



OFFICE OF  
INSPECTOR GENERAL

UNITED STATES  
**SECURITIES AND EXCHANGE COMMISSION**  
WASHINGTON, D.C. 20549

**M E M O R A N D U M**

October 5, 2018

**TO:** Jay Clayton, Chairman

**FROM:** Carl W. Hoecker, Inspector General 

**SUBJECT:** *The Inspector General's Statement on the SEC's Management and Performance Challenges, October 2018*

The Reports Consolidation Act of 2000 requires the U.S. Securities and Exchange Commission's (SEC or agency) Office of Inspector General to identify and report annually on the most serious management and performance challenges facing the SEC.<sup>1</sup> In deciding whether to identify an issue as a challenge, we consider its significance in relation to the SEC's mission; its susceptibility to fraud, waste, and abuse; and the SEC's progress in addressing the challenge. We compiled this statement on the basis of our past and ongoing audit, evaluation, investigation, and review work; our knowledge of the SEC's programs and operations; and information from the U.S. Government Accountability Office and SEC management and staff. We reviewed the agency's response to the prior year's statement and efforts to address prior recommendations for improvement in areas of concern. We also provided a draft of this statement to SEC officials and considered all comments received when finalizing the statement. As we begin fiscal year 2019, we have again identified the following as areas where the SEC faces management and performance challenges to varying degrees:

- Meeting Regulatory Oversight Responsibilities
- Ensuring an Effective Information Security Program
- Improving Contract Management
- Ensuring Effective Human Capital Management

The challenges and corresponding audit, evaluation, investigation, or review work are discussed in the attachment. If you have any questions, please contact Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects.

Attachment

cc: Lucas Moskowitz, Chief of Staff, Office of Chairman Clayton  
Sean Memon, Deputy Chief of Staff, Office of Chairman Clayton  
Peter Uhlmann, Managing Executive, Office of Chairman Clayton

---

<sup>1</sup> Pub. L. No. 106-531, § 3a, 114 Stat. 2537-38 (2000).

Kara M. Stein, Commissioner  
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein  
Robert J. Jackson Jr, Commissioner  
Caroline Crenshaw, Counsel, Office of Commissioner Jackson  
Prashant Yerramalli, Counsel, Office of Commissioner Jackson  
Hester M. Peirce, Commissioner  
Jonathan Carr, Counsel, Office of Commissioner Peirce  
Elad Roisman, Commissioner  
Christina Thomas, Counsel, Office of Commissioner Roisman  
Robert B. Stebbins, General Counsel  
Rick Fleming, Investor Advocate  
John J. Nester, Director, Office of Public Affairs  
Bryan Wood, Director, Office of Legislative and Intergovernmental Affairs  
Stephanie Avakian, Co-Director, Division of Enforcement  
Steven Peikin, Co-Director, Division of Enforcement  
Peter Driscoll, Director, Office of Compliance Inspections and Examinations  
Kenneth Johnson, Chief Operating Officer  
Vance Cathell, Director, Office of Acquisitions  
Charles Riddle, Acting Chief Information Officer, Office of Information Technology  
Jamey McNamara, Acting Chief Human Capital Officer, Office of Human Resources  
Julie Erhardt, Acting Chief Risk Officer, Office of the Chief Operating Officer

## **Attachment. THE INSPECTOR GENERAL'S STATEMENT ON THE SEC'S MANAGEMENT AND PERFORMANCE CHALLENGES, OCTOBER 2018**

### ***CHALLENGE: Meeting Regulatory Oversight Responsibilities***

#### ***Impacts of Changing Markets, Increasing Responsibilities, and Other Developments.***

The U.S. Securities and Exchange Commission (SEC, agency, or Commission) is charged with overseeing more than 26,000 registered market participants, including investment advisers, mutual funds, exchange-traded funds, broker-dealers, municipal advisors, and transfer agents. The agency also oversees 21 national securities exchanges, 10 credit rating agencies, and 7 active registered clearing agencies, as well as the Public Company Accounting Oversight Board, Financial Industry Regulatory Authority, Municipal Securities Rulemaking Board, the Securities Investor Protection Corporation, and the Financial Accounting Standards Board. In addition, the SEC is responsible for selectively reviewing the disclosures and financial statements of more than 8,000 reporting companies.

As in previous years, agency management and the Office of Inspector General (OIG) recognize that, as markets evolve, so must the SEC. According to the agency's Fiscal Year (FY) 2019 Congressional Budget Justification and Annual Performance Plan,<sup>2</sup> in the last 5 years, the number of registered advisers has grown by more than 15 percent and the assets under management of these firms has increased by more than 40 percent. In addition, both the scope and number of clearing agencies required to be examined by the SEC have grown, and the registration of municipal advisors has added responsibility for hundreds of additional registrants with increasingly complex business lines. At the same time, there has been rapid growth in distributed ledger (i.e., blockchain) technologies and in the cryptocurrency markets, and the SEC has reported that cyber threats in securities markets have continued to increase in both frequency and sophistication. The FY 2019 Congressional Budget Justification and Annual Performance Plan states that, "These types of industry developments and financial innovation will continue to present challenges to the staff, requiring additional staff expertise, resources, and a program that is agile, responsive, and continuously improving."

As further noted in the document, the agency's annual appropriation to maintain effective oversight in this changing environment has remained essentially flat since FY 2016 at about \$1.6 billion. To stay within the agency's annual appropriated amounts, in January 2017 the SEC implemented a hiring freeze that continued throughout FY 2018. With only few exceptions to the hiring freeze permitted, according to the SEC's Office of Human Resources (OHR), the agency's overall staffing level declined from 4,689 positions at the beginning of the hiring freeze to 4,459 positions at the end of FY 2018 (or about 5 percent).<sup>3</sup> In FY 2019, the SEC seeks to restore 100 positions to address critical priorities and enhance the agency's expertise in key areas.

*Office of Compliance Inspections and Examinations (OCIE).* Changes in the securities markets and financial industry, as well as difficult fiscal realities, have agency-wide impacts; however, since 2014, we have reported as a challenge the immediate and pressing need for

---

<sup>2</sup> U.S. Securities and Exchange Commission, *Fiscal Year 2019 Congressional Budget Justification and Annual Performance Plan; Fiscal Year 2017 Annual Performance Report*; February 12, 2018.

<sup>3</sup> We further discuss the challenge of ensuring effective human capital management on page 12.

ensuring sufficient examination coverage of registered investment advisers by OCIE. OCIE directs the SEC's National Examination Program, which protects the interests of retail investors by determining whether money managers handling retail customer funds are complying with SEC rules. According to the agency's FY 2019 Congressional Budget Justification and Annual Performance Plan, in FY 2017, staff examined about 15 percent of registered investment advisers (an increase over prior years), yet nearly 35 percent of all registered investment advisers have never been examined. The document further states:

Significant additional resources are critical to the examination program in order to improve the examination coverage of these entities. . . . As stated above, the number of registered investment advisers and their assets under management has grown steadily over the years, while staff resources have not kept pace with the growing responsibilities. OCIE expects this growth to continue through FY 2018 and FY 2019 and estimates there will be approximately 20 investment advisers per staff member. In addition, it is anticipated that the population of investment advisers will be larger and more complex than ever.

In light of these challenges, in FY 2019 the SEC requested 24 positions for OCIE—the largest increase for any division or office—to partially restore critical staffing losses from the last 2 years, enhance examination coverage of investment advisers, focus on critical risks impacting market participants, address new responsibilities, and implement other program improvements. It is imperative that agency management effectively use risk-based processes and leverage technology and analytics to address regulatory responsibilities, including those of the examination program, given limited resources.

To assess aspects of the SEC's investment adviser examinations, in FY 2017, we initiated an audit to determine whether OCIE established effective controls over its investment adviser examination completion process. In part, we sought to determine whether OCIE effectively used findings from examinations and Corrective Action Reviews as part of its risk-based, data-driven examination selection process. In our report titled *Audit of the Office of Compliance Inspections and Examinations' Investment Adviser Examination Completion Process* (Report No. 541, issued July 21, 2017), we made three recommendations for corrective action, including that OCIE develop and disseminate to staff guidance for assigning final examination risk ratings before closing examinations. As of the date of this memorandum, this recommendation remains open.<sup>4</sup>

In FY 2018, we completed an evaluation of OCIE's Technology Controls Program (TCP), which manages a relatively new area of responsibility for the SEC. In November 2014, the SEC adopted Regulation Systems Compliance and Integrity (SCI), under which the agency monitors the security and capabilities of U.S. securities markets' technological infrastructure.<sup>5</sup>

---

<sup>4</sup> We closed the other two recommendations in August 2018. According to OCIE management, in response to the remaining open recommendation, management has developed and disseminated general guidance for assigning risk ratings and is undertaking technological updates to implement the guidance. Formal guidance will be issued program-wide once the technological updates are finalized.

<sup>5</sup> Regulation SCI applies primarily to the systems of SCI entities—self-regulatory organizations, certain alternative trading systems, disseminators of consolidated market data (known as plan processors), and certain exempt clearing agencies—that directly support any one of the following six key securities market functions: (1) trading, (2) clearance and settlement, (3) order routing, (4) market data, (5) market regulation, and (6) market surveillance.

OCIE's TCP is responsible for ensuring SCI entity compliance and for evaluating whether entities have established, maintained, and enforced written policies and procedures reasonably designed to ensure the capacity, integrity, resiliency, availability, and security of their Regulation SCI systems.<sup>6</sup> Our evaluation assessed OCIE's TCP to determine, among other things, whether the program provided effective oversight of entities' compliance with Regulation SCI.

In our report titled *TCP Established Method to Effectively Oversee Entity Compliance With Regulation SCI But Could Improve Aspects of Program Management* (Report No. 551, issued September 24, 2018), we reported that TCP has an established method to effectively oversee entity compliance with Regulation SCI through its CyberWatch program and through TCP examinations. However, we identified opportunities to improve aspects of TCP program management, including its development and use of information technology systems (further discussed on page 6). We made three recommendations for corrective action. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

*Division of Enforcement (Enforcement).* Enforcement plays an essential role in carrying out the SEC's mission by investigating and bringing actions against those who violate Federal securities laws. The Commission's enforcement actions cover a broad range of subject areas, including investment management, securities offerings, issuer reporting and accounting, market manipulation, insider trading, broker-dealer activities, cyber-related conduct, and the Foreign Corrupt Practices Act, among others.

Despite Enforcement's successes in returning funds to harmed investors, agency management has acknowledged a recent development that threatens Enforcement's ability to continue doing so for long-running frauds. Specifically, in their May 16, 2018, congressional testimony, and in the Office of the Investor Advocate's Report on Objectives for FY 2019, Enforcement's co-directors and the agency's Investor Advocate, respectively, cited as a concern the Supreme Court's June 2017 decision in *Kokesh v. SEC*.<sup>7</sup> The Court held that Commission claims for disgorgement are subject to a 5-year statute of limitations—a decision that agency officials have stated may have a far-reaching impact on SEC enforcement actions and the Commission's ability to recover funds stolen from investors. Enforcement's co-directors stated in their congressional testimony that the *Kokesh* decision has already had a significant impact on the Division, and they estimated that, in the year since the decision, Enforcement has had to forego more than \$800 million of disgorgement in both litigated and settled actions.<sup>8</sup>

---

<sup>6</sup> Regulation SCI established rules for SCI entities designed to reduce the occurrence of systems issues, improve resiliency when systems problems occur, and enhance the SEC's oversight and enforcement of securities market technology infrastructure.

<sup>7</sup> Co-Directors, Division of Enforcement, Stephanie Avakian and Steven Peikin, *Oversight of the SEC's Division of Enforcement*, before the Committee on Financial Services, Subcommittee on Capital Markets, Securities, and Investment, U.S. House of Representatives; May 16, 2018.

U.S. Securities and Exchange Commission, Office of the Investor Advocate, *Report on Objectives for Fiscal Year 2019*; June 29, 2018.

<sup>8</sup> Webcast of verbal testimony available at: <https://financialservices.house.gov/calendar/eventsingle> (40:50 mark).

Although the ultimate impact of *Kokesh* remains to be seen, it is imperative that Enforcement uncover, investigate, and bring cases as quickly as possible. We note that, in FY 2017, the percentage of first enforcement actions filed within 2 years of the opening of the matter under inquiry or investigation was 52 percent. This did not meet the FY 2017 target of 65 percent and was a decrease from FYs 2012 through 2016, when the percentage ranged from 64 percent to 53 percent. In addition, in FY 2017, the average number of months between opening a matter under inquiry or investigation and commencing an enforcement action was 24 months, which was the same in the 2 previous years. This also did not meet the FY 2017 target of 20 months and was an increase from FYs 2012 through 2014 when the average number of months was 21. To address the issue of timeliness in investigations, Enforcement has reported measures that include emphasizing expediency in quarterly case reviews, promoting best practices regarding efficiencies in various phases of the investigative process, leveraging data analytics capabilities, and conducting training on tools that expedite investigations.<sup>9</sup>

*Obstruction of SEC Programs.* The SEC depends on the provision of accurate, truthful information from the people and entities it regulates. To this end, as we reported in 2017, the OIG conducts investigations of individuals who provide false or misleading information to the SEC during its examinations and enforcement actions. In one such case, and as a result of a joint Federal Bureau of Investigation and OIG investigation, the former Vice President of Investor Relations at a Massachusetts-based company pleaded guilty to charges of securities fraud in connection with a scheme to manipulate trading in the company's shares and obstruction of proceedings before the SEC. At his plea, the individual admitted that, beginning in or about November 2016, he engaged in manipulative trades in company stock that simulated market interest in the stock and artificially pushed up the trading price. These trades included orders to buy at a price much higher than the price of the preceding market transaction. The individual also admitted that during a 2017 SEC investigation into manipulative trading in the company's stock, he testified falsely before the SEC. Two associates of the former Vice President of Investor Relations were also arrested and charged.

In another case, two former senior officials of a company were arrested and charged for their role in an alleged conspiracy and fraud scheme. From at least 2013 to 2017, individuals conspired in a scheme to defraud by making misrepresentations to raise money for an outdoor media company, and then by misappropriating that money from the company through another entity. They then both concealed their misstatements and misappropriation in various ways, and obstructed an SEC investigation into their conduct.

***Importance of Leveraging Technology and Analytics.*** As in previous years, agency management and the OIG recognize that technology and analytics are critical to the mission of the SEC and its ability to deliver information to the public, identify risks, uncover frauds, sift through large volumes of data, inform policy-making, and streamline operations. The SEC's FY 2019 Congressional Budget Justification and Annual Performance Plan states:

---

<sup>9</sup> The SEC's FY 2017 Annual Performance Report (February 12, 2018) (1) includes Performance Goal 2.3.2, *Percentage of first enforcement actions filed within two years of the opening of an investigation*, and Performance Goal 2.3.3, *Average months between opening a matter under inquiry or an investigation and commencing an enforcement action*; (2) compares the agency's results from FY 2012 through FY 2017; and (3) describes plans for improving program performance, where necessary.

Long-term investment and development in technology and analytical tools will be critical to the future success of the Commission's oversight responsibilities. Particularly important in FY 2019 will be a continued focus on enhancing quantitative and data analytic efforts. These tools will provide staff with a greater ability to monitor for trends and emerging risks, ultimately enabling the staff to allocate SEC resources more effectively.

In support of these efforts, the SEC requested an additional \$45 million in FY 2019 to fund critical requirements. This request relies on continued access to the Reserve Fund, created by the Dodd-Frank Wall Street Reform and Consumer Protection Act.<sup>10</sup> We note that the President's Budget for FY 2019 again proposes to eliminate the Reserve Fund beginning in 2020.<sup>11</sup> Critical requirements the SEC seeks to fund include:

- continuing the development of advanced analytics solutions for detecting suspicious behavior in high frequency trading and other complex trading areas;
- improving storage, processing, security, and management of large volumes of data;
- modernizing the SEC's infrastructure and computing environment to enhance security, improve performance, and streamline delivery; and
- improving the SEC's ability to analyze fixed income market data.

Other key information technology initiatives include improving examinations through risk assessment and surveillance tools; enhancing systems that support the enforcement program; increasing investments in cybersecurity (further discussed on page 7); and improving access and usefulness of information available to the public through the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system.

The EDGAR system is at the heart of the SEC's mission of protecting investors; maintaining fair, orderly, and efficient markets; and facilitating capital formation. The system supports 18 of the agency's 23 major business functions (or about 78 percent), including the agency's corporation finance, examination, and enforcement functions. In FY 2017, we completed an audit of the SEC's progress in enhancing and redesigning the EDGAR system. In our report titled *Audit of the SEC's Progress in Enhancing and Redesigning the Electronic Data Gathering, Analysis, and Retrieval System* (Report No. 544, issued September 28, 2017), we made nine recommendations for corrective action. Management took corrective action sufficient to close all nine recommendations.

On September 20, 2017, the SEC Chairman publicly disclosed that a software vulnerability in a component of the EDGAR system previously detected in 2016 resulted in unauthorized access to non-public information, which may have provided a basis for illicit trading. After the Chairman's disclosure, the agency learned that an EDGAR test filing accessed by third parties contained personally identifiable information (PII)—names, dates of birth, and social security numbers—of two individuals. The Chairman, who began his service in May 2017 and was

---

<sup>10</sup> Pub. L. No. 111-203, § 991e, 124 Stat. 1376, 1954-55 (2010).

<sup>11</sup> Office of Management and Budget, *Budget of the U.S. Government, Efficient, Effective, Accountable An American Budget, Fiscal Year 2019*.

notified of the incident in August 2017, initiated several work streams, including requesting that the OIG review the agency's handling of, and response to, the 2016 incident. As we further discuss on page 8, during FY 2018, we completed our evaluation and provided our results and recommendations to agency management.

We also investigated allegations that a false filing announcing a bid to take over a company was submitted in the EDGAR system and that the filing had the effect of manipulating the price of the company's stock. The investigation determined that an individual submitted the false information to the SEC. On May 5, 2017, a criminal complaint was filed, charging the individual with violations of 15 United States Code (USC) §§ 78j(b) and 78ff, Securities Fraud, Manipulative and Deceptive Devices; 17 Code of Federal Regulations §240.10b-5, Securities and Exchange Act, Employment of Manipulative and Deceptive Devices; and 18 USC § 1343, Wire Fraud. The individual pleaded guilty to criminal charges relating to the false EDGAR filing. As a result of the individual's guilty plea, the individual was sentenced to 24 months imprisonment and 24 months supervised release; the individual was also ordered to forfeit \$3,914.08 and pay a \$100.00 special assessment.

Finally, in FY 2018 we assessed OCIE's continued development of the SEC's Technology Risk Assurance, Compliance, and Examination Report (TRACER) system in support of the TCP. Between September 2015 and January 2018, TCP continued development of the system at a cost of nearly \$780,000. TRACER was originally intended to intake filings and monitor SCI entity system outages and changes; but the system evolved into the system of record for TCP examinations. In our report titled *TCP Established Method to Effectively Oversee Entity Compliance With Regulation SCI But Could Improve Aspects of Program Management* (Report No. 551, issued September 24, 2018), we reported that certain planned system capabilities were not realized and, based on a lack of documentation, it was unclear how TCP assessed or managed system requirements. On May 4, 2018, TCP management decided to discontinue developing the TRACER system and transition the TCP examination program to OCIE's Tracking and Reporting Examinations National Documentation System, which is expected to yield operational and cost savings benefits.

In FY 2019, we will continue assessing how well the SEC achieves its regulatory oversight responsibilities and leverages technology and analytics. We will follow-up on previous recommendations related to OCIE's examination programs and to enhancing and redesigning the EDGAR system. As needed, we will leverage our resources to investigate obstruction of SEC programs. We are also planning work to (1) determine whether Enforcement's case tracking system facilitates efficient and effective information sharing; (2) determine whether the Division of Trading and Markets has provided adequate oversight of broker-dealers; (3) follow up on a prior OIG assessment of the Office of Investor Education and Advocacy's efficiency in addressing investor inquiries and processing investor complaints; (4) assess agency processes and controls for suspending trading in stocks; and (5) assess whether the SEC is adequately managing certain information technology investments to ensure investments meet budget and schedule goals and contribute to mission-related outcomes. Moreover, we will complete an ongoing evaluation of the Division of Economic and Risk Analysis' use of analytics and data in support of agency risk assessment and enforcement activities.

## **CHALLENGE: Ensuring an Effective Information Security Program**

**Strengthening the SEC's Cybersecurity Posture.** As stated in the SEC's FY 2017 Agency Financial Report, "Cybersecurity is vitally important to [the SEC], especially given the increased use of and dependence on data and electronic communications, greater complexity of technologies present in the financial marketplace, and continually evolving threats from a variety of sources."<sup>12</sup> The SEC's information systems process and store significant amounts of sensitive, non-public information, including information that is personally identifiable, commercially valuable, and market sensitive. The agency reported that its e-Discovery program alone is approaching one petabyte of data,<sup>13</sup> and management has worked to implement technological enhancements and additional data protection technologies.<sup>14</sup> However, in the FY 2017 Agency Financial Report, the SEC recognized a material weakness in its internal control over agency operations as a result of cybersecurity risks. Moreover, in his June 21, 2018, congressional testimony, the SEC Chairman acknowledged that more needs to be done to strengthen the SEC's cybersecurity posture.<sup>15</sup>

In recognition of these risks and organizational deficiencies identified by reviewing the 2016 intrusion into the EDGAR system, the SEC requested additional funds for FY 2019 to advance its cybersecurity program. Among other things, the agency is working to strengthen its data management capabilities and migrate select applications and workloads to secure cloud environments. As noted in the Chairman's congressional testimony, principal efforts to date include improving the SEC's:

- information technology governance and oversight,
- preventive and detective cybersecurity controls,
- awareness across the agency of the sensitivity and risks related to data collection and storage, and
- efforts to modernize key legacy information systems, especially EDGAR.

As previously stated, the EDGAR system is central to the agency's mission and critical to the functioning of the capital markets. On a typical day, investors and other market participants access more than 50 million pages of disclosure documents through the system, making the availability of accurate, complete, and timely information essential. Without adequate controls to ensure the SEC identifies, handles, and responds to EDGAR system incidents in a timely manner, threat actors could gain unauthorized access to the system, which could lead to illicit

---

<sup>12</sup> U.S. Securities and Exchange Commission, *Agency Financial Report, Fiscal Year 2017*; November 14, 2017.

<sup>13</sup> A petabyte is a unit of information equal to about 1 quadrillion bytes, 1 million gigabytes, or 1 thousand terabytes. One petabyte of data is roughly equivalent to the amount of information that can be stored in about 20 million four-drawer filing cabinets (See U.S. Government Accountability Office, *Military Base Realignment and Closures: The National Geospatial-Intelligence Agency's Technology Center Construction Project*; GAO-12-770R; June 29, 2012).

<sup>14</sup> U.S. Securities and Exchange Commission, *Fiscal Year 2019 Congressional Budget Justification and Annual Performance Plan; Fiscal Year 2017 Annual Performance Report*; February 12, 2018.

<sup>15</sup> SEC Chairman Jay Clayton, *Testimony on Oversight of the U.S. Securities and Exchange Commission*, before the Committee on Financial Services, U.S. House of Representatives; June 21, 2018.

trading, negative impacts to the economy and public access to filings, and loss of public confidence in the SEC.

In response to the 2016 intrusion into the EDGAR system, the SEC Chairman initiated several work streams to assess the nature, cause, and scope of the intrusion; the potential factors that may have led to the intrusion; the agency's response at the time; and the extent to which cybersecurity enhancements are needed at the SEC. One work stream was a request that the OIG review the agency's handling of, and response to, the 2016 incident. In November 2017, we initiated an evaluation. In July 2018, we presented the Chairman and other SEC Commissioners with the non-public results of our evaluation relative to the 2016 EDGAR intrusion. In addition, on September 21, 2018, we issued a report titled *Evaluation of the EDGAR System's Governance and Incident Handling Processes* (Report No. 550), which presented the OIG's findings and recommendations from our broader assessment of the information security practices applicable to the EDGAR system between FYs 2015 and 2017.

In our report, we noted that, during the period we reviewed, the EDGAR system lacked adequate governance commensurate with the system's importance to the SEC's mission. In addition, certain preventive controls either did not exist or operate as designed, and the SEC lacked an effective incident handling process. Among other things, these weaknesses potentially increased the risk of EDGAR security incidents and impeded the SEC's efforts to respond to incidents. An internal review conducted by the agency's Office of General Counsel reached similar conclusions.

The SEC has strengthened EDGAR's system security posture, including the handling of and response to vulnerabilities. Among other actions, the agency established a Cyber Initiative Working Group to oversee and lead a number of priority cyber initiatives such as an EDGAR security uplift. In addition, the Commission has acted to eliminate the collection of social security numbers and dates of birth on a number of EDGAR forms where it was determined that the information was not necessary to the SEC's mission. As this and other work continues, opportunities for further improvement exist. Our report made 14 recommendations to improve the SEC's EDGAR system governance, security practices, and incident handling processes. We also noted that open recommendations from prior OIG work should address some of our observations, and we encouraged management to implement all agreed-to corrective actions.

***Maturing the SEC's Information Security Program.*** Federal guidance makes clear that, from senior management down to individual users, many individuals in an organization have a stake in information security and should work collaboratively to ensure information security.<sup>16</sup> The SEC's own privacy and information security awareness training acknowledges the collective responsibility for maintaining data security. To comply with the Federal Information Security Modernization Act of 2014 (FISMA),<sup>17</sup> annually, we assess the SEC's implementation of FISMA information security requirements and the effectiveness of the agency's information security program on a maturity model scale. In addition, as further described below, we

---

<sup>16</sup> National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*; October 2006 (Updated March 7, 2007).

<sup>17</sup> Pub. L. No. 113-283, which amended the Federal Information Security Management Act of 2002, Title III of the E-Government Act of 2002 (Pub. L. No. 107-347).

continue to identify opportunities to mature the SEC's information security program outside the scope of our FISMA-related work, often where responsibility for information security crosses organizational boundaries.

Since our audit of the SEC's compliance with FISMA for FY 2016,<sup>18</sup> the agency's Office of Information Technology improved aspects of the SEC's information security program. Among other actions taken, the Office of Information Technology implemented improved identification and authentication processes, finalized the SEC's information security continuous monitoring strategy, developed and delivered privacy and information security awareness training to SEC employees and contractors (achieving a 99-percent compliance rate), and conducted two incident response exercises and an annual test of the agency's enterprise disaster recovery plan. Although the agency took steps to strengthen its information security program, we determined in FY 2017 that the program had not significantly matured and, as in FY 2016, did not meet annual Inspector General FISMA reporting metrics' definition of "effective."<sup>19</sup>

In our report titled *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017* (Report No. 546, issued March 30, 2018), we noted that the SEC's maturity level for the five Cybersecurity Framework security functions ("identify," "protect," "detect," "respond," and "recover") was either Level 2 ("Defined") or Level 3 ("Consistently Implemented"). None of the functions reached Level 4 ("Managed and Measurable"). These results were similar to the previous year's results. We reported opportunities for improvement in each of the assessment domains identified by the Department of Homeland Security, stating that the SEC can mature its programs for risk management, configuration management, identity and access management, information security training, information security continuous monitoring, incident response, and contingency planning. Acting on these opportunities will help minimize the risk of unauthorized disclosure, modification, use, and disruption of the SEC's sensitive, non-public information, and assist the agency's information security program reach the next maturity level.

Our FY 2017 FISMA report made 20 recommendations for corrective action. Management concurred with each recommendation and is working to implement corrective actions.<sup>20</sup> In addition, our FY 2018 evaluation of the SEC's compliance with FISMA, which began in May 2018, is ongoing.

Lastly, in June 2018, we completed our *Audit of the SEC's Internal Controls for Retaining External Experts and Foreign Counsel for the Division of Enforcement* (Report No. 547, issued June 15, 2018). Although not related to our FISMA work, we identified certain information security risks that crossed organizational boundaries.

---

<sup>18</sup> U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2016*, Report No. 539; March 7, 2017.

<sup>19</sup> *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, Version 1.0; April 17, 2017.

*FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, Version 1.1.3; September 26, 2016.

<sup>20</sup> As of the date of this memorandum, we have closed 19 of the 21 recommendations from our FY 2016 FISMA report, and 1 of the 20 recommendations from our FY 2017 FISMA report.

Enforcement routinely retains outside experts—attorneys, accountants, economists, and other professionals—and foreign counsel (collectively referred to hereafter as “experts”) to fulfill a variety of roles during investigations and litigation. So that experts can fulfill contract requirements, Enforcement may provide experts sensitive, non-public information, including information that is personally identifiable, commercially valuable, and market-sensitive.

We judgmentally selected and reviewed 21 of Enforcement’s 197 contracts for expert services awarded between April 1, 2015, and March 31, 2017. Although the SEC established some requirements in recognition of certain information security risks, agency personnel did not always enforce those requirements. For example, more than half of the 113 individuals reported as having worked on the contracts we reviewed either had not signed the required non-disclosure agreement or had signed one after beginning work. For one contract we reviewed, 11 of 12 non-disclosure agreements on file were signed, on average, 305 days after individuals began work. The remaining six individuals who performed work under the contract had not signed a non-disclosure agreement. In addition, in at least five instances, agency personnel had not enforced contract requirements related to safeguarding PII even though experts had access to PII, including investors’ names, addresses, dates of birth, and customer account information. We also found that contracts lacked controls regarding the inadvertent release or disclosure of information after the SEC transmits information to experts. As a result, the agency lacked assurance that experts and their information systems achieved basic levels of security to protect the SEC’s sensitive, non-public information, including PII. We did not identify instances in which unauthorized individuals accessed such information after it was provided to experts. However, the agency should take steps to minimize the risk of unauthorized disclosure, modification, and use of its sensitive, non-public information provided to experts.

We made seven recommendations for corrective action, including that Enforcement and Office of Acquisitions personnel work together to assess protection of PII under expert services contracts, develop a process that ensures contracting officers enforce contract requirements related to PII when necessary, and implement a standardized process to verify receipt of non-disclosure agreements from individuals who will perform work under contracts for expert services. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action. We further discuss this audit on the following page.

In FY 2019, we will continue to assess the SEC’s information security program, including its cybersecurity program. In particular, we will (1) determine whether the agency has an effective process to acquire, implement, and manage its cloud computing environment; (2) evaluate the SEC’s mobile device program and controls for protecting information stored and/or processed on such devices; and (3) assess the agency’s implementation of its data loss prevention program. As necessary, we will also continue making recommendations for improvement where processes and responsibilities for information security cross organizational lines.

### ***CHALLENGE: Improving Contract Management***

In 2017, we identified contract management, including systemic issues regarding the performance and oversight of SEC CORs, as an agency management and performance challenge. In response, SEC management reported that the agency’s Office of Acquisitions

worked on a variety of fronts to further promote effective contract management. Such actions included improving communications between contracting officers and CORs, ensuring CORs received proper training and enforced their use of the Electronic Contract File system, conducting annual reviews of contract files to make sure files contain all appropriate documentation, and improving reporting. In addition, over the last year, SEC management developed and provided training to contracting officers and CORs around the potential for fraud in the area of procurement, and the OIG provided a block of instruction during training. The agency is also working to address prior OIG recommendations related to agency management of contracts we reviewed.

According to the agency's FY 2019 Congressional Budget Justification and Annual Performance Plan, in FY 2019, the Office of Acquisitions plans to continue the COR Improvement Initiative "to create a more comprehensive COR Program that will provide efficient and functional control, transparency, and management of the COR Program across the SEC."

As previously stated, in June 2018, we completed our *Audit of the SEC's Internal Controls for Retaining External Experts and Foreign Counsel for the Division of Enforcement* (Report No. 547, issued June 15, 2018), which again raised concerns about the performance of SEC CORs. For example, to help CORs monitor the agency's contracts for expert services, the SEC required experts to submit monthly status reports. Experts generally did not submit these reports, and agency personnel did not enforce the requirement to do so. In addition, some experts submitted invoices with little to no detail about the work performed and the personnel who performed it. Because CORs for the contracts we reviewed had limited first-hand knowledge of the sufficiency of contract deliverables and work performed, the CORs were unable to determine whether invoices accurately reflected work performed. Instead, CORs relied on Enforcement attorneys for that determination. As a result, CORs' ability to conduct surveillance of contractors' performance was limited.

We also completed an audit to determine whether the SEC's Information Services Branch (Library)—directly or through SEC divisions, offices, and/or working groups—developed and implemented effective controls for acquiring, maintaining, and tracking electronic information sources (EIS) and data source subscriptions, including proper assessment of agency needs and associated costs. In our report titled *The SEC Should Take Action to Strengthen Its Management of Electronic Information Sources, Data Sources, and Print Materials* (Report No. 548, issued September 11, 2018), we identified improvements needed in the acquisition and management of the SEC's EIS, data source, and print material resources. Specifically, we found that:

- contracting staff did not detect in 2 vendors' price quotes \$157,650 in calculation errors;
- 3 of the 22 contract files we reviewed were missing adequate support to justify a fair and reasonable price determination;
- in multiple instances, the responsible COR approved vendor invoices without validating receipt of deliverables; and
- Library personnel were unable to support certain print material acquisitions because personnel did not retain the justification of need.

Moreover, although the Library assesses usage of the SEC's EIS, data source, and print material resources before renewing subscriptions, no policies or procedures existed to guide this process. Also, the final decision whether an assigned Bloomberg resource (used by staff to access real-time market data) should be cancelled or transferred to another user remains with divisions and offices, which limits the Library's ability to ensure these resources are fully used. In fact, we found 128 instances of potentially underused Bloomberg resources, with an estimated cost of \$231,745. We made nine recommendations for corrective action. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

In FY 2019, we will further assess the SEC's contract management and acquisition processes. Specifically, we will complete an ongoing audit of the agency's infrastructure support services contract. To better determine the nature and extent of progress and/or deficiencies in the area of contract management, we will also continue to leverage standardized steps we created to obtain an understanding of the agency's contract management when contracting is central to answering an audit's or evaluation's objectives. Lastly, we will continue to support the SEC's efforts to train contracting officers and CORs about the potential for procurement-related fraud.

### ***CHALLENGE: Ensuring Effective Human Capital Management***

The SEC's new, multi-year strategic plan establishes that strengthening the agency's human capital management program is key to achieving agency goals.<sup>21</sup> Likewise, according to the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*, effective management of an entity's workforce, its human capital, is essential to achieving results and an important part of internal control.<sup>22</sup> In the February 2017 update to its High-Risk Series, GAO again recognized Strategic Human Capital Management as a high-risk area needing attention by Congress and the executive branch.<sup>23</sup> Moreover, in 2016, we and the GAO reported needed improvements in the SEC's management of human capital.<sup>24</sup> As in previous years, in 2017 we recognized human capital management as an agency management and performance challenge.

To determine the SEC's progress toward addressing human capital management challenges, in March 2018, we initiated an evaluation that assessed the SEC's implementation of applicable Federal internal control standards and plans for aligning the agency's human capital management strategy with key elements of the Office of Personnel Management's (OPM)

---

<sup>21</sup> U.S. Securities and Exchange Commission, *Strategic Plan Fiscal Years 2018-2022*, draft for comment.

<sup>22</sup> U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government*; GAO-14-704G, September 2014.

<sup>23</sup> U.S. Government Accountability Office, *HIGH-RISK SERIES Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*; GAO-17-317, February 2017.

<sup>24</sup> U.S. Securities and Exchange Commission, Office of Inspector General, *Final Closeout Memorandum: Audit of the SEC's Hiring Practices*; August 19, 2016.

Human Capital Framework (HCF).<sup>25</sup> In our report titled *The SEC Made Progress But Work Remains To Address Human Capital Management Challenges and Align With the Human Capital Framework* (Report No. 549, issued September 11, 2018), we reported that the SEC's OHR has taken steps to address the human capital management challenges the agency faces. Among other things, OHR worked to identify competency gaps and address succession planning, conducted quality of new hire surveys and annual human capital reviews, began developing a workforce dashboard, and implemented various quality assurance reviews. However, we identified limitations and delays in OHR's efforts and additional challenges and opportunities for improvement. Specifically, the SEC:

- has faced delays in identifying competency gaps, and limitations in efforts to develop a plan to fill supervisory positions;
- lacks a formal succession plan; and
- lacks periodic validations of the agency's current performance management system and related standard operating procedures.

Many of these issues resulted from delays in reaching agreements with the National Treasury Employees Union.

Also, although it appears that additional controls implemented since 2016 have helped to improve the accuracy of the SEC's Workforce Transformation and Tracking System data, OHR could maintain more detailed hiring action information in the system to explain inconsistencies in the data when they occur. In addition, OHR may have opportunities to improve hiring processes to better meet its hiring timeframes.

Although OHR has also taken steps to align with OPM's HCF, work remains. Specifically, in addition to the work that remains related to competency assessments, succession planning, and performance management, OHR's internal evaluation system needs improvement, as described in our report. Moreover, we surveyed OHR and SEC divisions, offices, and regional offices on areas of the HCF that correlate to the agency's previously identified human capital management challenges. We encouraged OHR to explore significant differences in survey responses and to address the four areas in which OHR acknowledged that additional work is needed to fully align with corresponding aspects of the HCF.

In our most recent evaluation report, we made nine recommendations for corrective action. Management concurred with the recommendations and has already made progress in some areas. For example, in August 2018, the SEC signed a Memorandum of Understanding with the National Treasury Employees Union. As of the date of this memorandum, agency-wide competency surveys were underway and were targeted for completion by the end of calendar year 2018. Additionally, the SEC engaged OPM to assist with assessing and implementing the current performance management program. OPM is expected to complete its assessment in March 2019. Our recommendations will be closed upon completion and verification of these and other corrective actions.

---

<sup>25</sup> Although implementing Federal regulations for OPM's HCF (5 CFR Part 250, Subpart B, Strategic Human Capital Management) apply only to Chief Financial Officers Act agencies (which do not include the SEC), the SEC is transitioning aspects of the agency's human capital management strategy to align with OPM's HCF guidance.

Section 962 of the Dodd-Frank Wall Street Reform and Consumer Protection Act mandates GAO to report triennially on the SEC's personnel management, including the competence of professional staff; the effectiveness of supervisors; and issues related to employee performance assessments, promotion, and intra-agency communication.<sup>26</sup> GAO issued its first and second reports in 2013 and 2016, respectively. In FY 2019, we will continue to (1) monitor the SEC's progress toward addressing previously identified human capital management challenges, and (2) coordinate with GAO on its next personnel management review.

---

<sup>26</sup> Pub. L. No. 111-203, § 962, 124 Stat. 1376, 1908-09 (2010).