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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

October 5, 2017

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 2017*

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 challenges that the SEC faces. 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 SEC management and staff, and the U.S. Government Accountability Office. We previously provided a draft of this statement to SEC officials and considered all comments received when finalizing the statement. As we begin fiscal year 2018, 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
Michael S. Piwowar, Commissioner
Richard Grant, Counsel, Office of Commissioner Piwowar

Kara M. Stein, Commissioner
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein
Robert B. Stebbins, General Counsel
Rick A. Fleming, Investor Advocate
Bryan Wood, Director, Office of Legislative and Intergovernmental Affairs
John J. Nester, Director, Office of Public Affairs
Kenneth Johnson, Acting Chief Operating Officer
Vance Cathell, Director, Office of Acquisitions
Lacey Dingman, Chief Human Capital Officer, Office of Human Resources
Pamela C. Dyson, Director/Chief Information Officer, Office of Information Technology
Caryn Kauffman, Acting Chief Financial Officer, Office of Financial Management
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

Attachment. THE INSPECTOR GENERAL'S STATEMENT ON THE SEC'S MANAGEMENT AND PERFORMANCE CHALLENGES, OCTOBER 2017

CHALLENGE: Meeting Regulatory Oversight Responsibilities

Overseeing Evolving Markets With Static Resources. Increases in the U.S. Securities and Exchange Commission's (SEC or agency) responsibilities in recent years continue to present challenges for the agency as it carries out its mission. For fiscal year (FY) 2018, the SEC requested about $1.6 billion, essentially the same as its FY 2017 appropriation. Despite difficult fiscal realities, as stated in the SEC's FY 2018 Congressional Budget Justification, the entities and organizations the agency is charged with overseeing continue to grow and advance:

> As markets have evolved—including as a result of innovation, technology, and globalization—the SEC's responsibilities have continued to grow and become more complex. . . . As the markets, products, and participants that the SEC oversees and regulates increase in size and complexity, the agency's mandate to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation becomes more challenging. To maximize the use of the SEC's resources to fulfill this mission, the agency continually strives to allocate its time and funds toward the highest and best uses.[1]

The SEC is charged with overseeing over 26,000 market participants, including about 12,000 investment advisers, about 10,000 mutual funds and exchange traded funds, over 4,000 broker-dealers, over 650 mutual advisors, and 400 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 8,800 reporting companies. As the SEC Chairman testified to in June 2017, registered investment advisers now manage "more than $70 trillion in assets, which is more than three times 2001 levels."[2]

Since 2014, we have reported that the SEC has identified as a challenge the immediate and pressing need for ensuring sufficient examination coverage of registered investment advisers. According to the SEC's 2016 Agency Financial Report,[3] the SEC's Office of Compliance Inspections and Examinations (OCIE) enhanced its National Exam Program risk assessment efforts to focus limited time and resources on those firms presenting the highest risk. OCIE has also hired staff and transitioned resources from other areas to its program for investment advisers and investment companies. In his June 2017 congressional testimony, the SEC

---

[1] U.S. Securities and Exchange Commission, *Fiscal Year 2018 Congressional Budget Justification, Annual Performance Plan, and Fiscal Year 2016 Annual Performance Report*.

[2] SEC Chairman Jay Clayton, *Testimony on the Fiscal Year 2018 Budget Request of the U.S. Securities and Exchange Commission,* before the Subcommittee on Financial Services and General Government, Committee on Appropriations, United States Senate; June 27, 2017.

[3] U.S. Securities and Exchange Commission, *Agency Financial Report, Fiscal Year 2016*.

Chairman stated that, as a result of this shift and the introduction of efficiencies, the SEC was on track to deliver a 20 percent increase in the number of investment adviser examinations in FY 2017. Furthermore, the Chairman stated that, for FY 2018, OCIE anticipates being able to deliver an additional 5 percent increase in the number of investment adviser exams. The Chairman expected that, for at least the next several years, the SEC will need to do more each year to increase its examination coverage of investment advisers in light of continuing changes in the markets.

To assess the agency's progress in this area, in FY 2016, we initiated an audit to determine whether OCIE established effective controls over its investment adviser examination completion process to improve compliance with Federal securities laws, prevent fraud, inform policy, and monitor risk. We also 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 reported that controls over OCIE's investment adviser examination completion process were generally effective but improvements were needed to ensure OCIE staff appropriately review and consistently document investment adviser examination results and risk assessments. Doing so could help ensure staff can effectively consider the results of examinations during evaluations of risk for future examinations. Moreover, we found that OCIE can improve its investment adviser examination completion process and internal controls by updating or documenting policies and procedures consistent with the *Standards for Internal Control in the Federal Government*.[4]

We recommended that OCIE (1) design control activities related to the review and approval of examination work products to require adequate segregation of duties, (2) update National Exam Program policies and procedures to more clearly define the requirements for documenting examination meetings and interviews, and (3) develop and disseminate to OCIE staff guidance for assigning final examination risk ratings before closing examinations. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

In addition, the SEC depends on the provision of accurate, truthful information from the people and entities it regulates. To this end, the Office of Inspector General (OIG) conducts investigations of individuals who provide false or misleading information to the SEC during its examinations and enforcement actions. In one such case, the former president of a financial services company entered a guilty plea and was sentenced in Federal court to 1 year of probation, with 4 months to be served in home detention, and a fine of $4,000. The sentencing followed an OIG investigation that determined the official obstructed an SEC investigation into allegations that he concealed secret and improper referral payments he made to a lawyer in order to secure the business of a wealthy client.

Leveraging Technology To Keep Pace With Advances in Regulatory Areas. The SEC continues to modernize its information technology (IT) systems and seek ways to leverage technology to keep pace with the increasing size and complexity of capital markets that are often driven by advances in technology. The agency's FY 2018 budget request relied on

[4] U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014).

continued access to the Reserve Fund, created by the Dodd-Frank Wall Street Reform and Consumer Protection Act, to further the agency's goals in this area. As stated in the SEC Chairman's June 2017 congressional testimony:

> These funds, which have been dedicated to technology, have been important in our efforts to keep pace with the rapid technology advancements occurring in areas regulated by the SEC, as well as meeting emerging cybersecurity challenges. The continued availability of the Reserve Fund historically has allowed us to commit to critical, long-term technology initiatives that otherwise may have been more difficult for us to execute.

We note that the President's Budget for FY 2018 proposes to eliminate the Reserve Fund beginning in 2019.[5] As we have previously reported, the SEC's continuing key technology initiatives, funded by the Reserve Fund, include:

- expanding data analytics tools;
- improving the examination program through risk assessment and surveillance tools;
- enhancing systems that support the enforcement program;
- improving access and usefulness of information available to the public through the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system; and
- investing in further business process automation and enhancements.

The SEC is also increasing investments in cybersecurity, as discussed further on page 5 of this memorandum.

Recognizing the importance of technology in achieving the SEC's regulatory oversight responsibilities, we have continued assessing the SEC's progress in enhancing its technology. For example, in 2015, we issued a management letter that addressed the SEC's project to redesign the Tips, Complaints, and Referrals (TCR) system. The management letter (*Final Management Letter: Observations Noted During TCR System Audit Support Engagement*, issued May 20, 2015) identified various factors that led to schedule delays and cost increases in the SEC's TCR system redesign project and noted that, at the time, the SEC had not accepted the redesigned TCR system and a final user acceptance date had not been established. To follow-up on this important project, we conducted additional work and issued a second management letter in May 2017. Our May 2017 management letter on this subject (*Final Management Letter: Progress on the SEC's Tips, Complaints, and Referrals Intake and Resolution System Redesign and Vulnerability Remediation Efforts*, issued May 31, 2017) reported that the SEC had successfully tested and conditionally accepted the redesigned TCR system. However, the agency had not implemented the system, in part, because the system's multiple users considered new requirements and enhancements not previously required in the development effort. As of the date of our May 2017 management letter, the overall value of the SEC's contract to implement the system had increased by about $12.2 million (or

[5] Office of Management and Budget, *Budget of the U.S. Government, A New Foundation for American Greatness, Fiscal Year 2018*.

170 percent), and the SEC had obligated about $16.6 million and expended about $14.4 million of the total contract value (or twice the amount initially planned). Moreover, the SEC does not expect the redesigned TCR system to go-live until later this month (more than 3 years behind schedule).

Additionally, we reported that the most recent delays in accepting and implementing the redesigned TCR system were due, in part, to instability in the SEC's Oracle platform, which may have also impacted the agency's ability to test and deploy at least two other systems. At the same time, the SEC continued to operate the current TCR system but had not timely remediated some of the system's security vulnerabilities. In June 2017, SEC management provided a description of the actions the agency has taken or planned to take to address our concerns.

During FY 2017, we also assessed 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 reported that, since 2014, the SEC has made several improvements in its planning and governance of the program to redesign the EDGAR system while continuously enhancing the system in operation. Nonetheless, we identified opportunities for further improvement. Specifically, we determined that:

- the SEC's governance of EDGAR system enhancements, including the governance and operation of the EDGAR Requirements Subcommittee and the EDGAR system enhancement lessons learned process, needed improvement;

- the Office of Information Technology (OIT) did not consistently manage the scope of EDGAR system releases to ensure SEC needs were achieved;

- the SEC should improve its management of the EDGAR system engineering contract (discussed further on page 9 of this memorandum);

- OIT did not fully and consistently implement EDGAR system enhancements in compliance with Federal and SEC change management controls; and,

- although the SEC has taken steps to improve its ability to develop and implement a new electronic disclosure system that meets agency needs, further improvements can strengthen the agency's EDGAR redesign program governance and planning.

We made nine recommendations for corrective action. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

For FY 2018, we are planning additional work to assess how well the SEC leverages technology and achieves its regulatory oversight responsibilities. Specifically, we plan to review the agency's management of (1) examinations intended to strengthen the technology infrastructure of the U.S. securities markets, (2) investments in infrastructure support services, and (3) data accessed from the database known as the consolidated audit trail. In addition, we plan to evaluate the Division of Economic and Risk Analysis' use of analytics and data in support of risk assessment and enforcement activities.

CHALLENGE: Ensuring an Effective Information Security Program

The SEC generates and collects commercially valuable, market sensitive, proprietary, and other non-public information. According to the agency's FY 2018 Congressional Budget Justification, the SEC is increasing investments in information security (including cybersecurity) to address, as a top priority, the ability to monitor and avoid advanced persistent threats, and to improve risk management and monitoring. In May 2017, the SEC Chairman initiated an assessment of the agency's cybersecurity risk profile and approach to cybersecurity from a regulatory and oversight perspective. As noted in the Chairman's September 20, 2017, statement on cybersecurity, components of the agency's cybersecurity initiative build on prior agency efforts and include establishing a senior-level cybersecurity working group to coordinate information sharing, risk monitoring, and incident response efforts throughout the agency.[6]

We closed the remaining two recommendations from our FY 2014 Federal Information Security Management Act evaluation report and the remaining four recommendations from our FY 2015 Federal Information Security Modernization Act (FISMA) audit because OIT took steps to improve key information security program areas. These steps included: (1) defining and documenting access methods for externally-hosted systems, (2) re-authorizing systems with expired authorizations to operate, (3) updating the OIT Risk Committee charter to address vacancies, (4) conducting OIT Risk Committee meetings in accordance with the updated charter, (5) implementing capabilities to more efficiently address plans of action and milestones, and (6) updating configuration management policies and procedures in support of rollback to previous versions of baseline configurations. Furthermore, OIT continues to enhance capabilities and develop tools in areas such as risk analytics and vulnerability management. However, we continue to identify and assess opportunities for improvement in the agency's information security controls.

Specifically, we completed our FY 2016 FISMA audit and reported opportunities for improvement in each of the eight assessment domains identified by the Department of Homeland Security (DHS). As stated in our report titled *Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2016* (Report. No. 539, issued March 7, 2017), the SEC's information security program did not meet DHS' definition of "effective" as defined in the FY 2016 Inspector General FISMA Reporting Metrics. A summary of our observations for each of the eight assessment domains follows:

1. *Risk Management.* The SEC is taking steps to improve its risk management program, including updating Interconnection Security Agreement memorandums. However, these activities were not fully implemented in FY 2016, limiting the SEC's ability to effectively manage information security risk to organizational operations, organizational assets, individuals, and other organizations.

2. *Contractor Systems.* An ongoing agency project seeks to develop suggested security contract clauses for different types of contracts. However, we identified concerns in the Contractor Systems domain that could expose systems to unmitigated vulnerabilities.

[6] SEC Chairman Jay Clayton, *Statement on Cybersecurity*; September 20, 2017.

3. *Configuration Management.* The SEC is taking steps to strengthen its configuration management program, including leveraging the results of its participation in DHS's Cyber Hygiene Initiative, which aims to assist agencies in identifying critical vulnerabilities associated with public-facing assets. However, the SEC's configuration management program was not fully effective, which could expose SEC systems to configuration management vulnerabilities and exploitation.

4. *Identity and Access Management.* Although the SEC has established an identity and access management program, including policies and procedures, we identified areas for improvement. For example, access management processes did not ensure that 28 of 200 judgmentally sampled users requiring access to SEC information and information systems signed appropriate access agreements and participated in required training before gaining access.

5. *Security and Privacy Training.* The SEC has developed a security and privacy awareness and training program that includes comprehensive agency policies and procedures. However, we determined that OIT's practices did not ensure that SEC employees received privacy and information security awareness training annually as required by the Code of Federal Regulations. In addition, the SEC had not fully implemented a process to evaluate the skills of users with significant security and privacy responsibilities, and then provide those users with additional security and privacy training content or implement strategies to close any identified skills gaps as recommended by the National Institute of Standards and Technology.

6. *Information Security Continuous Monitoring.* The SEC is obtaining additional continuous monitoring tools and assistance as part of a DHS Continuous Diagnostics and Mitigation contract. However, the SEC did not have a mature and consistently implemented information security continuous monitoring program.

7. *Incident Response.* The SEC's incident response program is consistently implemented. To further mature the agency's incident response program, the SEC must ensure incident response activities are repeatable and metrics are used to measure and manage the implementation of the program, achieve situational awareness, and control ongoing risk.

8. *Contingency Planning.* The SEC has established a business continuity and disaster recovery policy to reduce the impact of a disruptive event or disaster. However, the SEC did not annually test its system-specific contingency plans and disaster recovery plan, in accordance with agency policy.

To improve the SEC's information security program, we made 21 recommendations. Management concurred with all 21 recommendations and provided evidence of corrective action taken for each one. We have closed 3 of the recommendations and are reviewing evidence of corrective action taken for the remaining 18 recommendations. In addition, our FY 2017 audit of the SEC's compliance with FISMA is ongoing.

In FY 2017, we also completed several investigations with information security implications. In one matter, we determined that an employee of one of the SEC's two data center facility service providers failed to follow the company's established access control procedures,

resulting in unauthorized access to the SEC's computer server space by an individual unaffiliated with the SEC. There was no evidence that the SEC's data center space was breached intentionally or that SEC servers were accessed. We issued a Management Implication Report to agency management recommending corrective action.

In two other investigations, we determined that SEC employees sent personally identifiable information or other non-public information to personal e-mail accounts. We reported the results of these investigations to SEC management to determine whether corrective administrative actions may be warranted.

As part of its audit of the SEC's FYs 2015 and 2016 financial statements, the U.S. Government Accountability Office (GAO) reported in July 2017 that the SEC improved the security controls over its key financial systems.[7] According to GAO, as of September 2016, the agency had resolved 47 of the 58 recommendations GAO had previously made that had not been implemented by the conclusion of GAO's FY 2015 audit. However, the SEC had not fully implemented the remaining 11 recommendations that included the following:

- consistently protecting its network boundaries from possible intrusions,
- identifying and authenticating users,
- authorizing access to resources,
- auditing and monitoring actions taken on its systems and network, and
- encrypting sensitive information while in transmission.

In addition, GAO reported that 15 newly identified control deficiencies limited the effectiveness of the SEC's controls for protecting the confidentiality, integrity, and availability of its information systems. For example, GAO found that the agency did not consistently control logical access to its financial and general support systems. In addition, although the agency enhanced its configuration management controls, it used unsupported software to process financial data. Furthermore, the SEC did not adequately segregate incompatible duties for one employee.

GAO found that these weaknesses existed, in part, because the SEC did not fully implement key elements of its information security program. For example, the SEC did not maintain up-to-date network diagrams and asset inventories in its system security plans for its general support system and its key financial system application to accurately and completely reflect the current operating environment. The agency also did not fully implement and continuously monitor those systems' security configurations.

GAO recommended that, in addition to the 11 prior recommendations that had not been fully implemented, the SEC should take 13 actions to address newly identified control deficiencies

[7] U.S. Government Accountability Office, *INFORMATION SECURITY SEC Improved Control of Financial Systems but Needs to Take Additional Actions* (GAO-17-469, July 27, 2017).

and 2 actions to more fully implement its information security program. Management concurred with GAO's recommendations and reported to us that the SEC has submitted to GAO evidence of corrective action taken for all prior year and newly identified recommendations.

In FY 2018, we will continue to leverage the expertise of OIG auditors, special agents, and IT specialists to assess the SEC's information security program. In particular, we will expand our digital extraction, forensic, and investigation capabilities in order to pursue complex IT crimes committed against the SEC and to provide digital forensics support during investigations and audits as needed.

CHALLENGE: Improving Contract Management

According to the SEC's 2016 Agency Financial Report, the Office of Acquisitions (OA) returned more than $40 million to the SEC by de-obligating funds from existing and expired contracts and agreements. OA also awarded enterprise agreements, reported one of the highest small-business participation levels across the Federal government, and began implementing an electronic filing system for contract and Contracting Officer's Representative (COR) files. In addition, OA reported that, in FY 2017, it would provide customized training to SEC CORs and continue to increase the number of certified program and project managers to improve contract management. However, as discussed below, we completed two audits in FY 2017 that assessed elements of the SEC's contract management and, during both audits, we identified areas of needed improvements, particularly regarding the performance and oversight of SEC CORs.

In 2016, we reported that OA improved the SEC's COR Program by sufficiently addressing all six recommendations from an OIG audit of the Program completed in 2015.[8] Nonetheless, in 2017, we completed our *Audit of the SEC's Management of Its Data Centers* (Report No. 543, issued September 29, 2017), and found that the SEC did not adequately manage or monitor its two data center contracts. Specifically, we found that CORs responsible for overseeing contractors who provide critical data center services[9] did not always validate contractor invoices. Moreover, the agency's data center contract files were incomplete and did not contain adequate support for key decisions, including cost increases and changes to data center infrastructure. Also, the SEC's data center contractors did not provide (and the SEC did not request) all required contract deliverables, such as annual security assessments and monthly reports, and the power consumption reports provided by one data center contractor were unusable.

We determined that the inadequate management and monitoring of the SEC's data center contracts was caused by (1) a lack of understanding and communication among key stakeholders in OA and OIT, including the Contracting Officer (CO) and CORs, and (2) insufficient oversight. Generally, the CORs did not fully understand their duties and responsibilities or the limits of their authority, and did not perform certain duties as required.

[8] U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Contracting Officer's Representative Program* (Report No. 530; September 18, 2015).

[9] The SEC's data centers house critical telecommunications, data, and computing resources, including EDGAR, which supports the financial reporting of public companies in the United States.

For example, a COR mistakenly thought he had the authority to waive deliverables required by the contracts. Furthermore, the CO did not provide effective oversight of the CORs' invoice validation process and never reviewed the COR contract files. The CO also did not ensure that the CORs monitored the contractors' compliance with the terms and conditions of the contracts. We observed similar deficiencies during our 2015 COR Program audit and our 2016 audit of the SEC's management of its protective security force contract.[10]

As a result of inadequate management and monitoring of the SEC's data center contracts, the SEC paid contractor invoices containing formula errors resulting in $217,159 in overpayments (which has since been refunded). We also determined that the agency paid about $2.8 million in unsupported costs.[11] If the SEC does not take the recommended corrective action to validate certain costs and if all contract options are exercised, the agency may incur additional costs of about $2.7 million in funds that could be put to better use over the remaining life of one of its data center contracts.[12] Moreover, the SEC paid for reports that the contractors did not provide or provided in unusable formats. Without these deliverables, we question how agency personnel could adequately monitor the contractors' performance to ensure SEC equipment and data was not vulnerable to damage, loss, or system disruptions, or maintain an up-to-date understanding of the security state and risk posture of information systems and data stored and processed at the agency's data centers.

We made 10 recommendations for corrective action, including that the SEC conduct comprehensive reviews of actions taken in 2012 and 2013 to relocate the agency's data centers and improve data center-related contract management. We also strongly encouraged the Director of OA to conduct a comprehensive review of the SEC's COR Program and ensure controls are developed or strengthened to improve the agency's contract management specific to activities performed by CORs and COs. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

As stated on page 4 of this memorandum, we also reported in FY 2017 that the SEC should improve its management of the EDGAR system engineering contract. Specifically, 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 reported that the SEC did not complete four of five required steps to ensure that the agency's contractor responsible for the EDGAR system engineering contract properly used earned value management to monitor the SEC's investments in EDGAR system enhancements, as required by the Office of Management and Budget (OMB).[13] In addition, OIT did not effectively use established contract performance metrics to manage the contractor's performance because

---

[10] U.S. Securities and Exchange Commission, Office of Inspector General, *Management of the SEC's Protective Security Force Contract Needs Improvement* (Report No. 536; June 22, 2016).

[11] These costs resulted from a contract task order and a significant contract modification that, at the time of our audit, were not supported by adequate documentation. The term "unsupported cost" is defined in the Inspector General Act, as amended (Public Law 95–452; 5 U.S.C. App.).

[12] These costs are associated with a significant contract modification that we found, at the time of our audit, was not supported by adequate documentation. We recommended that the CO and COR validate the costs (See Recommendation 6 in OIG Report No. 543.). The term "recommendation that funds be put to better use" is defined in the Inspector General Act, as amended (Public Law 95–452; 5 U.S.C. App.).

[13] Office of Management and Budget, Memorandum M-05-23, *Improving Information Technology (IT) Project Planning and Execution* (August 2005).

OIT had not established processes or controls for each metric. Furthermore, the EDGAR system performance requirements specified in the contract were not consistent with requirements specified in another SEC contract. As a result, the SEC accepted unreliable earned value management data and did not monitor its investments in EDGAR system enhancements or the EDGAR system engineering contractor's performance as effectively as planned.

To improve the SEC's management of the EDGAR system engineering contract and the SEC's efforts to monitor agency investments in EDGAR system enhancements, we made four recommendations for corrective action. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

We plan to perform work in FY 2018 to further assess the SEC's contract management. To better determine the nature and extent of progress and/or deficiencies in this area, we established standardized steps that we will use to obtain an understanding of the agency's contract management when contracting is central to answering an audit's or evaluation's objectives.

CHALLENGE: Ensuring Effective Human Capital Management

The SEC seeks to hire and retain a skilled and diverse workforce and to ensure that all decisions affecting employees and applicants are fair and ethical. Attracting, engaging, and retaining a technically proficient and diverse workforce is one of the agency's stated strategic objectives.[14] To that end, on April 6, 2017, the SEC's Chief Human Capital Officer (CHCO) testified before the House Subcommittee on Government Operations that the Partnership for Public Service recognized the SEC as the "most improved" of any mid-size agency based on the agency's 2016 Federal Employee Viewpoint Survey results. According to the CHCO, "These positive results reflect the culmination of a persistent, multi-year effort by employees, the National Treasury Employees Union (NTEU), and the SEC's leadership team in working together to create an environment that engages employees and supports their commitment to excellence on behalf of America's investors and our markets."[15] We noted that the SEC's Federal Employee Viewpoint Survey results improved again in 2017.

In addition, according to the SEC's 2016 Agency Financial Report, the agency's Aspiring Leaders Program (intended to promote and build leadership competencies of senior employees) continued in its second successful year. Also during 2016, the SEC's Office of Human Resources (OHR) collaborated with the Office of Personnel Management and internal stakeholders to develop the agency's first Workforce Plan. As we reported in 2016, the Workforce Plan "provides an overview of the current workforce; identifies critical workforce competencies for SEC mission critical occupations; and identifies perceived workforce competency gaps from supervisors/managers." Based on the identified competency gaps, the Plan establishes goals to reduce gaps in core/professional and technical competencies across mission-critical occupations, and increase leadership-ready talent pools across all grade

[14] U.S. Securities and Exchange Commission Strategic Plan, Fiscal Years 2014 – 2018.

[15] Lacey Dingman, Director, Office of Human Resources and Chief Human Capital Officer, *Statement on "Best Places to Work Rankings,"* April 6, 2017, before the United States House of Representatives Subcommittee on Government Operations, Committee on Oversight and Government Reform.

levels. The Plan also outlines strategies to begin addressing the competency gaps and includes tasks that should be initiated or completed in the next 2 years. However, as stated in previous years, human capital management remains a challenge.

In December 2016, GAO issued its second triennial report on the SEC's personnel management required under the Dodd-Frank Wall Street Reform and Consumer Protection Act.[16] GAO surveyed all SEC staff, evaluated SEC policies and procedures, and analyzed information on the SEC's practices, and concluded that actions are needed to address limited progress in resolving long-standing personnel management challenges. GAO reported that, although employee views on the SEC's organizational culture have generally improved since 2013, GAO's survey indicated that the SEC still operates in a compartmentalized way and that there is little communication and collaboration between divisions. Moreover, although the SEC has addressed two of seven recommendations from GAO's 2013 report, GAO reported that the agency faces added challenges in cross-divisional collaboration and hiring and promotion. Specifically, GAO found that the SEC:

- continues to lack assurance that all staff have the necessary skills,
- lacks assurance that the new performance management system will perform better than the previous one, and
- has made little progress to address GAO's two recommendations related to improving cross-divisional collaboration.[17]

In addition, GAO found that because the SEC has not identified skills gaps among its hiring specialists, its training of these staff is limited. As a result, GAO concluded that the SEC lacks assurance that its hiring specialists have the necessary skills to hire and promote the most qualified applicants, in accordance with key principles of an effective control system. We note that, in its February 2017 update to its High-Risk Series, GAO recognized Strategic Human Capital Management as a high-risk area that continues to need attention by Congress and the Executive Branch. Specifically, GAO's 2017 report states that:

> Mission-critical skills gaps within the federal workforce pose a high risk to the nation. Regardless of whether the shortfalls are in such government-wide occupations as cybersecurity and acquisitions, or in agency-specific occupations such as nurses at the Veterans Health Administration (VHA), skills gaps impede the federal government from cost-effectively serving the public and achieving results.[18]

---

[16] U.S. Government Accountability Office, *Securities and Exchange Commission, Actions Needed to Address Limited Progress in Resolving Long-Standing Personnel Management Challenges* (GAO-17-65, December 29, 2016).

[17] In response to a draft of GAO's report, the SEC disagreed with GAO's characterization of the state of the SEC's intra-agency communication and collaboration. The SEC stated, among other things, that significantly more progress has been made to resolve recommendations from GAO's 2013 report (addressing interdivisional communication and collaboration) than GAO's 2016 report recognizes.

[18] U.S. Government Accountability Office, *HIGH-RISK SERIES Progress Made on Many High-Risk Areas, While Substantial Efforts Needed on Others* (GAO-17-317, February 15, 2017).

GAO recommended that the SEC should (1) provide authority to the Chief Operating Officer or other official to enhance cross-divisional collaboration, and (2) develop and implement training for hiring specialists that is informed by a skills gap analysis. GAO also reiterated the need to address the remaining five prior unaddressed recommendations on workforce planning, performance management, and intra-agency collaboration. The SEC disagreed that enhancing the role of the Chief Operating Officer would be the optimal means to achieve further enhancements, but agreed with GAO's second recommendation.

In 2016, we reported that OHR did not have an effective method for assessing the timeliness of the SEC's hiring process, including maintaining reliable hiring data and monitoring hiring actions according to established timelines. Furthermore, we reported that OHR did not analyze quality-of-new-hire survey results to improve the SEC's hiring process. We urged OHR to implement an effective system based on reliable data to conduct comprehensive assessments of the SEC's hiring process, further improve the agency's hiring process, and increase the likelihood that SEC divisions and offices timely hire highly qualified candidates to meet mission requirements (*Final Closeout Memorandum: Audit of the SEC's Hiring Practices*, issued August 19, 2016). In response, management noted steps it has taken to improve the SEC's hiring process.

OHR has reported enhancing and streamlining the hiring process by eliminating the practice of hiring to a deadline and allowing for more fluid and timely hiring throughout the year. However, at the beginning of 2017, several factors outside the SEC's control created additional challenges in this area. Specifically, on January 23, 2017, the President imposed a Federal hiring freeze to halt the growth of the Federal workforce. Then, on April 12, 2017, OMB issued Memorandum M-17-22 (OMB 17-22),[19] which provides agencies guidance on fulfilling the requirements of the hiring freeze and an Executive Order to reorganize Executive Branch departments and agencies. OMB 17-22 also requires all agencies to:

- begin taking immediate actions to achieve near-term workforce reductions and cost savings, including planning for funding levels in the President's FY 2018 Budget Blueprint;
- develop a plan to maximize employee performance by June 30, 2017; and,
- in September 2017, submit to OMB (as part of the agency's FY 2019 budget submission to OMB) an Agency Reform Plan that includes long-term workforce reductions.

As a result, in May 2017, OHR notified all SEC divisions and offices that the SEC was voluntarily continuing the external hiring freeze while the agency developed plans in response to OMB 17-22.

In FY 2018, we will continue to monitor the SEC's human capital management, including its progress toward (1) addressing competency gaps identified by supervisors and managers, (2) meeting goals established in agency human capital and workforce plans, (3) addressing GAO's recommendations, and (4) complying with OMB 17-22.

[19] Office of Management and Budget, Memorandum 17-22, *Comprehensive Plan for Reforming the Federal Government and Reducing the Federal Civilian Workforce*; April 12, 2017.