sufficient. Furthermore, during prior reviews of the SEC's

GPC program, cardholders were sometimes unable to provide documentation demonstrating that employees attended GPC-paid external training events, as required by an SEC administrative regulation. During our review of the SEC's FY 2019 GPC transactions, we noted that, although cardholders did not maintain proof of attendance as part of their GPC documentation, they established a database to track training requests, payments, and proof of attendance as an alternative control.

However, we also observed that SEC personnel did not validate the accuracy of quarterly purchase card refunds received, as required by the Charge Card Act and agency policy. Therefore, the SEC may not have received the correct amount of refunds in FY 2019. The SEC's GPC team indicated that it is working with U.S. Bank to understand how to validate such refunds. We will reassess the agency's validation of purchase card refunds during our next risk assessment of the SEC's GPC program.

As a result of our risk assessment, we determined that the overall risk of material illegal, improper, or erroneous purchases and payments in the SEC's GPC program is low. As a result, we do not plan on conducting an audit of the program at this time.

The Charge Card Act also requires periodic audits or reviews of travel card programs for agencies with more than \$10 million in travel card spending, but does not require travel card program risk assessments. We determined that, in FY 2019, the SEC did not meet the \$10 million threshold, and we did not perform a travel card program risk assessment. However, we recently completed an audit of the SEC's travel card program (*Controls Over the SEC's Travel Charge Card Program Could Be Strengthened To More Fully Comply With Requirements and Maximize Benefits*, Report No. 560, issued on March 30, 2020).

The OIG's memorandum on the results of the FY 2019 GPC risk assessment is available on our website at <https://www.sec.gov/files/Results-of-the-IGs-FY-2019-Purchase-Card-Program-Risk-Assessment.pdf>.

## ONGOING AUDITS AND EVALUATIONS

### Audit of the U.S. Securities and Exchange Commission's Management of Mobile Devices and Services

SEC employees and contractors increasingly use smartphones and tablets (collectively referred to as mobile devices) to perform their work and access SEC information resources anywhere at any time. In November 2011, President Barack Obama issued an executive order on promoting efficient spending, which directed agencies to assess current device inventories and usage, and establish controls to ensure that agencies are not paying for unused or underused IT equipment, including mobile devices. Moreover, in May 2012, OMB published a digital computing strategy governing the purchase and management of mobile devices across the government. As part of the strategy, and to promote fiscal responsibility, OMB requires agencies to take an enterprise-wide approach for procuring and managing mobile devices and services. Without adequate controls to effectively monitor and control spending, agencies, including the SEC, risk paying for unused or underused mobile devices or services. Also, although mobile devices with computing capabilities offer greater workplace flexibility, they are susceptible to security compromise; vulnerable to theft, loss, and damage; and create challenges for ensuring the confidentiality, integrity, and availability of the information they access, store, and process. Therefore, mobile device programs with inadequate security controls may result in the compromise and/or unauthorized access of agency data, including but not limited to nonpublic or personally identifiable information (PII).

The OIG has initiated an audit to evaluate the SEC's management of mobile devices and services. Specifically, we will assess the SEC's controls for managing costs associated with SEC-issued mobile devices in FY 2019 and the first quarter of FY 2020; and efforts to safeguard SEC information accessed, stored, or processed on mobile devices with access to the agency's network in FY 2020.

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

### Evaluation of the U.S. Securities and Exchange Commission's Fiscal Year 2019 Compliance With the Improper Payments Elimination and Recovery Act of 2010

In general, an improper payment is any payment that (1) should not have been made or that was made in an incorrect amount; (2) was made to an ineligible recipient; (3) was for ineligible goods or services; or (4) was for goods or services not received. In addition, a payment is considered improper if it lacks sufficient documentation.

The Improper Payments Elimination and Recovery Act of 2010 (IPERA) (Public Law 111-204, 124 Stat. 2224 [2010]) requires executive branch agencies to annually review all programs and activities, identify those susceptible to significant improper payments, and submit to Congress an estimate of the annual amount of improper payments from the susceptible programs. Agencies must review their programs at least once every 3 years in accordance with OMB guidance. "Significant improper payments" is defined as gross annual improper payments (the total of overpayments plus underpayments) exceeding both 1.5 percent of program outlays and \$10 million of all program payments made during the FY reported, or \$100 million of improper payments regardless of percentage. IPERA also established additional agency requirements and that each agency IG will

annually determine whether his or her respective agency complied with those requirements.

The OIG has begun an evaluation of the SEC's compliance with the requirements of IPERA for FY 2019.

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

#### Audit of the U.S. Securities and Exchange Commission's Oversight of the Infrastructure Support Services Contractor Performance

On January 25, 2016, the SEC awarded a combination-type contract (time-and-materials and fixed-price), to SRA International Inc. (CSRA) to provide infrastructure support services (ISS) for all SEC divisions and offices, including regional offices. Specifically, the contract (hereafter referred to as "the ISS contract") called for CSRA to support the SEC's OIT in the following four task areas that comprise the SEC's IT program: (1) Enterprise Operations, (2) Enterprise Infrastructure, (3) Enterprise Architecture, and (4) Common Services. As of January 2020, the SEC's ISS contract was the agency's largest active contract.

The OIG has begun an audit of the SEC's oversight of CSRA's performance. The overall objective of this audit is to assess the SEC's oversight and monitoring of the ISS contractor's performance. Specifically, we will (1) determine whether the SEC developed and leveraged a quality assurance surveillance plan, service level agreements, contractor performance reports, or other methods to monitor and document CSRA's performance, address areas in need of improvement, and drive desired performance outcomes in accordance with the Federal Acquisition Regulation, OMB guidance, and SEC policy; (2) evaluate CSRA's submission of contract deliverables and the SEC's

use of those deliverables to assess the contractor's performance; and (3) assess the SEC's monitoring of the contractor's corrective action plans for known performance issues.

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

#### Evaluation of the U.S. Securities and Exchange Commission's Tips, Complaints, and Referrals Program

The SEC's mission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. In pursuing its mission, the SEC encourages the public to file complaints or submit tips of possible securities law violations, broker or firm misconduct, or any unfair practices in the securities industry that pose a risk of harm to investors (collectively referred to as tips, complaints, and referrals [TCR]). Each year, the SEC receives thousands of TCR from members of the public, including industry professionals and attorneys, as well as referrals from self-regulatory organizations and exchanges, foreign and domestic Federal and local agencies, and law enforcement and other entities.

The OIG has initiated an evaluation of the SEC's TCR program. The overall objective of this evaluation is to assess the SEC's management of the TCR program, including reviewing controls for collecting, triaging, and responding to credible allegations of violations of the Federal securities laws; safeguarding and maintaining TCR source materials, as required; and monitoring TCR program risks and trends.

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



# INVESTIGATIONS

## OVERVIEW

The OIG OI investigates allegations of criminal, civil, and administrative violations relating to SEC programs and operations.

The subject of an OIG investigation can be an SEC employee, contractor, consultant, or any person or entity involved in alleged wrongdoing affecting the agency. Substantiated allegations may result in criminal prosecutions, fines, civil penalties, administrative sanctions, or personnel actions.

OI conducts investigations in accordance with the CIGIE *Quality Standards for Investigations* and applicable guidelines issued by the U.S. Attorney General. OI continues to enhance its systems and processes to ensure investigations are conducted in an independent, fair, thorough, and timely manner.

Investigations require extensive collaboration with separate SEC OIG component offices, other SEC divisions and offices, and outside agencies, law enforcement agencies, as well as coordination with DOJ and other prosecutive agencies. During the course of investigations, OI may discover vulnerabilities and internal control deficiencies and

via Management Implication Reports, promptly report these issues to SEC management for corrective actions.

OI manages the OIG Hotline, which is available 24 hours a day, 7 days a week, to receive and process tips and complaints about fraud, waste, or abuse related to SEC programs and operations. The hotline allows individuals to report their allegations to the OIG directly and confidentially.

Staffed by Special Agents and an IT Specialist, the OIG's Digital Forensics and Investigations Unit performs digital forensic acquisitions, extractions, and examinations, in support of SEC OIG operations, and conducts network intrusion and exploitation investigations, as well as other investigations involving threats to the SEC's IT infrastructure.

## REPORT ON INSTANCES OF WHISTLEBLOWER RETALIATION

For this semiannual reporting period, the OIG found no instances of whistleblower retaliation to report.

## STATUS OF PREVIOUSLY REPORTED INVESTIGATIONS

### SEC Contractor Photographs Nonpublic Computer Screen Information

As reported in a previous semiannual report, the OIG initiated an investigation after receiving allegations that a contractor working in the Office of Support Operations (OSO) was observed taking pictures with a personal cellular phone of SEC information on a computer screen.

The OIG investigation determined that the contractor admitted taking occasional pictures of SEC information on a computer screen with the contractor's own personal cellular phone. The contractor explained that the computers sometimes displayed an error message, and the contractor would take a picture of the error message for SEC's OIT because it is easier to read the error message off the phone. The contractor denied taking pictures of nonpublic information. The investigation determined that the contractor had contacted the OIT help desk 47 times for various computer issues over a 3½-year period preceding the report. The OIG also determined that the relevant computers did not contain PII.

The OIG reported the results of the investigation to management to determine whether corrective administration action may be warranted. During this reporting period, management responded that the employee was directed to re-take the SEC's online Privacy and Information Security Awareness Training, reminded of employees' responsibility to protect PII, and was counseled to refrain from using personal devices to capture SEC data.

### Allegations of Fraud

As reported in a previous semiannual report, the OIG investigated an allegation that a copy of a contract award document was falsified. The document contained an inaccurate contract number, an unknown requisitions number, and what appeared to be a forged signature. The OIG identified a certified public accountant as the creator of the fraudulent document and learned that the U.S. Postal Inspection Service was also investigating the individual for allegations involving wire fraud related to an investment scheme.

This certified public accountant, who had been a partner at a Manhattan accounting firm, pleaded guilty to participating in two wire fraud schemes. In the first, he falsely claimed to have entered into multimillion-dollar intellectual property deals and defrauded investors out of \$2 million. In the second, he falsely claimed to have entered into client engagements and defrauded an employer out of more than \$270,000.

The certified public accountant established his own firm, which he allegedly told victims was a company specializing in assisting other entities in taking intellectual property to the market. He induced victims to invest in this firm by providing them with false documents showing the firm's involvement in multimillion-dollar transactions that would reap millions of dollars in future profits. Ultimately, the victims learned that the deals did not exist and that they were victims of an alleged scheme to defraud them out of millions of dollars.

After leaving the Manhattan accounting firm, the certified public accountant sought employment with a legal firm in Chicago, Illinois. He induced the Chicago legal firm to hire him and provide him with \$240,000 in draw payments based on false and fraudulent statements, including by sending the Chicago legal firm fraudulent contracts.

On June 24, 2019, the certified public accountant was charged with violating two counts of Title 18, U.S.C. §1343, Wire Fraud. During this reporting period (in January 2020), the certified public accountant was sentenced to 51 months imprisonment, 3 years supervised release, and ordered to pay restitution of \$936,246, forfeiture of the same amount, and a \$200 assessment fee.

## OPEN AND COMPLETED INVESTIGATIONS

### SEC Employee Impersonation and SEC Seal Fraud Scheme

The OIG initiated a preliminary investigation based on a referral from the SEC's Office of Investor Education and Advocacy regarding a fraud scheme that involved a letter containing the SEC's seal and an SEC employee's name. Specifically, the referral reported that the scheme's victim, a Canadian citizen, began communicating with a person purporting to be Richard Baros after meeting him online through social media. Between April and June 2019, the victim sent Baros about 50,000 Canadian dollars' worth of Bitcoin. When Baros subsequently offered to repay the funds, the victim received a letter that provided instructions to send more funds for penalties and taxes in order for the victim to receive repayment. The letter contained the SEC seal with an actual SEC employee's name

and was from a China-based law firm, which the investigation determined that firm did not author. The OIG also interviewed the SEC employee identified in the fraudulent letter, who stated that she did not author the letter and did not authorize the use of her information. After receiving the purported SEC letter, the victim did not send any additional funds and reported the issue to the SEC.

The OIG pursued the United States-based investigative leads, which did not result in identifying any of the fraudsters. Because the victim did not send any funds related to the purported SEC letter and there were no further United States-based investigative leads, the OIG closed its preliminary investigation.

### Unaccountable SEC Special Agent Badges

The OIG initiated an investigation after the discovery of three special agent badges in an SEC Headquarters basement storage area. The OIG determined that the badges originated from an order of 15 special agent badges placed by the OSO, Office of Security Services (OSS) in the year 2010. The badges were issued to some OSS personnel in the Personnel Security Office. Because of the lack of records, the OIG could not determine who authorized and placed the badge order. The OIG also found no evidence of any inventory control for the badges, nor any applicable policies or rationale for OSS obtaining and using badges with the SEC seal and the inscription "Special Agent."

During the course of the investigation, the OIG recovered four additional badges, including a badge from the OSO Director. In total, eight badges were not accounted for. Accordingly, the OIG sought the assistance of the Metropolitan Police

Department of the District of Columbia in entering the eight unaccounted badges as lost/missing law enforcement equipment in the National Crime Information Center database.

The OIG referred the results of the investigation to management to determine whether corrective administration action may be warranted. The OSO Director responded that OSS conducted its own review of the missing badges and uncovered no evidence of misuse. The OSO response also stated that it has been common practice for security organizations to issue badges and credentials to assist personnel in the performance of their routine duties.

#### SEC Employee Impersonation and SEC Seal Fraud Scheme

The OIG initiated a joint investigation with the U.S. Department of Homeland Security, Homeland Security Investigations and DOJ based on a referral from SEC's Office of Investor Education and Advocacy involving fake letters that included the SEC's seal and forged signatures of actual or fictitious SEC employees.

The investigation identified two fraud schemes whereby several individuals attempted to obtain money from investors. The schemes' participants were foreign nationals who resided outside of the U.S. and used fake letters to entice their victims to send money to (1) purchase what the victims believed to be legitimate investments, or (2) sell investments or recover losses incurred in the

purchase of those investments. The investigation identified more than 50 international victims who received letters soliciting funds as a part of the fraud schemes. The investigation also identified several domestic bank accounts owned by the foreign nationals and used as passthrough accounts in connection with the fraud scheme. As a result, Homeland Security Investigations seized funds of \$178,234.93 on deposit in these accounts.

On October 17, 2017, the matter was initially under consideration for prosecution by the U.S. Attorney's Office (USAO) for the Southern District of Florida, but was transferred to the USAO for the District of Columbia, and then the USAO for the Central District of California. On October 1, 2019, the USAO for the Central District of California ultimately declined prosecution of this matter because it lacked prosecutorial merit.

#### Disclosure of Nonpublic Investigative Information

The OIG initiated an investigation into allegations of disclosures of nonpublic information related to an ENF investigation. Specifically, ENF reported that on May 30, 2014, the *New York Times* published an article titled, "Investor, Bettor, Golfer: Insider Trading Inquiry Includes Mickelson, Icahn and William T. Walters." The article mentioned that the Federal Bureau of Investigation and SEC were conducting an investigation into "well-timed trades" of Clorox conducted by professional golfer Phil Mickelson, investor Carl Icahn, and professional gambler William Walters. On June

11, 2014, in a *New York Times* article titled, “Golfer Mickelson’s Role Said to Be Overstated in Insider Inquiry,” corrected the May 30, 2014, article and stated Mickelson “did not trade in the shares of Clorox.”

The OIG’s investigation determined that there were parallel civil and criminal investigations focused on Clorox trades. The OIG found that the nonpublic information referenced in the articles was the existence of the investigations of Clorox. However, the OIG found no evidence that any SEC employee improperly disclosed any nonpublic information included in the *New York Times* articles. Furthermore, a Federal Bureau of Investigation special agent who had access to nonpublic information about the investigations admitted to leaking information to the *New York Times*, which was referred to the DOJ OIG for investigation.

On December 15, 2016, the facts of the investigation concerning the Federal Bureau of Investigation agent’s actions were presented to the DOJ Criminal Division’s Public Integrity Section, which declined to prosecute on October 10, 2019.

### Whistleblower Misconduct and False Statements

The OIG initiated an investigation into an allegation that two individuals may have obstructed an SEC ENF proceeding. The first individual, who filed a Whistleblower Claim with the SEC, made false declarations in that claim regarding the first individual’s participation in the misconduct which

was reported. During ENF’s investigation, both individuals made misleading statements in an ENF interview. Additionally, the first individual contacted a witness’ father by telephone and attempted to have the father influence the witness’ future testimony.

This investigation revealed that the first individual appeared to have engaged in the same misconduct reported in the Whistleblower Claim. In that claim, the first individual reported that the second individual had purchased sensitive customer information for \$15,000. A review of witness interviews and evidence revealed that the first individual also appeared to have purchased sensitive customer information from the same seller. Also, the first individual appeared to have provided false testimony that stated that the first individual was unaware of other persons purchasing sensitive customer information, when the individual was apparently purchasing that information as well. Furthermore, the first individual telephoned the seller’s father, stated that the SEC was investigating them and did not want the seller to cooperate.

This investigation also revealed that the second individual appeared to have provided false testimony to ENF when the second individual stated that the second individual had not purchased sensitive customer information from other sellers. During interviews, both sellers admitted that they had sold customer data to the second individual for \$7,500 each.

On September 6, 2019, the matter was presented to the USAO, Southern District of New York, which declined prosecution on October 10, 2019. Before the OIG's investigation, the matter had been considered and declined for prosecution with the District Attorney's Office—New York County. On October 22, 2019, the OIG confirmed that the District Attorney's Office—New York County maintained its decision to decline this matter for prosecution.

#### SEC Manager Solicited and Accepted Gifts From Contractors

The OIG initiated an investigation into allegations that a Branch Chief solicited and accepted gifts from SEC contractors, and that when confronted by another supervisor about accepting gifts, the Branch Chief replied “their money spends green.”

At that time, other reported allegations were referred to SEC management for review and appropriate action. Subsequently, SEC management provided the OIG with information (determined during its inquiry) that the Branch Chief voluntarily admitted to soliciting and accepting gifts, including candy, cookies, and snacks.

The OIG's investigation confirmed the information that the Branch Chief provided to management. As such, the OIG referred this entire matter to SEC management for review. During SEC management's review, the Branch Chief separated from employment with the SEC.



## REVIEW OF LEGISLATION AND REGULATIONS

**D**uring this semiannual reporting period, the OIG reviewed and monitored the following legislation and regulations:

### Public Law 115-336, 21st Century Integrated Digital Experience Act

The act requires public-facing agency websites to have a consistent design and functionality. The websites will need to achieve compliance with standards developed by the Technology Transformation Service of the General Services Administration. The act requires that websites are usable by people with disabilities and are mobile-friendly.

### Public Law 115-414, Good Accounting Obligation in Government Act

The act requires each Federal agency, in its annual budget justification, to include a report on: (1) each public recommendation of GAO that is classified as “open” or “closed, unimplemented”; (2) each public recommendation for corrective action from the agency’s OIG for which no final action has been taken; and (3) the implementation status of each such recommendation. Each agency shall also provide a copy of this information to its OIG and to GAO.

### Public Law 116-6, Consolidated Appropriations Act, 2019

This act provides appropriations for the SEC under the Financial Services and General Government Appropriations Act of 2019. The act provides \$1,674,902,000, to remain available until expended, of which not less than \$15,206,000 shall be for the OIG. Section 629 provides that none of the funds made available by this act shall be used by the SEC to finalize, issue, or implement any rule, regulation, or order regarding the disclosure of political contributions, contributions to tax exempt organizations, or dues paid to trade associations.

### Public Law 116-92, National Defense Authorization Act for Fiscal Year 2020

Section 1710 creates a new semiannual reporting requirement by amending Section 5(a)(19) of the IG Act. When reporting on substantiated misconduct investigations involving senior government employees, OIGs are now required to include “the name of the senior government official (as defined by the department or agency) if already made public by the Office.” Section 6711, a technical correction, amends the “Enhanced Personnel Security Program” to allow covered IGs to conduct a

“review” (instead of the currently required “audit”) of agency security clearance review practices (5 United States Code [U.S.C.] 11001). Section 5332 creates an “External Review Panel” for claims of whistleblower reprisals affecting security clearances under 50 U.S.C. 3234 (relating to Intelligence Community elements) or 50 U.S.C. 3341(j) (relating to agencies under 5 U.S.C. 105).

#### Public Law 116-93, Consolidated Appropriations Act, 2020

This act provides appropriations for the SEC under the Financial Services and General Government Appropriations Act of 2019. The act provides \$1,815,000,000, to remain available until expended, of which not less than \$15,662,000 shall be for the OIG. Section 530 requires that within 1 year of the enactment of this act, the SEC shall submit to the Committees on Appropriations of the House of Representatives and the Senate, the Committee on Financial Services of the House of Representatives, and the Committee on Banking, Housing, and Urban Affairs of the Senate, a report concerning the Municipal Securities Rulemaking Board. Section 626 establishes that no funds provided in this act shall be used to deny an IG funded under this act timely access to any records, documents, or other materials available to the department or agency over which that IG has responsibilities under the IG Act, or to prevent or impede that IG’s access to such records, documents, or other materials, under any provision of law, except a provision of law that expressly refers to the IG and expressly limits the IG’s right of access. Each IG covered by this section shall report to the Committees on Appropriations of the House of Representatives and the Senate within 5 calendar

days any failures to comply with this requirement. Section 634 of the act prohibits funds made available by this to be used by the SEC to finalize, issue, or implement any rule, regulation, or order regarding the disclosure of political contributions, contributions to tax exempt organizations, or dues paid to trade associations.

#### Public Law 116-94, Further Consolidated Appropriations Act, 2020

This act makes further consolidated appropriations for the FY ending September 30, 2020, and for other purposes. Section 171 requires a briefing on the impact of Cryptocurrencies on United States Sanctions. Not later than 180 days after the date of the enactment of this act, the Secretary of State and the Secretary of Treasury, after consultation with the Chairman of the SEC and the Chairman of the Commodity Futures Trading Commission, shall develop a methodology to assess how any digital currency, digital coin, or digital token, that was issued by, for, or on behalf of the Nicolás Maduro regime is being used to circumvent or undermine United States sanctions. Not later than 180 days after the date of the enactment of this act, the Secretary of State and the Secretary of Treasury shall brief the appropriate congressional committees on the methodology developed under subsection (b).

#### Public Law 116-117, Payment Integrity Information Act of 2019

The act reorganizes and revises existing improper payments statutes, which establish requirements for Federal agencies to cut down on improper payments. Additionally, the act establishes an interagency working group on payment integrity.

#### Public Law 116-136, CARES Act

Section 3 of this law exempts the budgetary effects of this act from the Pay-As-You-Go scorecards maintained under the Statutory Pay-As-You-Go Act of 2010 or by the Senate under the FY 2018 congressional budget resolution. Section 15010 requires that a Pandemic Response Accountability Committee be established within CIGIE. The Pandemic Response Accountability Committee is established to (1) prevent and detect fraud, waste, abuse, and mismanagement; and (2) mitigate major risks that cut across program and agency boundaries. Much of the legislative text is similar to that which established the Recovery Accountability Transparency Board in 2009.

#### H.R. 736, Access to Congressionally Mandated Reports Act

To require the Director of the Government Publishing Office to establish and maintain an online portal accessible to the public that allows the public to obtain electronic copies of all congressionally mandated reports in one place, and for other purposes.

#### H.R. 4382, Integrity Committee Transparency Act of 2019

To amend the IG Act to require CIGIE to include additional information in requests and reports to Congress, to make information available to Congress regarding allegations closed without referral, to expand the membership of CIGIE, and for other purposes.

#### S. 2220, Open and Responsive Government Act of 2019

A bill to modify the exemption for trade secrets and commercial or financial information in the Freedom of Information Act, and for other purposes.



# MANAGEMENT DECISIONS

## STATUS OF RECOMMENDATIONS WITH NO MANAGEMENT DECISIONS

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

## REVISED MANAGEMENT DECISIONS

Management initially did not sustain the questioned and unsupported costs associated with OIG Audit Report No. 554 as disallowed. However, based on further discussions, we understand that management is reviewing these costs to determine whether some or all of these questioned and unsupported costs should in fact be characterized as disallowed. Discussions between management and OIG on this issue are ongoing.

## AGREEMENT WITH SIGNIFICANT MANAGEMENT DECISIONS

OIG agrees with all significant management decisions regarding audit and evaluation recommendations.

## REPORTS FOR WHICH NO AGENCY COMMENT WAS RETURNED WITHIN 60 DAYS

There were no audit or evaluation reports issued before the beginning of this reporting period for which no agency comment was returned within 60 days of providing the report to the agency.

## INSTANCES WHERE THE AGENCY UNREASONABLY REFUSED OR FAILED TO PROVIDE INFORMATION TO THE OIG OR ATTEMPTED TO INTERFERE WITH OIG INDEPENDENCE

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

# TABLES

Table 1. List of Reports: Audits and Evaluations

Financial Management	
11/4/2019	Audit of the SEC's Compliance With the Digital Accountability and Transparency Act for Fiscal Year 2019
557	
Information Security	
11/7/2019	The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services
556	
Regulatory Oversight	
12/17/2019	Final Management Letter: Evaluation of the U.S. Securities and Exchange Commission's Delinquent Filings Program
N/A	
Information Security	
12/18/2019	Fiscal Year 2019 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014
558	
Regulatory Oversight	
2/26/2020	The SEC's Office of Broker-Dealer Finances Provides Effective Oversight, But Opportunities To Improve Efficiency Exist
559	
Financial Management	
3/30/2020	Controls Over the SEC's Travel Charge Card Program Could Be Strengthened To More Fully Comply With Requirements and Maximize Benefits
560	

Table 2. Reports Issued With Questioned Costs or Recommendations That Funds Be Put to Better Use (Including Disallowed Costs)

Description	Number of Reports	Total		
		Questioned Costs	Unsupported Costs	Recommended Funds Put to Better Use
Reports for which no management decision had been made by the start of the reporting period (Report No. 554)	1	\$42,801	\$2,977,379	\$0
Reports issued during the reporting period (Report No. 560)	1	\$209	\$109,882	\$124,773
<b>Totals</b>	<b>2</b>	<b>\$43,010</b>	<b>\$3,087,261</b>	<b>\$124,773</b>

Management initially did not sustain the questioned and unsupported costs associated with OIG Audit Report No. 554 as disallowed. However, based on further discussions, we understand that management is reviewing these costs to determine whether some or all of these questioned and unsupported costs should in fact be characterized as disallowed. Discussions between management and OIG on this issue are ongoing.

The term “questioned cost” means a cost that is questioned because of (A) an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds; (B) a finding that, at the time of the audit, such cost is not supported by adequate documentation; or (C) a finding that the expenditure of funds for the intended purpose is unnecessary or unreasonable.

The term “unsupported cost” means a cost that is questioned because the Office found that, at the time of the audit, such cost is not supported by adequate documentation.

The term “disallowed cost” means a questioned cost that management, in a management decision, has sustained or agreed should not be charged to the government.

The term “recommendation that funds be put to better use” means a recommendation that funds could be used more efficiently if management took actions to implement and complete the recommendation, including (A) reductions in outlays; (B) deobligation of funds from programs or operations; (C) withdrawal of interest subsidy costs on loans or loan guarantees, insurance, or bonds; (D) costs not incurred by implementing recommended improvements related to the operations of the establishment, a contractor or grantee; (E) avoidance of unnecessary expenditures noted in pre-award reviews of contract or grant agreements; or (F) any other savings which are specifically identified. Consistent with Section 5 of the IG Act, as amended, dollar amounts shown in this category reflect the dollar value of recommendations that funds be put to better use by management.

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

During this most recent semiannual reporting period, SEC management provided the OIG with documentation to support the implementation of OIG recommendations. In response, the OIG closed 13 recommendations related to 6 OA reports. The following table lists recommendations issued before the commencement of this semiannual reporting period that remain open. (“Redacted text” indicates recommendations that include one or more redactions of nonpublic information.)

Report Number and Title	Rec. No.	Issue Date	Recommendation Summary
546–Audit of the SEC’s Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017	1	3/30/2018	Redacted Text
546–Audit of the SEC’s Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017	3	3/30/2018	Redacted Text
546–Audit of the SEC’s Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017	5	3/30/2018	(a) Continue efforts to define and formalize a plan addressing how enterprise architecture program management will be integrated with other institutional management disciplines, such as organizational strategic planning, strategic human capital management, performance management, information security management, and capital planning and investment control; and (b) define and implement a process to ensure information technology initiatives undergo an enterprise architecture compliance review before funding.
546–Audit of the SEC’s Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017	7	3/30/2018	Improve the agency’s acquisition of information systems, system components, and information system services by coordinating with Acquisitions to (a) identify, review, and modify as necessary the agency’s existing information technology contracts (including those we reviewed) to ensure the contracts include specific contracting language, such as information security and privacy requirements, material disclosures, Federal Acquisition Regulation clauses, and clauses on protection, detection, and reporting of information; and (b) define and implement a process to ensure that future acquisitions of information technology services and products include such provisions.
546–Audit of the SEC’s Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017	8	3/30/2018	Redacted Text

Table 3. Reports With Recommendations on Which Corrective Action Has Not Been Completed (*Continued*)

Report Number and Title	Rec. No.	Issue Date	Recommendation Summary
546–Audit of the SEC’s Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017	9	3/30/2018	Redacted Text
546–Audit of the SEC’s Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017	12	3/30/2018	Redacted Text
546–Audit of the SEC’s Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017	15	3/30/2018	Develop and implement a process to ensure that all individuals with significant security responsibilities receive required specialized training before gaining access to information systems or before performing assigned duties.
546–Audit of the SEC’s Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017	16	3/30/2018	Update the existing continuous monitoring strategy to define (a) qualitative and quantitative performance measures or data that should be collected to assess the effectiveness of the agency’s continuous monitoring program; (b) procedures for reviewing and modifying all aspects of the agency’s continuous monitoring strategy; and (c) the agency’s ongoing authorization process.
546–Audit of the SEC’s Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017	17	3/30/2018	Review and update incident response plans, policies, procedures, and strategies to (a) address all common threat and attack vectors and the characteristics of each particular situation; (b) identify and define performance metrics that will be used to measure and track the effectiveness of the agency’s incident response program; (c) develop and implement a process to ensure that incident response personnel obtain data supporting the incident response metrics accurately, consistently, and in a reproducible format; (d) define incident response communication protocols and incident handlers’ training requirements; and (e) remove outdated terminology and references.
547–Audit of the SEC’s Internal Controls for Retaining External Experts and Foreign Counsel for the Division of Enforcement	7	6/15/2018	Develop a process that ensures contracting officers enforce contract requirements related to PII, when necessary, for any new contracts for expert services.

Table 3. Reports With Recommendations on Which Corrective Action Has Not Been Completed (*Continued*)

Report Number and Title	Rec. No.	Issue Date	Recommendation Summary
549–The SEC Made Progress But Work Remains To Address Human Capital Management Challenges and Align With the Human Capital Framework	2	9/11/2018	Finalize standard operating procedures for the agency’s performance management program.
550–Evaluation of the EDGAR System’s Governance and Incident Handling Processes	5	9/21/2018	Redacted Text
550–Evaluation of the EDGAR System’s Governance and Incident Handling Processes	14	9/21/2018	Redacted Text
552–Fiscal Year 2018 Independent Evaluation of SEC’s Implementation of the Federal Information Security Modernization Act of 2014	1	12/17/2018	Redacted Text
552–Fiscal Year 2018 Independent Evaluation of SEC’s Implementation of the Federal Information Security Modernization Act of 2014	2	12/17/2018	Redacted Text
552–Fiscal Year 2018 Independent Evaluation of SEC’s Implementation of the Federal Information Security Modernization Act of 2014	3	12/17/2018	Redacted Text
552–Fiscal Year 2018 Independent Evaluation of SEC’s Implementation of the Federal Information Security Modernization Act of 2014	4	12/17/2018	Redacted Text

Table 3. Reports With Recommendations on Which Corrective Action Has Not Been Completed (*Continued*)

Report Number and Title	Rec. No.	Issue Date	Recommendation Summary
552-Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014	5	12/17/2018	Redacted Text
552-Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014	6	12/17/2018	Define and implement a control to detect instances where contractor personnel received network accounts but were not assigned privacy and information security awareness training, nor tracked within system reporting tools.
552-Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014	7	12/17/2018	Redacted Text
552-Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014	8	12/17/2018	Redacted Text
552-Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014	9	12/17/2018	Redacted Text
553-Although Highly Valued by End Users, DERA Could Improve Its Analytics Support by Formally Measuring Impact, Where Possible	3	4/29/2019	Incorporate the results of analytics impact measurements in the Division of Economic and Risk Analysis' outreach efforts.
555-The SEC Has Processes to Manage Information Technology Investments But Improvements Are Needed	1	9/19/2019	Update capital planning and investment control policies and procedures and implement processes for selecting, managing, and evaluating steady state investments in accordance with the Clinger-Cohen Act of 1996 and with applicable OMB circulars and other guidance.

Table 3. Reports With Recommendations on Which Corrective Action Has Not Been Completed (*Continued*)

Report Number and Title	Rec. No.	Issue Date	Recommendation Summary
555-The SEC Has Processes To Manage Information Technology Investments But Improvements Are Needed	2	9/19/2019	Ensure capital planning and investment control policies meet the intent of OMB guidance on information technology investment baseline management policies.
555-The SEC Has Processes To Manage Information Technology Investments But Improvements Are Needed	3	9/19/2019	Provide training to personnel with investment oversight and program management responsibilities that, at a minimum, addresses the SEC's information technology investment baseline management policies and procedures.
555-The SEC Has Processes To Manage Information Technology Investments But Improvements Are Needed	4	9/19/2019	Update capital planning and investment control policies and procedures and implement processes to (a) establish a uniform refresh plan or a strategic approach for the replacement of hardware assets, and document performance against planned cost, quantities, and type of hardware assets to be replaced annually; and (b) monitor investments in hardware asset purchases beyond receipt of the assets to ensure the assets are efficiently and effectively deployed and the investments achieve expected outcomes or goals and provide requested capabilities.

Table 4. Summary of Investigative Activity for the Reporting Period of October 1, 2019, to March 31, 2020

The data contained in this table was compiled from the OIG’s investigations case management system.

Investigative Caseload	Number
Cases Open at Beginning of Period	36
Cases Completed but Not Closed* at Beginning of Period	1
Cases Opened During Period	26
Cases Closed During Period	8
Cases Completed but Not Closed at End of Period	2
Open Cases at End of Period	53
Investigative Reports Issued During the Reporting Period	6

\* A case is “completed” but not “closed” when the investigative work has been performed but disposition (such as corrective administrative action) is pending.

Criminal and Civil Investigative Activities	Number
Referrals for Criminal Prosecution to DOJ	11
Accepted	2
Indictments/Informations	2
Arrests	2
Convictions	1
Referrals for Criminal Prosecution to State and Local Prosecuting Authorities	0
Referrals for Civil Prosecution to DOJ	0
Accepted	0
Referrals for Civil Prosecution to State and Local Prosecuting Authorities	0

Table 4. Summary of Investigative Activity for the Reporting Period of October 1, 2019, to March 31, 2020 (Continued)

Monetary Results	Number
Criminal Fines/Restitutions/Recoveries/Assessments/Forfeitures	\$2,157,092
Criminal Seizures	\$0
Civil Fines/Restitutions/Recoveries/Penalties/Damages/Forfeitures	\$0

  

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

  

Complaints Received	Number
Hotline Complaints	131
Other Complaints	193
Total Complaints During Period	324

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

Section	Inspector General Act Reporting Requirement	Page(s)
4(a)(2)	Review of Legislation and Regulations	25-27
5(a)(1)	Significant Problems, Abuses, and Deficiencies	9-17, 19-24
5(a)(2)	Recommendations for Corrective Action	9-17
5(a)(3)	Prior Recommendations Not Yet Implemented	32-36
5(a)(4)	Matters Referred to Prosecutive Authorities	19-24, 37-38
5(a)(5)	Summary of Instances Where the Agency Unreasonably Refused or Failed to Provide Information to the OIG	29
5(a)(6)	List of OIG Audit and Evaluation Reports Issued During the Period	30
5(a)(7)	Summary of Significant Reports Issued During the Period	9-17, 19-24
5(a)(8)	Statistical Table on Management Decisions With Respect to Questioned Costs	31
5(a)(9)	Statistical Table on Management Decisions on Recommendations That Funds Be Put to Better Use	31
5(a)(10)(A)	Summary of Each Audit, Inspection or Evaluation Report More Than 6 Months Old for Which No Management Decision Has Been Made	29
5(a)(10)(B)	Summary of Each Audit, Inspection or Evaluation Report More Than 6 Months Old for Which No Establishment Comment Was Returned Within 60 Days of Providing the Report to the Establishment	29
5(a)(10)(C)	Summary of Each Audit, Inspection or Evaluation Report More Than 6 Months Old for Which There Are Any Outstanding Unimplemented Recommendations, Including the Aggregate Potential Cost Savings of Those Recommendations	29
5(a)(11)	Significant Revised Management Decisions	29
5(a)(12)	Significant Management Decisions With Which the Inspector General Disagreed	29
5(a)(14)(B)	Date of the Last Peer Review Conducted by Another OIG	41
5(a)(16)	Peer Reviews Conducted by Another OIG	41
5(a)(17)(A)	Statistical Table Showing the Total Number of Investigative Reports Issued During the Reporting Period	37-38
5(a)(17)(B)	Statistical Table Showing the Total Number of Persons Referred to DOJ for Criminal Prosecution During the Reporting Period	37-38

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

Section	Inspector General Act Reporting Requirement	Page(s)
5(a)(17)(C)	Statistical Table Showing the Total Number of Persons Referred to State and Local Prosecuting Authorities for Criminal Prosecution During the Reporting Period	37-38
5(a)(17)(D)	Statistical Table Showing the Total Number of Indictments and Criminal Informations During the Reporting Period That Resulted From Any Prior Referral to Prosecuting Authorities	37-38
5(a)(18)	Description of the Metrics Used for Developing the Data for the Statistical Tables Under 5(a)(17)	37-38
5(a)(19)	Report on Each Investigation Conducted Involving a Senior Government Employee Where Allegations of Misconduct Were Substantiated	19-24
5(a)(20)	Instances of Whistleblower Retaliation	19
5(a)(21)	Attempts by the Establishment To Interfere With the Independence of the OIG	29
5(a)(22)(A)	Each Inspection, Evaluation, and Audit Conducted by the OIG That Is Closed and Was Not Disclosed to the Public	N/A
5(a)(22)(B)	Each Investigation Conducted by the OIG Involving a Senior Government Employee That Is Closed and Was Not Disclosed to the Public	N/A

# PEER REVIEWS OF OIG OPERATIONS

## PEER REVIEW OF THE SEC OIG'S AUDIT OPERATIONS

In accordance with generally accepted government auditing standards and CIGIE quality control and assurance standards, an OIG audit team assesses another OIG's audit function every 3 years. The Legal Services Corporation OIG conducted the most recent assessment of the SEC OIG OA's system of quality control for the 3-year period ending March 31, 2018. The review focused on whether the SEC OIG established and complied with a system of quality control that was suitably designed to provide the SEC OIG with a reasonable assurance of conforming to applicable professional standards.

On September 5, 2018, the Legal Services Corporation OIG issued its report, concluding that the SEC OIG complied with its system of quality control and that the system was suitably designed to provide the SEC OIG with reasonable assurance of performing and reporting in conformity with applicable government auditing standards in all material respects. On the basis of its review, the Legal Services Corporation OIG gave the SEC OIG a peer review rating of "pass." (Federal audit organizations can receive a rating of "pass," "pass with deficiencies," or "fail.")

The peer review report is available on the SEC OIG website at <https://www.sec.gov/files/External-Peer-Review-Report-for-the-SEC-OIG-Audit-Org.pdf>. The next peer review of the OIG's audit function is scheduled for FY 2021.

## PEER REVIEW OF THE SEC OIG'S INVESTIGATIVE OPERATIONS

The Investigative Operations did not undergo a peer review this reporting period. The most recent peer review was performed by the National Science Foundation (NSF) OIG in November 2017. The NSF OIG conducted its review in conformity with the *Quality Standards for Investigations* and the *Quality Assessment Review Guidelines for Investigative Operations of Federal Offices of Inspector General* established by CIGIE and the *Attorney General Guidelines for Offices of Inspectors General With Statutory Law Enforcement Authority*.

The NSF OIG concluded that the SEC OIG was in compliance with the quality standards established by CIGIE and other applicable guidelines and statutes listed above. Furthermore, the NSF OIG concluded the SEC OIG's system of internal policies and procedures provide reasonable assurance that the SEC OIG is conforming with professional standards in the planning, execution, and reporting of its investigations.

# OIG GENERAL OFFICE CONTACT INFORMATION

**PHONE:** (202) 551-6061

**FAX:** (202) 772-9265

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

## REPORT FRAUD, WASTE, OR ABUSE

To report suspected fraud, waste, or abuse in SEC programs or operations, as well as SEC staff or contractor misconduct, use our online OIG hotline complaint form, [https://sec.govcomhotline.com](https://sec.govcom hotline.com), or call (833) 732-6441. This number is answered 24 hours, 7 days a week.

Information received through the hotline is held in confidence upon request. Although the OIG encourages complainants to provide information on how we may contact them for additional information, we also accept anonymous complaints.

## EMPLOYEE SUGGESTION PROGRAM

The OIG SEC Employee Suggestion Program, established under Dodd-Frank, welcomes suggestions by all SEC employees for improvements in the SEC's work efficiency, effectiveness, productivity, and use of resources. The OIG evaluates all suggestions received and forwards them to agency management for implementation, as appropriate. SEC employees may submit suggestions by calling (202) 551-6062 or sending an e-mail to [OIGESProgram@sec.gov](mailto:OIGESProgram@sec.gov).

## COMMENTS AND IDEAS

The SEC OIG also seeks ideas for possible future audits, evaluations, or reviews. We will focus on high-risk programs, operations, and areas where substantial economies and efficiencies can be achieved. Please send your input to [AUDPlanning@sec.gov](mailto:AUDPlanning@sec.gov).





This report is available on the Inspector General's website  
[www.sec.gov/oig](http://www.sec.gov/oig)