U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Audit of the SEC's Progress in Enhancing and Redesigning the Electronic Data Gathering, Analysis, and Retrieval System

September 28, 2017
Report No. 544

REDACTED FOR PUBLIC RELEASE

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

September 28, 2017

TO: Kenneth Johnson, Acting Chief Operating Officer

Carl W. Hoecker

FROM: Carl W. Hoecker, Inspector General

SUBJECT: *Audit of the SEC's Progress in Enhancing and Redesigning the Electronic Data Gathering, Analysis, and Retrieval System*, Report No. 544

Attached is the Office of the Inspector General (OIG) final report detailing the results of our audit of the U.S. Securities and Exchange Commission's (SEC) progress in enhancing and redesigning the Electronic Data Gathering, Analysis, and Retrieval system. The report contains nine recommendations for corrective action that, if fully implemented, should improve the SEC's controls over EDGAR system enhancements and redesign efforts.

On September 15, 2017, we provided management with a draft of our report for review and comment. In its September 26, 2017, response, management concurred with our recommendations. We have included management's response as Appendix III in the final report.

Within the next 45 days, please provide the OIG with a written corrective action plan that addresses the recommendations. The corrective action plan should include information such as the responsible official/point of contact, timeframe for completing required actions, and milestones identifying how the agency will address the recommendations.

We appreciate the courtesies and cooperation extended to us during the audit. If you have questions, please contact me or 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
John J. Nester, Director, Office of Public Affairs

Bryan Wood, Director, Office of Legislative and Intergovernmental Affairs
Pamela C. Dyson, Director/Chief Information Officer, Office of Information Technology
Vance Cathell, Director, Office of Acquisitions
Mark Ambrose, Director, Office of Strategic Initiatives, Office of the Chief Operating Officer
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

Executive Summary

Audit of the SEC's Progress in Enhancing and Redesigning the Electronic Data Gathering, Analysis, and Retrieval System
Report No. 544
September 28, 2017

Why We Did This Audit

The U.S. Securities and Exchange Commission's (SEC or agency) ability to fulfill its mission is, in part, dependent on the successful operation of the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system. The SEC consistently spends over $14 million a year on the EDGAR system, or about 6 percent of the agency's information technology budget. These costs cover both ongoing operations and enhancements to the current EDGAR system. Separately, since fiscal year 2014, the agency has spent at least $3.4 million on efforts to redesign the EDGAR system. A disciplined process for managing the enhancements and redesign of the EDGAR system is necessary to ensure adequate system functionality and to avoid cost overruns and schedule delays in the SEC's efforts related to this mission-essential system.

What We Recommended

We made nine recommendations, including that the SEC more clearly define the EDGAR system governance structure; enhance the relevant lessons learned process; improve EDGAR system scope management processes; ensure the EDGAR system engineering contractor complies with earned value management requirements and performance expectations; update the EDGAR change management policies and procedures; and address constraints impacting the timely completion, review, and approval of ERD contract deliverables. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action. This report contains non-public information about the SEC's EDGAR system. We redacted (deleted) the non-public information to create this public version.

What We Found

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. Our audit included reviewing a non-statistical sample of 6 of the 29 releases (or about 21 percent) deployed by the SEC to enhance the EDGAR system between October 1, 2013, and September 30, 2016. We also interviewed personnel and reviewed program documentation to assess the planning and governance of the SEC's EDGAR Redesign (ERD) program. 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, needs 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;
- 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 ERD program governance and planning.

In addition, during our audit, two other matters of interest that did not warrant recommendations came to our attention. The first matter related to two systems the SEC used for enterprise configuration management, including to manage the configurations of the EDGAR system. We determined that OIT miscategorized one of the two systems, and did not clearly define the other system as a component of the EDGAR system authorization boundary. The second matter related to potential negative impacts on system operations of ongoing EDGAR system enhancements resulting from rules adopted by the Commission. We discussed these matters with agency management for their consideration.

For additional information, contact the Office of Inspector General at (202) 551-6061 or https://www.sec.gov/oig.

TABLE OF CONTENTS

Figures and Table

Appendices

ABBREVIATIONS

ANSI/EIA-748	American National Standards Institute/Electronic Industry Alliance Standards 748
(b)(7)(E) [redacted]	[redacted]
(b)(7)(E) [redacted]	[redacted]
COO	Chief Operating Officer
EDGAR	Electronic Data Gathering, Analysis, and Retrieval System
ERD	EDGAR Redesign
ERS	EDGAR Requirements Subcommittee
EVM	earned value management
(b)(7)(E) [redacted]	[redacted]
FY	fiscal year
GAO	U.S. Government Accountability Office
GSA 18F	U.S. General Services Administration 18F Consulting Services
GSS	General Support System
IT	information technology
LOE	level of effort
NIST	National Institute of Standards and Technology
(b)(7)(E) [redacted]	[redacted]
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OSI	Office of Strategic Initiatives
PCR	programming change request
(b)(7)(E) [redacted]	[redacted]
(b)(7)(E) [redacted]	(b)(7)(E) [redacted]
SEC or agency	U.S. Securities and Exchange Commission
SP	Special Publication
(b)(7)(E) [redacted]	(b)(7)(E) [redacted]

Background and Objectives

Background

The U.S. Securities and Exchange Commission's (SEC or agency) ability to fulfill its mission—protecting investors, facilitating efficient markets, and promoting capital formation—is in part, dependent on the successful operation of the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system. According to the SEC's website, the EDGAR system's primary purpose is to "increase the efficiency and fairness of the securities market for the benefit of investors, corporations, and the economy by accelerating the receipt, acceptance, dissemination, and analysis of time-sensitive corporate information filed with the agency." EDGAR receives more than 700,000 disclosure documents every year from publicly traded companies, investment companies, and individuals who are required by Federal securities laws to file forms with the SEC. According to SEC officials, if EDGAR were to fail, companies and other persons would be unable to satisfy their legal obligations to file, investors would be unable to have ready access to information they need to make investment decisions, and the public's confidence in the SEC's ability to fulfill its mission would be deeply shaken. Furthermore, the SEC consistently spends over $14 million[1] a year on the EDGAR system, or about 6 percent of the agency's information technology (IT) budget. These costs cover both ongoing operations and enhancements to the current EDGAR system. Separately, since fiscal year (FY) 2014, the agency has spent at least $3.4 million on efforts to redesign the EDGAR system.

EDGAR system enhancements—which the SEC considers major IT investments[2]—are regularly scheduled changes to the existing, legacy EDGAR platform. Multiple times each year, the SEC implements EDGAR system enhancements to support the requirements of the SEC's regular rulemaking, including requirements that new rules impose on registrants. While EDGAR system enhancements focus on the functionality of the current system, the EDGAR Redesign (ERD) program is a multi-year, cross-agency initiative aimed toward delivering a new electronic disclosure solution to replace the current system. Around February 2015, the SEC decided to extract the ERD program from the umbrella of EDGAR Modernization[3] and created a distinct program in recognition of the strategic significance and importance of the redesign effort and a desire to give it the appropriate level of visibility, clarity, and identity.

[1] This amount does not include overhead costs attributed to the EDGAR system.

[2] According to Office of Management and Budget (OMB) Circular A-11, *Preparation, Submission, and Execution of the Budget* (July 2016), a major IT investment is one that requires special management attention because of its importance to an agency's mission or the magnitude of the investment.

[3] EDGAR Modernization is a broad initiative, which until September 2014, included efforts to enhance the EDGAR system and replace it.

According to OMB, “Federal [IT] projects too often cost more than they should, take longer than necessary to deploy, and deliver solutions that do not meet our business needs.”[4] Moreover, OMB stated that “the large-scale modernization efforts undertaken by Federal agencies are leading to complex project management requirements that are difficult to manage.” The U.S. Government Accountability Office (GAO) has also reported that Federal IT investments too frequently fail or incur cost overruns and schedule slippages while contributing little to mission-related outcomes. According to GAO, these investments often suffer from a lack of disciplined and effective management, such as project planning, requirements definition, and program oversight and governance.[5] Therefore, a disciplined process for managing the enhancements and redesign of the EDGAR system is necessary to ensure adequate system functionality and to avoid cost overruns and schedule delays in the SEC’s efforts related to this mission-essential system.

History and Purpose of the EDGAR System. The SEC implemented the EDGAR system in 1992, although development of an “electronic library” began almost a decade before.[6] Since 1996, the SEC has required all domestic public companies to make their filings electronically through the system, absent an exemption.[7] The EDGAR system provides the capability for corporate, public, and private information to be assembled, received, accepted, and analyzed by SEC personnel, then disseminated immediately to the public. The system also allows SEC personnel to query all submission/entity-related information, enter data into the system to process paper submissions, upload related materials for submissions, make private correspondence and uploads public, generate and disseminate effectiveness orders, and update previously accepted submissions.

The EDGAR system (b)(7)(E) [redacted] called EDGAR Fee Momentum. EDGAR system processing is performed using several platforms and operating systems. In addition, the EDGAR system uses (b)(7)(E) [redacted] to allow filers to submit filings to the SEC, get status

[4] OMB Memorandum M-10-26, *Immediate Review of Financial Systems IT Projects*; June 28, 2010.

[5] 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).

[6] According to a May 2016 speech by SEC Commissioner Kara Stein, the SEC began building an “electronic library” in 1984. The agency awarded the first contract to build the EDGAR system, as a source of information for investors, in 1989.

[7] The Securities Act of 1933 regulates public offerings of securities, requiring that issuers register securities with the SEC and provide certain disclosures. Securities Act of 1933, Pub. L. No. 73-22, 48 Stat. 74 (1933) (codified as amended at 15 U.S.C. §§ 77a -77aa). The Securities Exchange Act of 1934 established the SEC and provided it with broad authority over all aspects of the securities industry, including the power to require periodic reporting of information by companies with publicly traded securities. Securities Exchange Act of 1934, Pub. L. No. 73-291, 48 Stat. 881 (codified as amended at 15 U.S.C. §§ 78a -78qq). Today, EDGAR filings are disseminated electronically and are displayed on the SEC’s website (*www.sec.gov*). See the SEC’s Regulation S-T, *General Rules and Regulations for Electronic Filings*, codified at 17 C.F.R. part 232.

on filings, and maintain company information.[8] The SEC uses (b)(7)(E) [redacted] to support the SEC's acceptance and review of corporate filings.[9] According to SEC officials, while the agency has made ongoing enhancements and improvements, the EDGAR system remains a complex, monolithic system architected and designed in the 1990s.

In 1999, the SEC proposed and adopted rules to modernize the EDGAR system to accommodate changes in technology since the system was developed.[10] Since 1999, the SEC has continued to modernize the system and add functionalities to address the increasing complexity and volume of filings submitted to the agency. The SEC implements these system enhancements through three types of EDGAR system releases: (1) standard (or quarterly), (2) emergency, or (3) break-fix.[11] With the deployment of each release, the SEC typically addresses multiple programming change requests (PCRs) to enhance the EDGAR system.

While the SEC continues to enhance the EDGAR system, in September 2014, the agency launched a "multi-year initiative to develop the next generation electronic disclosure system," called the ERD program. The intent of the ERD program is to create a new, modernized system that will, among other things:

- meet requirements for real-time system updates,
- reduce filer burden by providing simplified search and filing options based on filer experience,
- improve data capture by moving to structured formats for various SEC forms that will reduce the burden of producing and consuming the data, and
- limit the long-term costs of operating and maintaining the system.

Figure 1 depicts some of the key dates and events from initial implementation of the EDGAR system to the present system.

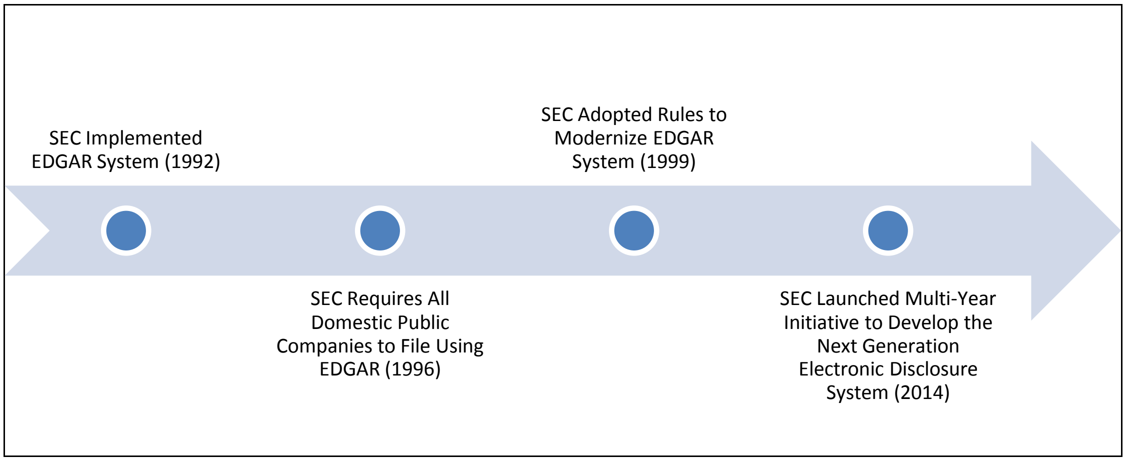
[8] (b)(7)(E) [redacted]

[9] (b)(7)(E) [redacted]

[10] SEC, *Rulemaking for EDGAR System*, Federal Register, Vol. 64, No. 50; March 16, 1999. See also *Final Rule: Rulemaking for EDGAR System*.

[11] A standard release is a change to alter the system. An emergency release is a change that must be introduced as soon as possible; for example, to resolve a major incident or implement a security patch. A break-fix release is a change to correct a defect discovered in the production environment.

Figure 1. Timeline of Key EDGAR System Dates and Events


SEC Implemented EDGAR System (1992)
SEC Requires All Domestic Public Companies to File Using EDGAR (1996)
SEC Adopted Rules to Modernize EDGAR System (1999)
SEC Launched Multi-Year Initiative to Develop the Next Generation Electronic Disclosure System (2014)

Source: Office of Inspector General (OIG)-generated based on SEC reporting.

Responsible Organizations. The SEC's Office of Information Technology (OIT), through its EDGAR Development and EDGAR Operations branches, has provided direction on most EDGAR-related matters, including EDGAR system enhancements. OIT's EDGAR Development Branch oversees enhancements and updates to the EDGAR system. This branch also oversees the EDGAR system engineering contractor, (b)(7)(E)[12] and the EDGAR independent verification and validation contractor, (b)(7)(E)[13] (b)(7)(E) works with OIT personnel to develop system modifications, and has primary responsibility for developing EDGAR system enhancements, testing all code changes, and managing the code baseline. (b)(7)(E) serves as an independent reviewer of (b)(7)(E) deliverables and may test each EDGAR system release for SEC acceptance.

OIT's EDGAR Development Branch partners with OIT's EDGAR Operations Branch to ensure that new software updates to the system are supported after transition to the operating environment. The EDGAR Operations Branch is responsible for keeping EDGAR's "lights on" by maintaining the hardware and base software on the EDGAR system platforms. In addition, the EDGAR Operations Branch is responsible for updating the EDGAR system environments to the latest versioning required by OIT's Office of Information Security. Furthermore, the EDGAR Operations Branch performs application maintenance, which includes fixing code defects identified by the business

[12] The SEC awarded the (b)(7)(E) contract (contract number (b)(7)(E)) on (b)(7)(E). The initial base period of this firm-fixed price with award fee contract was 13 months, with four 1-year option periods. The initial base period award amount totaled $8,159,359.60. The contract includes similar amounts for each option year.

[13] The SEC awarded the (b)(7)(E) contract (order number (b)(7)(E)) under U.S. General Services Administration Schedule (b)(7)(E) on (b)(7)(E). The base year period of performance was (b)(7)(E), with four 1-year option periods. EDGAR independent verification and validation services are based on the schedule's specified labor rates, with a base year not-to-exceed amount of $712,538.80. The contract includes similar not-to-exceed amounts for each option year.

or filing community through software problem reports that are outside of (b)(7)(E) [redacted] warranty period.

In addition, the SEC established the EDGAR Requirements Subcommittee (ERS), in part, to provide control over new requirements to the EDGAR system and to act as a clearinghouse for EDGAR system enhancements. The ERS is composed of stakeholders from multiple SEC divisions and offices.[14]

Figure 2 depicts the SEC's EDGAR system enhancement process, including the roles of the responsible organizations discussed above.

Figure 2. (b)(7)(E) [redacted]

(b)(7)(E) [redacted]

(b)(7)(E) [redacted]

Until recently, various senior staff within the SEC's Office of the Chairman (previously referred to as the Office of the Chair) served as the EDGAR system's nominal business owner. According to SEC officials, without a business owner in the SEC's permanent organizational hierarchy, no senior leader viewed it as his or her primary job to provide leadership, vision, and strategic direction for the EDGAR system's continued success. As a result, responsibility for managing the system was largely shouldered by OIT, as previously described. Given the importance of the EDGAR system to the agency's

[14] The ERS is composed of stakeholders from the following SEC divisions and offices: Division of Corporation Finance, Division of Economic and Risk Analysis, Division of Enforcement, Division of Investment Management, Division of Trading and Markets, Office of Compliance Inspections and Examinations, Office of Financial Management, and OIT.

mission, in June 2017, the SEC established within the Office of Strategic Initiatives (OSI) the EDGAR Program Office. Among other things, OSI is responsible for partnering with OIT's EDGAR Development and EDGAR Operation branches to develop and deploy technical solutions addressing system stakeholders' requirements or change requests. The OSI Director now serves as the EDGAR system's business owner and Chair of the ERS.

Furthermore, in February 2015, the former SEC Chief Operating Officer (COO), citing the strategic importance of ERD and the need to involve key SEC stakeholders, moved the oversight and authority of the ERD program from OIT to the OSI Director.[15] In May 2015, the former COO approved a charter that established the ERD Oversight Board. The objective of the ERD Oversight Board is, in part, to provide oversight, input, review and acceptance of artifacts, approaches, recommendations, and, ultimately, the final functional requirements in support of ERD.

Objectives

Our overall objective was to determine whether the SEC established effective controls over EDGAR system enhancements and redesign efforts. Specifically, we sought to determine whether the SEC has effective:

1. controls to ensure the agency completes EDGAR system enhancements as planned and in accordance with the SEC's performance and budget goals;

2. controls to ensure that the agency implements EDGAR system enhancements in compliance with Federal and SEC change management controls; and

3. planning and governance controls to ensure that the ERD program meets agency needs.

Our audit scope covered EDGAR system enhancements implemented in FYs 2014, 2015, and 2016, and the activities of the ERD program from FY 2014 through February 2017. To address concerns that came to our attention during the audit, we increased our scope to include ongoing EDGAR system enhancements (b)(7)(E) [redacted] (See "Other Matters of Interest" section of this report).

To address our objectives, we reviewed a non-statistical sample of 6 of the 29 releases (or about 21 percent) deployed by the SEC to enhance the EDGAR system between October 1, 2013, and September 30, 2016. We also reviewed one PCR from each of

[15] The COO oversees both OIT and OSI.

[16] (b)(7)(E) [redacted]

the releases in our sample. To assess the SEC's management of the items in our sample, we (1) interviewed OIT officials and SEC stakeholders, (2) reviewed release and PCR documentation, and (3) assessed associated performance and change management attributes.

To assess the SEC's management of contractors involved in EDGAR operations, enhancements, and redesign, we reviewed relevant contract files and evidence of contractor performance. We also interviewed OSI personnel and reviewed program documentation to assess the planning and governance of the ERD program.

Appendices I and II include additional information about our objectives, scope, and methodology; our review of internal controls; prior coverage; and applicable Federal laws and guidance and SEC regulations, policies, and procedures.

Results

Finding 1: The SEC's Governance of EDGAR System Enhancements Needs Improvement

The SEC's governance of EDGAR system enhancements, including the governance and operation of the ERS and the EDGAR system enhancement lessons learned process, needs improvement to ensure agency performance and budget goals are achieved. Specifically, we determined that the ERS structure and operations during our scope period did not reflect Federal and industry guidance for effective IT investment management. In addition, stakeholders from SEC divisions and offices were not involved in the lessons learned process, and OIT officials did not perform post-implementation reviews to confirm that changes to the EDGAR system were implemented as approved and did not negatively impact the system's security. As a result, the SEC may not fully comply with applicable Federal law and guidance, including the Clinger-Cohen Act, OMB Circular A-11, GAO's *IT Investment Management Framework*, and guidance from the National Institute of Standards and Technology (NIST). In addition, the SEC may not implement EDGAR system enhancements cost effectively and based on agency-wide priorities. Finally, the SEC may be limited in the amount and scope of information available to improve the EDGAR system release management process.

Improvements Are Needed in the Governance and Operation of the ERS. The governance and operation of the ERS are in need of improvement to ensure adequate controls exist to maximize value, and to assess and manage IT acquisitions risks. OIT established the ERS, in part, to provide control over new requirements for the EDGAR system. According to the ERS's charter, the subcommittee acts as a clearinghouse for all activities related to developing and modifying the EDGAR system, including prioritizing new requirements and reviewing and prioritizing EDGAR system releases and their content. Federal requirements and guidelines emphasize the role an effective IT management structure plays in maximizing the value, assessing, and managing the risks of IT acquisitions.[17] However, we determined that during our scope period the

[17] The Clinger-Cohen Act of 1996 requires Federal agencies to establish a process for selecting, managing, and evaluating IT investments. GAO's *Information Technology Investment Management, A Framework for Assessing and Improving Process Maturity*, GAO-04-394G, Version 1.1, March 2004 (*IT Investment Management Framework*) also recommends that agencies define and establish an appropriate IT investment management structure. Specifically, GAO recommends, among other things, that: (1) organizations institute an IT investment management structure, such as an enterprise-wide IT investment board composed of senior executives from IT and business units, to oversee and select IT projects; (2) board members have sufficient knowledge; (3) organizations define each investment board's responsibilities and operating and decision making processes; and (4) organizations define the criteria for analyzing, prioritizing, and selecting new IT investment opportunities, and provide data on actual performance (including cost, schedule, benefit, and risk performance) to the appropriate IT investment board.

ERS structure did not reflect Federal and industry guidance for effective IT investment management. Specifically, we found that:

- the ERS was not composed of senior officials representing SEC divisions and offices;[18]
- ERS members were not always knowledgeable about the IT processes or activities related to the EDGAR system enhancements discussed during ERS meetings, and some ERS members left the subcommittee citing the technical nature of the meetings;
- ERS members' roles, responsibilities, and processes to prioritize change requests for inclusion in EDGAR releases, or to approve or reject change requests were not fully defined or documented; and
- ERS members may not have had sufficient cost and corrective action status information to make informed decisions.

The ERS membership composition and ERS members' IT knowledge were inadequate, in part, because the SEC had not established an EDGAR system business owner who was familiar with the system and could represent all the SEC divisions and offices' rulemaking and enhancement requests. Also, by design, OIT officials expected each ERS member to be knowledgeable of his or her division's or office's business processes, but not necessarily knowledgeable of IT processes. In addition, OIT officials stated that ERS member roles and responsibilities did not include a decision-making role or authority to prioritize, approve, or reject EDGAR system change requests because ERS members were not senior officials. Finally, OIT did not clearly report to the ERS cost information related to each release, in part, because EDGAR system enhancements are based on a firm-fixed price contract. With firm-fixed price contracts, the Government pays a fixed price regardless of the actual total costs or the contractor's effectiveness at controlling costs. However, when acquiring services, including engineering and technical services such as EDGAR system enhancements, agency officials need to be able to make sound judgements about requirements and estimated costs.[19]

Improvements Are Needed in the EDGAR System Enhancement Lessons Learned Process. The EDGAR system enhancements lesson learned process is in need of improvement to ensure the agency is able to implement EDGAR enhancements cost effectively and based on agency-wide priorities. According to GAO, building a

[18] In February 2017, a senior agency official (the OSI Director) began overseeing the ERS; however, the ERS members representing SEC divisions and offices remained the same. At the end of our audit, SEC officials told us that the ERS structure will be replaced by a governance structure composed of senior agency officials.

[19] OMB Policy Letter 93-1 (Reissued), *Management Oversight of Service Contracting* (May 1994).

foundation for IT governance involves not only instituting investment boards and selecting investments, but also providing investment oversight, which includes capturing and sharing lessons learned, and post-implementation reviews.[20] According to the EDGAR *Program Management Plan* (dated September 2014), following each major system release, OIT holds a lessons learned session with all release stakeholders to capture best practices and lessons learned. This process aligns with applicable Federal requirements and guidance.[21] However, for 4 of the 6 releases we reviewed (or about 67 percent), OIT did not document lessons learned. For the remaining two releases in our sample, OIT documented lessons learned; however, stakeholders from SEC divisions and offices were not involved in the lessons learned process. Furthermore, OIT officials did not perform post-implementation reviews for all six releases in our sample to confirm that changes to the EDGAR system were implemented as approved and did not negatively impact the system's security.

OIT did not consistently capture and share lessons learned, in part, because OIT did not fully define the lessons learned process to include capturing feedback from and communicating lessons learned to stakeholders from SEC divisions and offices for each release. In addition, OIT did not perform post-implementation reviews because OIT did not define a process to consistently perform such reviews after each release deployment.

The weaknesses we observed in the governance and operation of the ERS and in the lessons learned process challenge the SEC's ability to fully comply with applicable Federal law and guidance, including the Clinger-Cohen Act, OMB Circular A-11, GAO's *IT Investment Management Framework*, and NIST guidance. In addition, the agency may not implement EDGAR system enhancements cost effectively and based on agency-wide priorities. Finally, OIT may be limited in the amount and scope of information available to improve the EDGAR system release management process through its lessons learned process.

Recommendations, Management's Response, and Evaluation of Management's Response

To improve the SEC's ability to complete EDGAR system enhancements as planned and in accordance with the agency's performance and budget goals, we recommend

[20] U.S. Government Accountability Office, *Information Technology HUD Can Take Additional Actions to Improve Its Governance* (GAO-15-56, December 2014).

[21] According to OMB Circular A-11, at a minimum, a post-implementation review team should evaluate stakeholder and customer/user satisfaction with the end-product, mission/program impact, and technical capability. GAO's *IT Investment Management Framework* also states that a post-implementation review typically identifies lessons learned from an investment and determines whether the benefits anticipated in the business case for the investment have been achieved. Finally, NIST Special Publication (SP) 800-128, *Guide for Security-Focused Configuration Management of Information Systems* (August 2011), states that security impact analysis procedures include requirements for post-implementation review to confirm that the change was implemented as approved and that no additional security impact resulted.

that the Acting Chief Operating Officer ensure that the Office of Strategic Initiatives and the Office of Information Technology coordinate to:

Recommendation 1: Clearly define the EDGAR system governance structure to ensure (a) the governance structure is composed of senior officials who are knowledgeable about the information technology processes or activities related to EDGAR system enhancements; (b) roles, responsibilities, and processes to prioritize, approve, and reject EDGAR enhancements are fully defined and documented; and (c) enhancement cost information and corrective action status is provided to members of the governance structure to make informed decisions.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Strategic Initiatives and Office of Information Technology have begun defining a new EDGAR system governance structure composed of senior officials knowledgeable about the information technology processes related to EDGAR system enhancements. The Acting Chief Operating Office further stated that work is underway to fully define and document the roles, responsibilities, and processes to prioritize, approve, and reject EDGAR enhancements. Also, the Office of Strategic Initiatives and Office of Information Technology will work together to develop a comprehensive communication protocol. Management's complete response is reprinted in Appendix III.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 2: Enhance the EDGAR lessons learned process to ensure lessons learned are documented, and the process includes all stakeholders and post-implementation reviews to confirm that releases implemented into production did not negatively impact the EDGAR system security posture.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation and stated that the EDGAR lessons learned process has been enhanced to ensure lessons learned are documented and include all stakeholders. Also, the Office of Strategic Initiatives and Office of Information Technology will work together to develop, document, and implement a post-implementation assessment process to confirm that releases implemented into production do not negatively impact the EDGAR system security posture. Management's complete response is reprinted in Appendix III.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Finding 2: OIT Did Not Consistently Manage the Scope of EDGAR System Releases

OIT did not consistently manage the scope of EDGAR system releases to ensure EDGAR system enhancements met SEC needs or priorities. Specifically, based on our review of a sample of six releases deployed by the SEC to enhance the EDGAR system between October 1, 2013, and September 30, 2016, we determined that OIT did not consistently define, document, and track the scope of EDGAR releases and changes to the releases' scope. This occurred, in part, because established guidance did not fully define the scope management process, including mechanisms or processes to properly manage and communicate changes in the scope of EDGAR releases. As a result, EDGAR stakeholders may not have a clear understanding of the work required to achieve the expected benefits.

According to GAO, a program's scope represents the work required to deliver a benefit (major product, service, or result), and a defined scope provides the context and framework for reporting, tracking, and controlling program activities.[22] Scope management includes defining, assessing, and documenting the essential aspects to accomplish, and developing a plan for managing, documenting, and communicating scope changes. According to EDGAR release documents, the scope of an EDGAR release details the content or specific change requests (that is, business requirements) to be implemented by the release. We reviewed 6 of the 29 system releases (or about 21 percent) deployed by the SEC to enhance the EDGAR system between October 1, 2013, and September 30, 2016, including 4 standard releases and 2 emergency releases, and determined that OIT did not consistently define, document, and track the scope of the releases, including documenting changes in scope. Specifically, we found that OIT did not:

- consistently document the approved baseline scope for two of the four standard releases, and for both of the emergency releases we reviewed;
- consistently document required approvals and the basis for changes to the scope of each of the four standard releases we reviewed;
- perform and document an impact analysis of changes made to each release's scope, as required by EDGAR system release process documentation; and
- consistently track the reported level of effort (LOE) or actual hours spent by (b)(7)(E) on each release, which is necessary for the SEC to make sound judgements in selecting the EDGAR system enhancements to implement and to properly assess contractor performance.

[22] U.S. Government Accountability Office, *Joint Information Environment DOD Needs to Strengthen Governance and Management* (GAO-16-593, July 2016).

OIT did not consistently manage the scope of EDGAR system releases, in part, because established guidance did not fully define applicable requirements.[23] For example, OIT guidance described the process for changing the scope of an EDGAR system release by adding or removing PCRs. However, OIT guidance did not address the process for adding or removing other types of change requests (such as software problem requests or document change requests), which are generally included in the scope of an EDGAR system release. In addition, the guidance did not define requirements for documenting the basis for changing the scope of an EDGAR system release, or the authorization needed to change the scope of an EDGAR system release by adding or removing change requests.

Also, OIT officials stated that, at EDGAR Change Control Board meetings, they discussed changes in the scope of system releases. However, the meeting minutes did not always capture information about the changes discussed. Finally, during our scope period, OIT did not have a mechanism to perform and document impact analyses for changes in the scope of EDGAR system releases. Similarly, OIT did not have a process to validate the contractor's LOE estimates related to system release scope changes.

Without fully defining and consistently implementing EDGAR system release scope management processes, OIT is limited in its ability to effectively manage the scope of releases and efficiently assign PCRs to standard releases. Furthermore, according to the *EDGAR Program Management Plan*, "allowing informal changes that are not communicated to and evaluated by all managers and teams can impact project and release schedules resulting in customer dissatisfaction and financial penalties to (b)(7)(E) [redacted] and the EDGAR team."[24]

Recommendation, Management's Response, and Evaluation of Management's Response

To improve the SEC's management of the scope of EDGAR system releases, including changes in scope, we recommend that the Acting Chief Operating Officer ensure that the Office of Strategic Initiatives and the Office of Information Technology coordinate to:

Recommendation 3: Clarify, document, and implement EDGAR system scope management processes that ensure (a) consistent documentation of baseline release scope, (b) consistent documentation of approval and basis for changes to each release's scope, (c) an impact analysis is performed and documented for changes to each release's scope, and (d) consistent tracking and validation of reported level of effort or actual hours spent by the contractor on each release.

[23] OIT's guidance for tasks involved in managing the scope of EDGAR system releases includes *Change Management Process Description* and *Release Planning and Deliverables Standard Operating Procedures.*

[24] The EDGAR team includes (b)(7)(E) [redacted], and the OIT EDGAR Development Branch.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Strategic Initiatives and Office of Information Technology will work together to continue improvements to EDGAR system scope management processes. In addition, the Office of Strategic Initiatives and Office of Information Technology will work together to continue to ensure consistent tracking and validation of contractor level of effort estimates and actual hours spent on each release. Management's complete response is reprinted in Appendix III.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Finding 3: Improvements Are Needed in the SEC's Management of the EDGAR System Engineering Contract

The SEC should improve its management of the EDGAR system engineering contract with (b)(7)(E) [redacted]. Specifically, we reviewed contract and award fee[25] documents and determined that the SEC did not complete four of five required steps to ensure (b)(7)(E) [redacted] properly used earned value management (EVM) to monitor the agency's investments in EDGAR system enhancements, as required by OMB.[26] In addition, OIT did not effectively use contract performance metrics to manage (b)(7)(E) [redacted] performance, and the EDGAR system performance requirements specified in the (b)(7)(E) [redacted] contract were not consistent with requirements specified in another SEC contract. According to OIT officials, EVM is not as effective for firm-fixed price contracts such as the (b)(7)(E) [redacted] contract. In addition, OIT did not use certain contract performance metrics to manage (b)(7)(E) [redacted] performance because OIT had not established processes or controls for each metric. As a result, the SEC accepted unreliable EVM data and paid (b)(7)(E) [redacted] a total of $228,750 in award fees for FY 2015 and FY 2016, but did not monitor (b)(7)(E) [redacted] performance as effectively as planned. Also, without consistently defined system performance requirements, the SEC may not be able to effectively monitor contractor adherence to contractual terms.

The SEC Did Not Complete Most of the Required Steps To Ensure (b)(7)(E) [redacted] Properly Used EVM. Because OIT considers EDGAR system enhancements major IT investments, the SEC is required by OMB Circular A-11 (and in accordance with Federal Acquisition Regulation, Subpart 34.2) to monitor the investments' performance using an EVM system that complies with American National Standards Institute/Electronic Industry Alliance Standard 748 (ANSI/EIA-748).[27] When implemented properly, an EVM system measures progress against a baseline and provides an early warning of cost overruns and schedule delays. To implement EVM, OMB requires agencies to take the following five steps:[28]

[25] "Award fee" and "incentive fee" are used interchangeably within this report.

[26] OMB Memorandum M-05-23, *Improving Information Technology (IT) Project Planning and Execution* (August 2005).

[27] ANSI/EIA-748, *Earned Value Management Systems*, describes guidelines to provide strong benefits for program or enterprise planning and control. The processes include integration of program scope, schedule, and cost objectives; establishment of a baseline plan for accomplishment of program objectives; and use of earned value techniques for performance measurement during the execution of the program.

[28] OMB Memorandum M-05-23 lists the five steps to fully implement an EVM system and recommends the use of the National Defense Industrial Association guide to conduct compliance and integrated baseline reviews.

Step 1. Develop EVM policies.

Step 2. Include EVM system requirements in contracts for major IT projects.

Step 3. Provide documents demonstrating that contractor EVM systems comply with ANSI/EIA-748.

Step 4. Perform periodic surveillance or compliance reviews of contractor EVM systems to ensure the systems continue to meet ANSI/EIA-748.

Step 5. Perform integrated baseline reviews on contracts with EVM requirements before and after award, as appropriate.

We determined that the SEC completed Step 2 above by including EVM clauses in the agency's contract with (b)(7)(E). However, the SEC did not complete the other four required steps to ensure (b)(7)(E) properly used EVM to monitor the agency's investments in EDGAR system enhancements. Specifically, we found the following:

- The SEC had not developed and implemented comprehensive EVM policies (Step 1 above). Although SEC policy[29] states that the SEC's Capital Planning and Investment Control process shall use, where appropriate, an EVM process that is compliant with OMB requirements, the agency does not have a roadmap for implementing those requirements.

- OIT did not determine whether (b)(7)(E) EVM system complied with ANSI/EIA-748, or conduct periodic surveillance or compliance reviews of (b)(7)(E) EVM system (Steps 3 and 4 above). OIT provided a high-level description of the contractor's EVM process. However, the document provided was not sufficiently detailed as it did not describe the contractor's activities to address each of the management concepts used to verify ANSI/EIA-748 compliance. For example, the document did not address (b)(7)(E) organizational structure (including subcontractor management responsible for accomplishing the work), accounting considerations, or budget allocation and resource planning.

- OIT did not perform integrated baseline reviews of (b)(7)(E) EVM requirements before or after contract award (Step 5 above). One OIT official stated that EVM is not as effective for firm-fixed price contracts such as the SEC's contract with (b)(7)(E). However, OMB Circular A-11 states EVM shall be used on firm-fixed price contracts or task orders that meet the major acquisition threshold if the contract or task order contains a significant amount of development effort.

[29] SEC Administrative Regulation 24-02, *Information Technology Capital Planning and Investment Control*, Revision 2.1, May 2017.

Because the SEC did not complete all required EVM steps, the agency accepted unreliable EVM data in (b)(7)(E) [redacted] periodic reports and, therefore, did not monitor its investments in EDGAR system enhancements or (b)(7)(E) [redacted] performance as effectively as planned. Specifically, (b)(7)(E) [redacted] EVM system provides the SEC information about the budgeted cost of EDGAR system releases and states that costs are based largely on the LOE for each PCR in a release. However, we determined that (b)(7)(E) [redacted] reported LOEs may differ significantly from actual hours needed for each release. For example, (b)(7)(E) [redacted] estimated that 18,826 hours would be needed for Release 16.1 (one of the releases in our sample). However, the release actually required 27,786 hours (or about a 48 percent difference). Despite the increased LOE for Release 16.1, (b)(7)(E) [redacted] reported completing the release on schedule and under budget in its July 13, 2016, Quarterly Status Report.

OIT Did Not Effectively Use Contract Performance Metrics To Manage (b)(7)(E) [redacted] Performance. We reviewed the SEC's EDGAR system engineering contract with (b)(7)(E) [redacted] and related award fee documents and found that, in accordance with OMB guidance,[30] the contract includes the following four performance metrics as monetary incentives for (b)(7)(E) [redacted] to achieve certain performance objectives: (1) software quality, (2) on-time delivery of release documentation, (3) adherence to release schedule estimates, and (4) system performance and response time requirements. In addition, the Award Fee Determination Plan included in the contract set forth the basic procedures and criteria for the periodic evaluation and award fee determination for (b)(7)(E) [redacted]. However, OIT did not effectively use these performance metrics to manage (b)(7)(E) [redacted] performance and determine the award fee earned in FY 2015 and FY 2016.[31] For example, we found that OIT did not:

- consider in its FY 2015 and FY 2016 award fee calculations 8 releases (including 2 minor releases and 6 emergency and urgent releases) out of 21 releases deployed by (b)(7)(E) [redacted];
- consistently track whether (b)(7)(E) [redacted] delivered release documentation on time;
- clearly document original, expected, and actual dates used to track (b)(7)(E) [redacted] adherence to the release schedule; or

[30] According to an OMB Memorandum entitled *Appropriate Use of Incentive Contracts* (December 4, 2007), agencies should use incentive fee contracts to achieve specific performance objectives, such as delivering products and services on time, within cost goals, and with promised performance outcomes. In addition, OMB states that acquisition policies should ensure that incentive fees (1) are linked to acquisition outcomes such as cost, schedule, and performance results; and (2) are not earned if the contractor's performance is judged to be below satisfactory or does not meet the basic requirements of the contract.

[31] As previously stated, the SEC awarded the (b)(7)(E) [redacted] contract on (b)(7)(E) [redacted]. The agency paid award fees after the end of the base period and the first option year ((b)(7)(E) [redacted], respectively). We reviewed available award fee data from these first two award fee periods.

- develop a mechanism or measures necessary to link incentive fees to system response time requirements.

According to OIT officials, when preparing (b)(7)(E) award fee calculations in FY 2015 and FY 2016, OIT officials considered only standard releases. OIT officials did not include the eight releases we identified as missing because those releases addressed emergency fixes or patches. However, the contract does not explicitly preclude OIT from including such releases in its calculations of contractor award fee. According to the contract, "every release of EDGAR must demonstrate that quality code has been produced that is defect free," and "every release of EDGAR must ensure the required documentation is updated and delivered on time." The contract also states, "the schedule for every release will be tracked for adherence," and requires that the contractor, accompanied by the SEC, test and document system response times before and after each release deployment. In addition, OIT did not effectively assess the contractor's performance against each of performance metrics specified in the contract because OIT had not established processes or controls for each metric. According to OIT officials, OIT recently implemented a release closeout report to help determine whether (b)(7)(E) delivers release documentation on time. However, the new process is not yet formalized in OIT's guidance documentation.

As a result, OIT paid (b)(7)(E) a total of $228,750 in award fees for FY 2015 and FY 2016,[32] but did not monitor (b)(7)(E) performance as effectively as planned to ensure the contractor achieved the desired performance objectives.

EDGAR System Performance Requirements Are Inconsistent. Since (b)(7)(E), the SEC has contracted with (b)(7)(E) to operate and maintain agency software applications, including the EDGAR system. We compared EDGAR system performance requirements specified in the SEC's contracts with (b)(7)(E) and (b)(7)(E) and found that the requirements are inconsistent. For example, (b)(7)(E) According to both contracts, the contractor shall ensure that response time requirements are met.

The (b)(7)(E) contract also states that the contractor must test and document system response times before and after each system release to demonstrate that there has been no degradation in performance after the deployment of each release. Without consistently defined system performance requirements, the SEC may not be able to effectively monitor the contractors' adherence to contractual terms. In addition, the SEC may not be able to determine whether there has been any degradation in performance after the deployment of each system release. OIT officials told us that they would research the inconsistencies in contractual terms we identified.

[32] The total maximum award fee available for FY 2015 and FY 2016 was $360,000.

Recommendations, Management's Response, and Evaluation of Management's Response

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 recommend that the Acting Chief Operating Officer ensure that the Office of Acquisitions and the Office of Information Technology coordinate to:

Recommendation 4: Develop and implement a comprehensive earned value management policy specifying the requirements for implementing earned value management for information technology contracts, defining how contractors' earned value management systems will be verified for compliance with the applicable standards, and how integrated baseline reviews will be conducted.

> **Management's Response.** The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Acquisitions and Office of Information Technology will coordinate to clarify the requirements for implementing earned value management on major systems development contracts, and define how contractors' earned value management systems will be verified for compliance with the applicable standards and how integrated baseline reviews will be conducted. Management's complete response is reprinted in Appendix III.
>
> **OIG's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 5: Assess the EDGAR system engineering contractor's earned value management system for compliance with applicable standards.

> **Management's Response.** The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Acquisitions and Office of Information Technology will work together to reevaluate the requirements for earned value management on the EDGAR system engineering contract and, as appropriate, will assess the EDGAR system engineering contractor's earned value management system for compliance with applicable standards. Management's complete response is reprinted in Appendix III.
>
> **OIG's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 6: Define and implement processes to track the EDGAR system engineering contractor's performance that include (a) the full scope of releases deployed by the contractor during each fiscal year; (b) consistent tracking of on-time delivery of release documentation; (c) the documentation of original, expected, and actual dates used to track adherence to the release schedule; and (d) a mechanism or measure to link incentive fees to system response times.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Acquisitions, Office of Information Technology, and Office of Strategic Initiatives will work together to improve the current process for tracking the EDGAR system engineering contractor's performance. Management's complete response is reprinted in Appendix III.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 7: Consistently define the expected EDGAR system response time in agency contracts to operate, maintain, and enhance the EDGAR system.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Information Technology and Office of Acquisitions will coordinate to ensure consistency in the stated requirements for system response time across SEC contracts to operate, maintain, and enhance the EDGAR system. Management's complete response is reprinted in Appendix III.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Finding 4: OIT Did Not Fully and Consistently Implement EDGAR System Enhancements in Compliance with Federal and SEC Change Management Controls

Based on our review of a sample of EDGAR enhancements from FY 2015 and FY 2016, we determined that OIT did not fully and consistently implement EDGAR system enhancements in compliance with Federal and SEC change management controls. Specifically, OIT did not: (1) ensure that EDGAR system emergency releases requiring configuration control were subject to the change management process, (2) ensure that (b)(7)(E) [redacted] performed post-deployment performance testing to confirm that changes to the EDGAR system were implemented as approved and did not negatively impact the system's security, (3) obtain final user acceptance from internal EDGAR system users after implementing system changes, (4) adequately track EDGAR system defects, and (5) periodically review EDGAR system changes to determine whether unauthorized changes had occurred. These weaknesses occurred for a variety of reasons discussed further below. By not fully developing processes to enforce change management controls for EDGAR system enhancements, enhancements may be inconsistently developed, tested, and migrated into the production environment, placing the system at increased risk of unauthorized changes and security threats.

OIT Did Not Ensure That EDGAR System Emergency Releases Were Subject to the Change Management Process. NIST SP 800-128 states "it is incumbent upon information system owners to identify all sources of change to make certain that changes requiring configuration control go through the configuration change control process, ***even if it is after the fact*** [emphasis added]."[33] We interviewed OIT officials and reviewed the two emergency releases within our sample and determined that OIT did not ensure that EDGAR system emergency releases requiring configuration control were subject to a standard configuration change control process, even after the fact. For example, OIT did not consistently document emergency requests or validate the emergency changes. This occurred because OIT did not develop and document a configuration change control process for emergency releases. As a result, OIT did not maintain the standard degree of assurance that configuration controls effectively mitigated risks related to emergency releases. Therefore, emergency releases are at greater risk for negatively impacting the overall performance and security posture of the EDGAR system.

OIT Did Not Ensure That (b)(7)(E) [redacted] Performed Post-Deployment Performance Testing. NIST SP 800-53 recommends, "The organization, after the information system

[33] NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*; August 2011.

is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system."[34] In addition, according to the EDGAR system engineering contract, "the contractor, accompanied by the SEC (when stipulated by the [Contracting Officer's Representative]), must test and document system response times before and after each release to demonstrate that there has been no degradation in performance after the deployment of each release." Finally, OIT's *Release Planning and Deliverables Standard Operating Procedure* states that the post-deployment test analysis report includes pre- and post-release deployment performance test results.[35]

We interviewed OIT officials and reviewed test results for five EDGAR system releases in our sample[36] and determined that OIT did not ensure (b)(7)(E) performed post-deployment performance testing for any of the five releases to confirm that the changes to the EDGAR system were implemented as approved and did not negatively impact the system's security. This occurred because OIT did not develop and document a process to ensure that system performance was not degraded following deployment of each release. As a result, the SEC may lack assurance about whether recently implemented enhancements negatively impacted the EDGAR system. Furthermore, the SEC may be limited in its options to hold (b)(7)(E), as the EDGAR system engineering contractor, responsible for degrading the system's performance or weakening the system's security posture as a result of deployed enhancements.

OIT Did Not Obtain Final User Acceptance From SEC Users of the EDGAR System, After Implementing System Changes. Change management best practices state that, because testing is an iterative process that is generally performed at several levels, it is important that the entity adhere to a formal set of configuration management procedures for approving changes. These procedures should include obtaining final user acceptance only after testing is successfully completed and reviewed by the user.

We determined that OIT did not formally document final user acceptance from SEC users for four of the five releases in our sample. This occurred because OIT did not develop and document a process to ensure EDGAR system changes meet users' requirements. Without obtaining final user acceptance, OIT cannot validate whether a change meets user requirements before releasing the software. Furthermore, fixing defects after release deployment may result in reduced LOE available for future releases and enhancements.

[34] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* Revision 4; April 2013.

[35] *Release Planning and Deliverables Standard Operating Procedure,* January 2015.

[36] In FY 2015, OIT revised its change management controls. Therefore, we excluded from the change management portion of our audit the FY 2014 standard release in our sample.

OIT Did Not Adequately Track EDGAR Defects. According to NIST SP 800-128, the configuration change control process includes verifying that a system change was implemented correctly (that is, without any defects). In addition, NIST SP 800-128 states change control is not complete and a change request not closed until it has been confirmed that the change was deployed without issues.

OIT uses two different reports to track defects identified during testing. However, we determined that OIT did not consolidate or consistently update the two reports for any of the five releases we reviewed to ensure all defects were addressed before the changes were deployed. This occurred because OIT has not developed and documented a process to ensure all defects identified are addressed before deploying an EDGAR system release. As a result, OIT is at greater risk of deploying changes to the EDGAR system with unaddressed defects. Such defects may result in changes not meeting user needs. Furthermore, defects that carry over into production may increase EDGAR system security risk.

OIT Did Not Periodically Review EDGAR System Changes. NIST SP 800-53 states the organization reviews information system changes at a periodicity defined by the organization to determine whether unauthorized changes have occurred. Furthermore, NIST SP 800-128 addresses the need for management to periodically obtain and review monitoring reports to identify unauthorized changes.

According to OIT contract personnel, after (b)(7)(E) [redacted] deployed the EDGAR system releases in our sample, OIT did not periodically monitor the system to determine whether unauthorized changes occurred. OIT contract personnel stated that, during the deployment phase, they have the opportunity to detect anomalies between the planned and actual scope. However, after the release is deployed, OIT did not perform periodic analysis to detect unauthorized changes. This occurred because OIT did not develop and document a process to ensure the detection of unauthorized changes. Monitoring identifies undiscovered/undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes, all of which, if not addressed, can expose organizations to increased risk. Furthermore, unauthorized changes to information systems may be an indication that the systems are under attack or that change management procedures are not being followed. However, because OIT did not periodically review EDGAR system changes, OIT limited its ability to detect these issues.

Recommendation, Management's Response, and Evaluation of Management's Response

To improve the effectiveness of the SEC's EDGAR system change management controls, we recommend that the Office of Information Technology:

Recommendation 8: Update its EDGAR change management policies and procedures to include (a) a configuration change control process for emergency releases, (b) a process to ensure that EDGAR system performance has not degraded following each release deployment, (c) a process to ensure EDGAR system changes meet user requirements before deployment of the change, (d) a process to ensure all defects identified are addressed before deploying a release, and (e) a process to ensure detection of unauthorized changes to the EDGAR system.

Management's Response. The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Information Technology will review and update the EDGAR change management policies and procedures. Management's complete response is reprinted in Appendix III.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Finding 5: Further Improvements Are Needed in the ERD Program's Governance and Planning To Ensure Agency Needs Are Met

Since 2014, the SEC has made several improvements in its planning and governance of the ERD program to meet agency needs. Specifically, SEC officials took steps—including engaging a new contractor— to redirect the ERD program's focus from a technology solutions approach to an agency-wide strategic initiative, with a formal governance and SEC stakeholder participation structure. 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 ERD program's governance and planning. For example, we found that the SEC did not address constraints impacting the ERD program's progress such as OSI's capacity to timely review and approve contractor deliverables, and we noted that the ERD is experiencing delays in developing the requirements necessary to define and deliver a new electronic disclosure solution to replace the EDGAR system.

The SEC has taken steps to improve its ability to develop and implement a new electronic disclosure system that meets agency needs. As further described below, steps taken to improve the ERD program include, but are not limited to:

- reorganizing the EDGAR Modernization program to create a distinct program management approach to the EDGAR redesign portion of the broader initiative,
- contractually changing the ERD program direction from a technology solutions approach to an agency-wide strategic initiative,
- implementing an oversight board comprising SEC executives to provide ERD program oversight and leadership,
- engaging the U.S. General Services Administration's 18F Consulting Services (GSA 18F) to identify EDGAR system stakeholder needs and concerns, and
- initiating ERD functional and non-functional requirements gathering.

In late FY 2014 and under the direction of the former Chief Information Officer, the SEC awarded a time-and-materials contract to (b)(7)(E) [redacted] to review and analyze the current electronic disclosure environment and recommend improvements that would lead to the elimination of complexities and redundancies.[37]

[37] The SEC awarded the (b)(7)(E) [redacted] contract (contract number (b)(7)(E) [redacted]) on (b)(7)(E) [redacted]. The contract became effective on (b)(7)(E) [redacted] The contract was an indefinite delivery/indefinite quantity type with a not-to-exceed amount of $30 million.

Because of the strategic significance and importance of the ERD program, the former COO determined in February 2015 that the ERD program must involve key SEC stakeholders and be led by a senior officer who had full program responsibility. As a result, the former COO moved the oversight and authority of the ERD program—and therefore the management of the (b)(7)(E) contract—from OIT to the OSI Director. The former COO stated at the time that this new governance structure would ensure the ERD program had the appropriate level of senior executive focus, control, and support.

In April 2015, OSI began working with (b)(7)(E) to reorient the contract to better reflect ERD as a strategic initiative and to involve greater interaction with the SEC divisions and offices that use EDGAR regularly. After discussions, on June 18, 2015, (b)(7)(E) agreed to a contract modification memorializing the new direction of the ERD program.

In May 2015, the former COO approved a charter that established the ERD Oversight Board (Board), composed of key ERD stakeholders from SEC divisions and offices. The objective of the Board was, in part, to provide oversight, input, review and acceptance of artifacts, approaches, recommendations, and ultimately the final functional requirements in support of ERD.

After working with (b)(7)(E) on the new initiative and stakeholder interactions for several months, in September 2015, the SEC determined that the modified contract was not effectively achieving the ERD program reorientation desired because the contractor's effort continued to focus on technology rather than the non-technical aspects of the program. In addition, the OSI Director stated that the contract did not address significant needs of the program resulting from:

- the complexity of managing off-site contractors and a time-and-materials based contract,
- the lack of a robust program support function by the contractor,
- the lack of strong strategic thinking by the contractor, and
- a limited number of dedicated Federal staff.

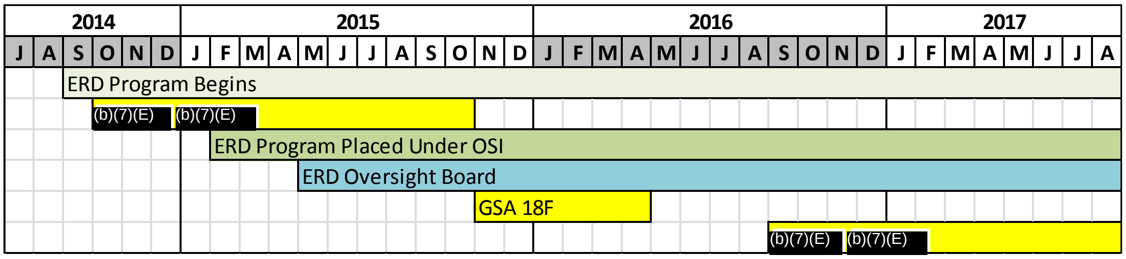
As a result, the agency terminated its contract with (b)(7)(E) for convenience.[38] At the time of the (b)(7)(E) contract's termination, the SEC had spent nearly $3 million. Following the termination of the (b)(7)(E) contract, the OSI Director engaged GSA 18F to identify EDGAR system stakeholder needs and concerns and help the SEC prepare a request for proposal to achieve its vision for the ERD program. This short-term GSA 18F consulting effort took place between November 2015 and April 2016 at a cost of $122,500. After taking into consideration the results of the GSA 18F effort, the SEC

[38] "Termination for convenience" means the exercise of the Government's right to completely or partially terminate performance of work under a contract when it is in the Government's interest.

awarded a new 18-month contract in the amount of $6.1 million to (b)(7)(E) [redacted] on (b)(7)(E).

Figure 3 depicts the key ERD program events described above.

Figure 3. Timeline of Key ERD Program Events



Source: OIG-generated based on information obtained from OSI.

The award of the (b)(7)(E) contract addressed some of the constraints identified by the OSI Director at the time of the SEC's decision to terminate the (b)(7)(E) contract. Specifically, instead of time-and-materials, the (b)(7)(E) contract is firm-fixed price. In addition, (b)(7)(E) approach to gathering ERD requirements involves interviewing dozens of SEC subject matter experts and stakeholders from across the agency and conducting 12 distinct working group cycles based on key EDGAR requirements themes. Furthermore, the (b)(7)(E) contract's final deliverable is the detailed comprehensive functional and non-functional requirements addressing all facets of the new electronic disclosure solution to include business functions, capabilities, processes, technology, and architecture.

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 ERD program's governance and planning. For example, the SEC has not fully addressed identified constraints impacting the ERD program's progress and the agency's decision to redirect the program. When SEC officials made the decision to redirect the ERD program in September 2015, one of the factors cited as impacting the program's success was a limited number of Federal staff dedicated to the program. According to the OSI Director, there are currently 25 percent less Federal staff dedicated to the program now than when the redirection decision occurred. Specifically, the SEC had four dedicated Federal staff assigned to the ERD program at the time SEC officials decided to redirect the program. According to the OSI Director, there are currently three Federal staff dedicated to the ERD program. We also noted that the ERD program is experiencing delays in developing the requirements necessary to achieve the SEC's strategic initiative of defining and delivering a new electronic disclosure solution to replace the EDGAR system.

Specifically, (b)(7)(E) and OSI missed early program documentation completion and approval deadlines established in the (b)(7)(E) contract. For example, OSI approved both the Program Management Plan and Integrated Master Schedule in February 2017, about 2 months behind schedule. Furthermore, (b)(7)(E) completed the first of 12 working group cycles ("as-is" requirements analysis) on May 17, 2017, nearly

2 months behind schedule. As of the beginning of August 2017 (10 months into the 18-month contract), OSI was in the process of reviewing the functional requirements documents (b)(7)(E) [redacted] developed under two additional working group cycles ("submission/form filings" and "filer access management"). According to (b)(7)(E) [redacted] integrated master schedule, these first three working group cycles were to be finished between March 21, 2017, and June 7, 2017.

The Contracting Officer's Representative for the (b)(7)(E) [redacted] contract stated that these documents were delayed, in part, because of OSI's review and approval cycle. In addition, the Contracting Officer's Representative told us that the original schedule depended on the SEC's review of the first two working group cycles and the cycles' outcomes. (b)(7)(E) [redacted] and the Contracting Officer's Representative agreed to revise and re-baseline the schedule to build in more time for OSI to review the deliverables prepared by (b)(7)(E) [redacted]. The revised schedule will not require additional funding.[39]

Recommendation, Management's Response, and Evaluation of Management's Response

To improve the effectiveness of the SEC's EDGAR Redesign program, we recommend that the Acting Chief Operating Officer:

Recommendation 9: Address constraints impacting the timely completion, review, and approval of contractor deliverables, commensurate with the EDGAR Redesign program's strategic significance and importance to the agency.

> **Management's Response.** The Acting Chief Operating Officer concurred with the recommendation and stated that he will work to address any constraints impacting the timely completion, review, and approval of contractor deliverables. Management's complete response is reprinted in Appendix III.
>
> **OIG's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

[39] As of the beginning of August 2017, (b)(7)(E) [redacted] has cumulatively invoiced about $375,600 of the contract's $6.1 million award amount.

Other Matters of Interest

During our audit, two other matters of interest that did not warrant recommendations came to our attention. We discussed these matters with OSI and OIT management for their consideration. These matters are described below.

[redacted] According to OIT staff, for the past 17 years, the SEC has used two systems—[redacted] and [redacted] for enterprise configuration management (that is, change control and version control), including to manage the configurations of the EDGAR system.[40] However, we determined that OIT miscategorized [redacted] and did not clearly define [redacted] as a component of the EDGAR system authorization boundary.[41]

[redacted] OIT categorized [redacted] as a General Support System (GSS) tool even though the system does not meet OIT's criteria for GSS tools. According to OIT guidance,[42] GSS tools are:

> …information worker tools, software applications and supporting minor hardware, such as locally attached devices that exist to perform operations on general data. These tools ***do not act as a system of record for any data***, and the tools operate independently of [any] Major or Minor application. Examples of GSS Tools include office software, add-ons and modules to web browsers or spreadsheets and simple data feeds. ***All security controls are inherited from the GSS*** [emphasis added].

Nonetheless, we found that (1) until June 2017, OIT used [redacted] as the system of record for EDGAR defects, and (2) [redacted] has application-specific access controls, such as separate login credential requirements. Therefore, OIT's categorization of [redacted] as a GSS tool does not comply with OIT guidance. In response, OIT officials stated that "revisions are in progress…to ensure continued clarity" of OIT guidance.

[redacted] We also found that OIT did not clearly define the components of the EDGAR system authorization boundary to include [redacted]. NIST SP 800-53 states organizations should develop and document an inventory of information system components that includes all components within the authorization boundary of the information system. In accordance with NIST guidance, OIT's *Information Security Controls Manual* states, for major applications (like the EDGAR system), the information system owners shall be responsible for developing, documenting, and maintaining an inventory of information system components including all components within the

[40] In June 2017, OIT replaced [redacted] with a new system called [redacted]

[41] OIT has ownership and managerial responsibility of [redacted] and [redacted], including the systems' development, support, and maintenance.

[42] OIT's *Information System Type Categorization*, version 8.2 (undated).

authorization boundary of the information system. OIT's *Information Security Controls Manual* also states that the system security plan shall explicitly define the authorization boundary for the system.

However, (b)(7)(E) [redacted]

We encourage OIT management to continue its efforts to revise OIT guidance to provide clarity on the rationale and documentation required to categorize information systems as GSS tools, and to update the software components section of the EDGAR system security plan.

EDGAR System Enhancements for (b)(7)(E) [redacted] The SEC is developing EDGAR system enhancements (b)(7)(E) [redacted]

During our audit, (b)(6) [redacted] (b)(7)(E) [redacted]

1. (b)(7)(E) [redacted]

2. (b)(7)(E) [redacted]

As a result, we conducted additional interviews, gathered background information, and determined that (b)(6) [redacted] (b)(7)(E) [redacted]

[43] (b)(7)(E) [redacted]

[44] (b)(7)(E) [redacted]

(b)(7)(E) [redacted]

While the SEC has made strides to gather (b)(7)(E) [redacted], the concerns identified (b)(6) [redacted] warrant management's attention.

(b)(7)(E) [redacted] During our audit, (b)(6) [redacted] (b)(7)(E) [redacted]

The SEC plans to (b)(7)(E) [redacted] Furthermore, (b)(7)(E) [redacted], although some potential exceptions were noted.

(b)(7)(E) [redacted] (b)(6) [redacted] (b)(7)(E) [redacted] Moreover, (b)(6) [redacted] provided specific recommendations to (b)(6) [redacted] to address the potential concerns.

(b)(7)(E) [redacted] In response, (b)(7)(E) [redacted] For other changes recommended by (b)(7)(E) [redacted]

[45] (b)(7)(E) [redacted]

[46] (b)(6) [redacted] (b)(7)(E) [redacted]

According to (b)(6) [redacted], (b)(7)(E) [redacted]

We encourage (b)(6) [redacted] to continue taking steps to obtain a (b)(7)(E) [redacted] Additionally, we encourage (b)(6) [redacted] (b)(7)(E) [redacted]

Appendix I. Scope and Methodology

We conducted this performance audit from November 2016 through September 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope. Our audit scope covered EDGAR system enhancements implemented in FYs 2014, 2015, and 2016, and the activities of the ERD program from FY 2014 through February 2017. Using the methodology described below, we sought to determine whether the SEC has effective:

1. controls to ensure the agency completes EDGAR system enhancements as planned and in accordance with the SEC's performance and budget goals;

2. controls to ensure that the agency implements EDGAR system enhancements in compliance with Federal and SEC change management controls; and

3. planning and governance controls to ensure that the ERD program meets agency needs.

In addition, we increased the scope of the audit to include ongoing EDGAR system enhancements (b)(7)(E) [redacted] (See "Other Matters of Interest" section of this report.) This audit did not assess enhancements made to the EDGAR Fee Momentum system, which is covered under the annual financial statement audit performed by GAO.

We performed fieldwork at the SEC's Headquarters in Washington, DC.

Methodology. To address our objectives, we reviewed Federal laws and regulations, and Federal and industry guidelines that address IT planning, governance, and configuration management. We also analyzed applicable SEC policies and procedures focusing on the following areas: (1) oversight of IT investments; (2) program composition, roles, and responsibilities; and (3) EDGAR system releases, enhancement prioritization, and change management. Appendix II lists key criteria documents included in our review.

We also reviewed a non-statistical sample of 6 of the 29 releases (or about 21 percent) deployed by the SEC to enhance the EDGAR system between October 1, 2013, and September 30, 2016, including 4 standard releases and 2 emergency releases. To obtain a sample, we judgmentally selected releases between October 1, 2013, and September 30, 2016. Table 1 summarizes the releases included in our sample.

Table. Sample of EDGAR System Releases Selected for Review

Fiscal Year	Standard Releases	Emergency Releases
2014	(b)(7)(E) [redacted]	[redacted]
2015	[redacted]	[redacted]
2016	[redacted]	[redacted]
Total No. of Releases Reviewed	[redacted]	[redacted]

Source: OIG-generated based on SEC report of EDGAR releases implemented in FYs 2014, 2015, and 2016.

We also reviewed one PCR from each of the releases in our sample. To assess the SEC's management of the items in our sample, we (1) interviewed OIT officials and SEC stakeholders; (2) reviewed release and PCR documentation; and (3) assessed associated performance and change management attributes.

Finally, we reviewed relevant contract files and evidence of contractor performance to assess the SEC's management of contractors involved in EDGAR operations, enhancements, and redesign. We also interviewed agency personnel from OSI and reviewed program documentation to assess the planning and governance of the ERD program.

Internal Controls. To assess internal controls relative to our objectives, we obtained and reviewed OIT's FY 2016 risk and control matrix, which stated that, if the EDGAR platform experiences performance issues or becomes unavailable, SEC and external users will be negatively impacted. We also reviewed OIT's FY 2016 management assurance statement, which stated that operations and programs were effective and efficient in the achievement of intended results, and all 15 controls tested passed the design assessment. However, OIT also reported that remediation actions were underway to correct an identified EDGAR control failure pertaining to a contractor transition. This failure was not relevant or material to our objectives.

In addition, we gained an understanding of the SEC's controls over EDGAR system enhancements and redesign efforts and identified and tested key internal controls related to our objectives. OIT and OSI personnel provided input and walkthroughs of their processes, which we used to identify potential control risks. Specifically, we assessed OIT and OSI controls related to (1) defining, approving, and tracking the cost, schedule, and scope of EDGAR enhancements; (2) establishing and consistently implementing configuration change processes; and (3) establishing and consistently implementing processes to measure, collect, and timely report ERD program performance information. We found that controls over the EDGAR program were generally effective. However, as stated in this report, we identified opportunities for further improvement. Our recommendations, if implemented, should improve the SEC's controls over EDGAR system enhancements and redesign efforts.

Computer-processed Data. GAO's *Assessing the Reliability of Computer-Processed Data* (GAO-09-680G, July 2009) states that "data reliability refers to the accuracy and completeness of computer-processed data, given the uses they are intended for. Computer-processed data may be data (1) entered into a computer system or (2) resulting from computer processing." Furthermore, GAO-09-680G defines "reliability," "completeness," and "accuracy" as follows:

- "Reliability" means that data are reasonably complete and accurate, meet intended purposes, and are not subject to inappropriate alteration.
- "Completeness" refers to the extent that relevant records are present and the fields in each record are appropriately populated.
- "Accuracy" refers to the extent that recorded data reflect the actual underlying information.

To address our objectives, we relied on computer-processed data such as reports from OIT's financial system detailing EDGAR enhancements and EDGAR Redesign program costs for FYs 2014, 2015, and 2016. We also relied on reports of EDGAR change requests and EDGAR releases from (b)(7)(E) OIT used (b)(7)(E) for software change management control, and to track issues and defects arising from the development of agency applications, including EDGAR. In June 2017, OIT moved (b)(7)(E) to (b)(7)(E). We did not perform extensive testing of these systems (that is, OIT's financial system and (b)(7)(E)) because they were not part of our audit objectives. However, we assessed the reliability of computer-processed data from these systems by tracing system reports to source documents, and through inquiries and interviews of OIT management knowledgeable of the systems and system data. Based on our assessment, we determined that the data in these systems were sufficiently reliable for the purposes of our audit.

Prior Coverage. Since 2015, the SEC OIG and GAO issued the following reports of particular relevance to this audit.

SEC OIG:

- *Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015* (Report No. 535; June 2, 2016).
- *Federal Information Security Management Act: Fiscal Year 2014 Evaluation* (Report No. 529; February 5, 2015).

GAO:

- *SEC Improved Control of Financial Systems but Needs to Take Additional Actions* (GAO-17-469; July 2017).

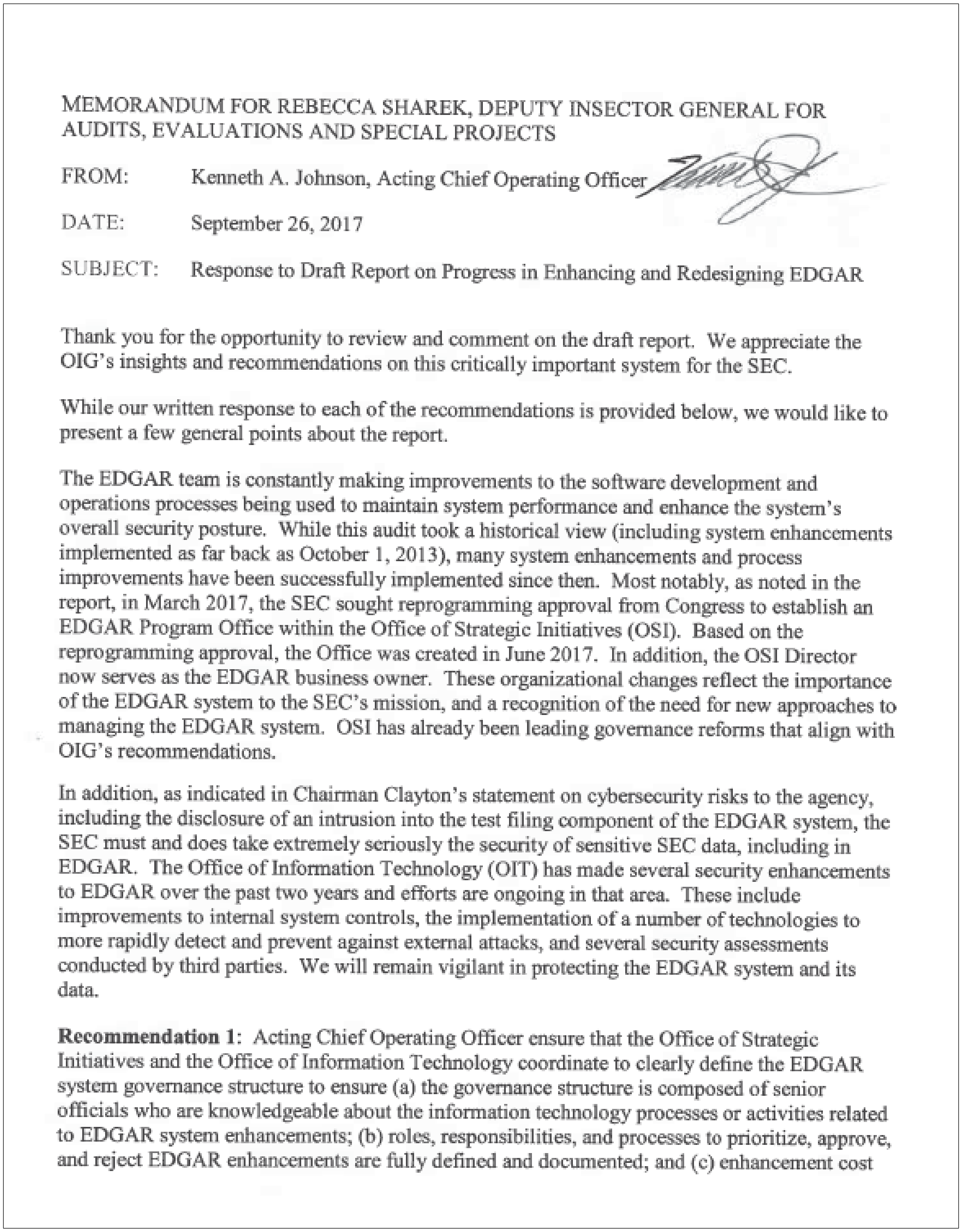
These reports can be accessed at: https://www.sec.gov/oig (SEC OIG) and https://www.gao.gov (GAO).

Appendix II. Applicable Federal Laws, SEC Regulations, and Guidance

To address our audit objectives, we reviewed applicable Federal laws, SEC regulations, and guidance, including, but not limited to, the following:

- Securities Act of 1933, Pub. L. No. 73-22, 48 Stat. 74; May 27, 1933.
- Securities Exchange Act of 1934, Pub. L. No. 73-291, 48 Stat. 881; June 6, 1934.
- Clinger-Cohen Act of 1996 (also called National Defense Authorization Act for Fiscal Year 1996), Pub. L. No. 104-106; February 10, 1996.
- SEC's Regulation S-T, *General Rules and Regulations for Electronic Filings*, codified at 17 C.F.R. part 232.
- (b)(7)(E) [redacted]
- OMB Circular A-11, Revised, *Transmittal Memorandum No. 90, Preparation, Submission, and Execution of the Budget*; July, 2016.
- OMB Memorandum M-05-23, *Improving Information Technology (IT) Project Planning and Execution*; August 2005.
- OMB Memorandum [unnumbered], *Appropriate Use of Incentive Contracts*; December 4, 2007.
- OMB Memorandum M-10-26, *Immediate Review of Financial Systems IT Projects*; June 28, 2010.
- OMB Policy Letter 93-1 (Reissued), *Management Oversight of Service Contracting*; May 1994.
- SEC Administrative Regulation 24-02, *Information Technology Capital Planning and Investment Control*, Revision 2.1; May 2017.
- SEC Administrative Regulation 24-04, *SEC OIT Information Technology Security Program*, Revision 2; August 12, 2015.
- *Information Technology Investment Management, A Framework for Assessing and Improving Process Maturity*, GAO-04-394G, Version 1.1; March 2004.
- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* Revision 4; April 2013.
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*; August 2011.

Appendix III. Management Comments



MEMORANDUM FOR REBECCA SHAREK, DEPUTY INSECTOR GENERAL FOR AUDITS, EVALUATIONS AND SPECIAL PROJECTS

FROM: Kenneth A. Johnson, Acting Chief Operating Officer

DATE: September 26, 2017

SUBJECT: Response to Draft Report on Progress in Enhancing and Redesigning EDGAR

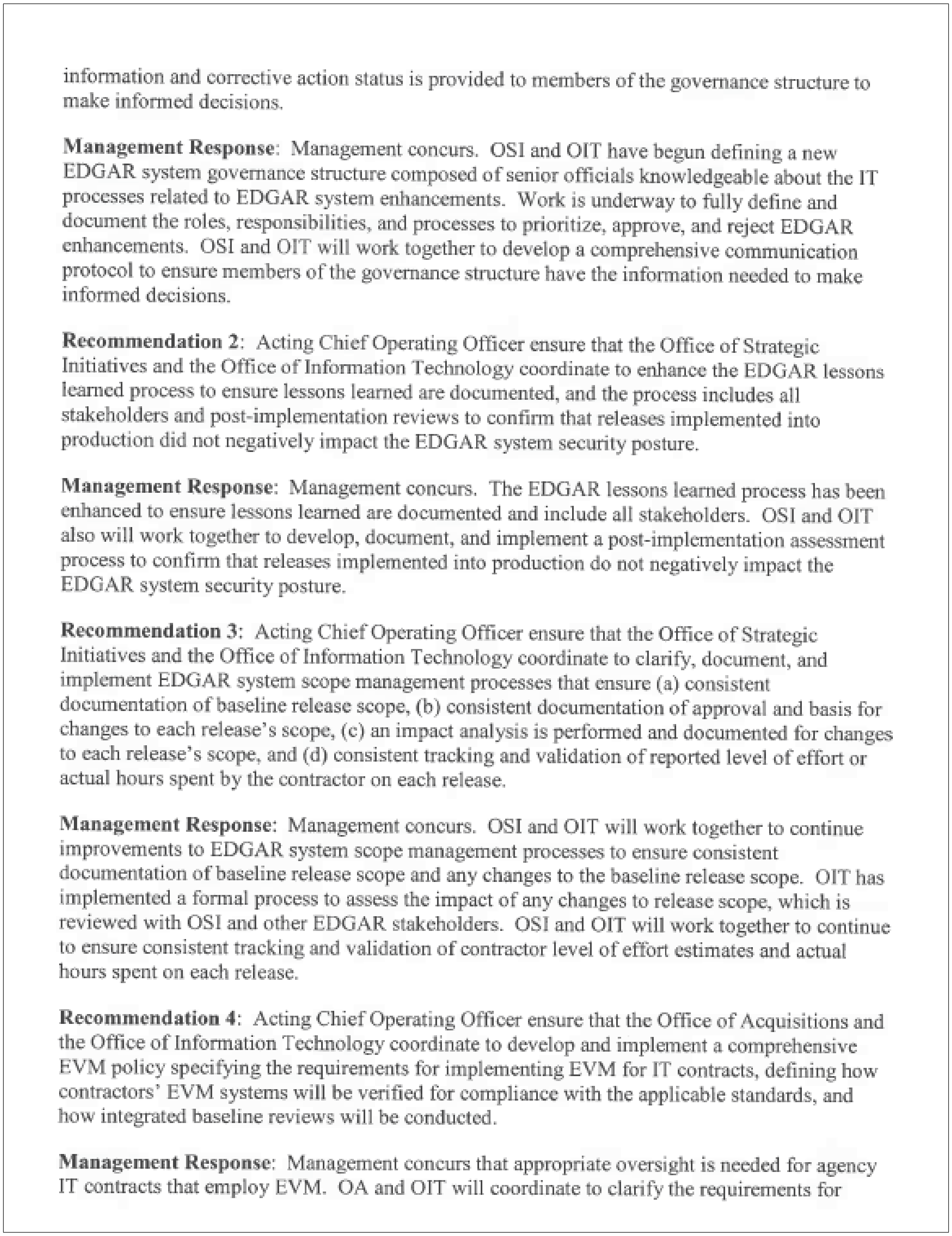
Thank you for the opportunity to review and comment on the draft report. We appreciate the OIG's insights and recommendations on this critically important system for the SEC.

While our written response to each of the recommendations is provided below, we would like to present a few general points about the report.

The EDGAR team is constantly making improvements to the software development and operations processes being used to maintain system performance and enhance the system's overall security posture. While this audit took a historical view (including system enhancements implemented as far back as October 1, 2013), many system enhancements and process improvements have been successfully implemented since then. Most notably, as noted in the report, in March 2017, the SEC sought reprogramming approval from Congress to establish an EDGAR Program Office within the Office of Strategic Initiatives (OSI). Based on the reprogramming approval, the Office was created in June 2017. In addition, the OSI Director now serves as the EDGAR business owner. These organizational changes reflect the importance of the EDGAR system to the SEC's mission, and a recognition of the need for new approaches to managing the EDGAR system. OSI has already been leading governance reforms that align with OIG's recommendations.

In addition, as indicated in Chairman Clayton's statement on cybersecurity risks to the agency, including the disclosure of an intrusion into the test filing component of the EDGAR system, the SEC must and does take extremely seriously the security of sensitive SEC data, including in EDGAR. The Office of Information Technology (OIT) has made several security enhancements to EDGAR over the past two years and efforts are ongoing in that area. These include improvements to internal system controls, the implementation of a number of technologies to more rapidly detect and prevent against external attacks, and several security assessments conducted by third parties. We will remain vigilant in protecting the EDGAR system and its data.

Recommendation 1: Acting Chief Operating Officer ensure that the Office of Strategic Initiatives and the Office of Information Technology coordinate to clearly define the EDGAR system governance structure to ensure (a) the governance structure is composed of senior officials who are knowledgeable about the information technology processes or activities related to EDGAR system enhancements; (b) roles, responsibilities, and processes to prioritize, approve, and reject EDGAR enhancements are fully defined and documented; and (c) enhancement cost



information and corrective action status is provided to members of the governance structure to make informed decisions.

Management Response: Management concurs. OSI and OIT have begun defining a new EDGAR system governance structure composed of senior officials knowledgeable about the IT processes related to EDGAR system enhancements. Work is underway to fully define and document the roles, responsibilities, and processes to prioritize, approve, and reject EDGAR enhancements. OSI and OIT will work together to develop a comprehensive communication protocol to ensure members of the governance structure have the information needed to make informed decisions.

Recommendation 2: Acting Chief Operating Officer ensure that the Office of Strategic Initiatives and the Office of Information Technology coordinate to enhance the EDGAR lessons learned process to ensure lessons learned are documented, and the process includes all stakeholders and post-implementation reviews to confirm that releases implemented into production did not negatively impact the EDGAR system security posture.

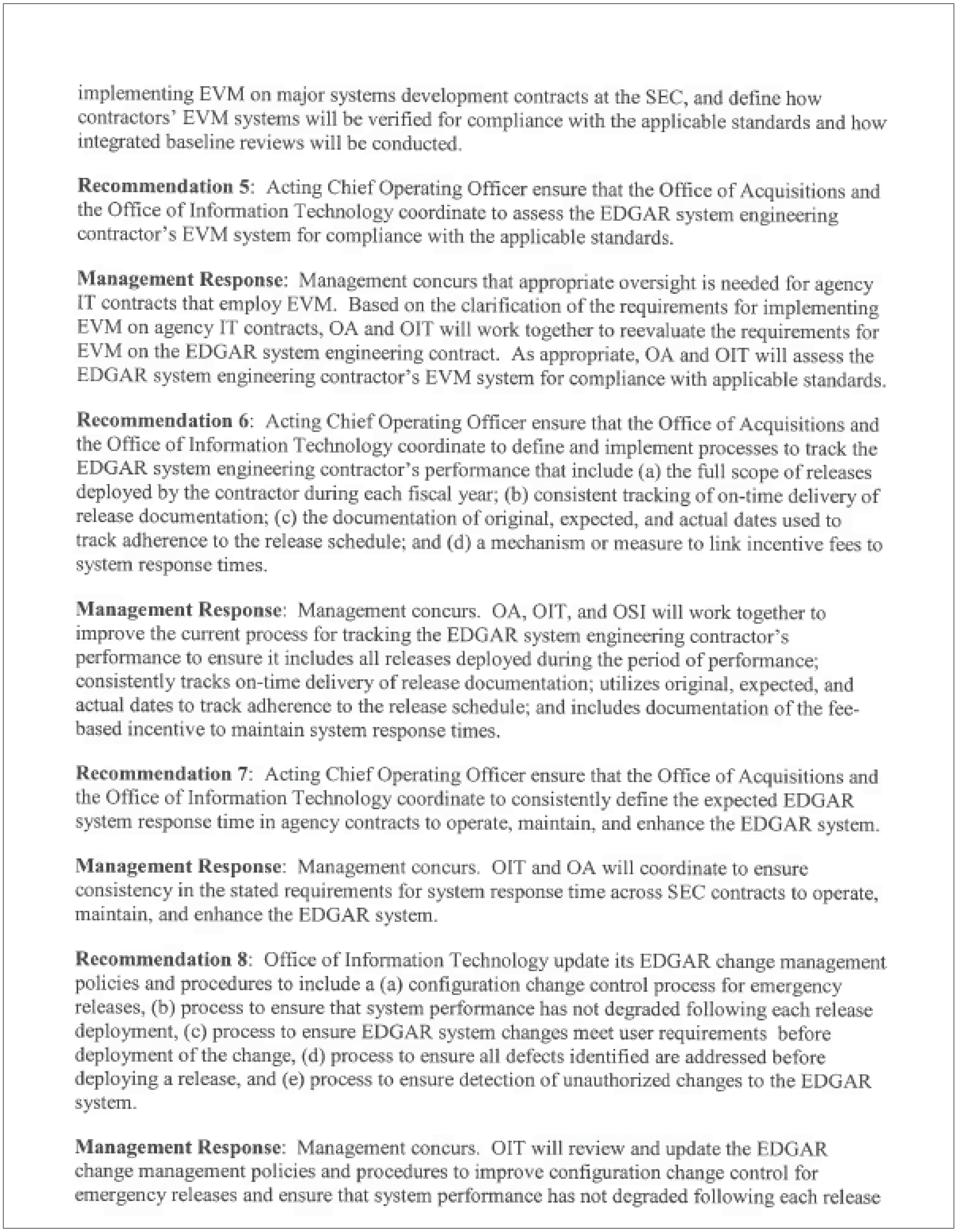
Management Response: Management concurs. The EDGAR lessons learned process has been enhanced to ensure lessons learned are documented and include all stakeholders. OSI and OIT also will work together to develop, document, and implement a post-implementation assessment process to confirm that releases implemented into production do not negatively impact the EDGAR system security posture.

Recommendation 3: Acting Chief Operating Officer ensure that the Office of Strategic Initiatives and the Office of Information Technology coordinate to clarify, document, and implement EDGAR system scope management processes that ensure (a) consistent documentation of baseline release scope, (b) consistent documentation of approval and basis for changes to each release's scope, (c) an impact analysis is performed and documented for changes to each release's scope, and (d) consistent tracking and validation of reported level of effort or actual hours spent by the contractor on each release.

Management Response: Management concurs. OSI and OIT will work together to continue improvements to EDGAR system scope management processes to ensure consistent documentation of baseline release scope and any changes to the baseline release scope. OIT has implemented a formal process to assess the impact of any changes to release scope, which is reviewed with OSI and other EDGAR stakeholders. OSI and OIT will work together to continue to ensure consistent tracking and validation of contractor level of effort estimates and actual hours spent on each release.

Recommendation 4: Acting Chief Operating Officer ensure that the Office of Acquisitions and the Office of Information Technology coordinate to develop and implement a comprehensive EVM policy specifying the requirements for implementing EVM for IT contracts, defining how contractors' EVM systems will be verified for compliance with the applicable standards, and how integrated baseline reviews will be conducted.

Management Response: Management concurs that appropriate oversight is needed for agency IT contracts that employ EVM. OA and OIT will coordinate to clarify the requirements for



implementing EVM on major systems development contracts at the SEC, and define how contractors' EVM systems will be verified for compliance with the applicable standards and how integrated baseline reviews will be conducted.

Recommendation 5: Acting Chief Operating Officer ensure that the Office of Acquisitions and the Office of Information Technology coordinate to assess the EDGAR system engineering contractor's EVM system for compliance with the applicable standards.

Management Response: Management concurs that appropriate oversight is needed for agency IT contracts that employ EVM. Based on the clarification of the requirements for implementing EVM on agency IT contracts, OA and OIT will work together to reevaluate the requirements for EVM on the EDGAR system engineering contract. As appropriate, OA and OIT will assess the EDGAR system engineering contractor's EVM system for compliance with applicable standards.

Recommendation 6: Acting Chief Operating Officer ensure that the Office of Acquisitions and the Office of Information Technology coordinate to define and implement processes to track the EDGAR system engineering contractor's performance that include (a) the full scope of releases deployed by the contractor during each fiscal year; (b) consistent tracking of on-time delivery of release documentation; (c) the documentation of original, expected, and actual dates used to track adherence to the release schedule; and (d) a mechanism or measure to link incentive fees to system response times.

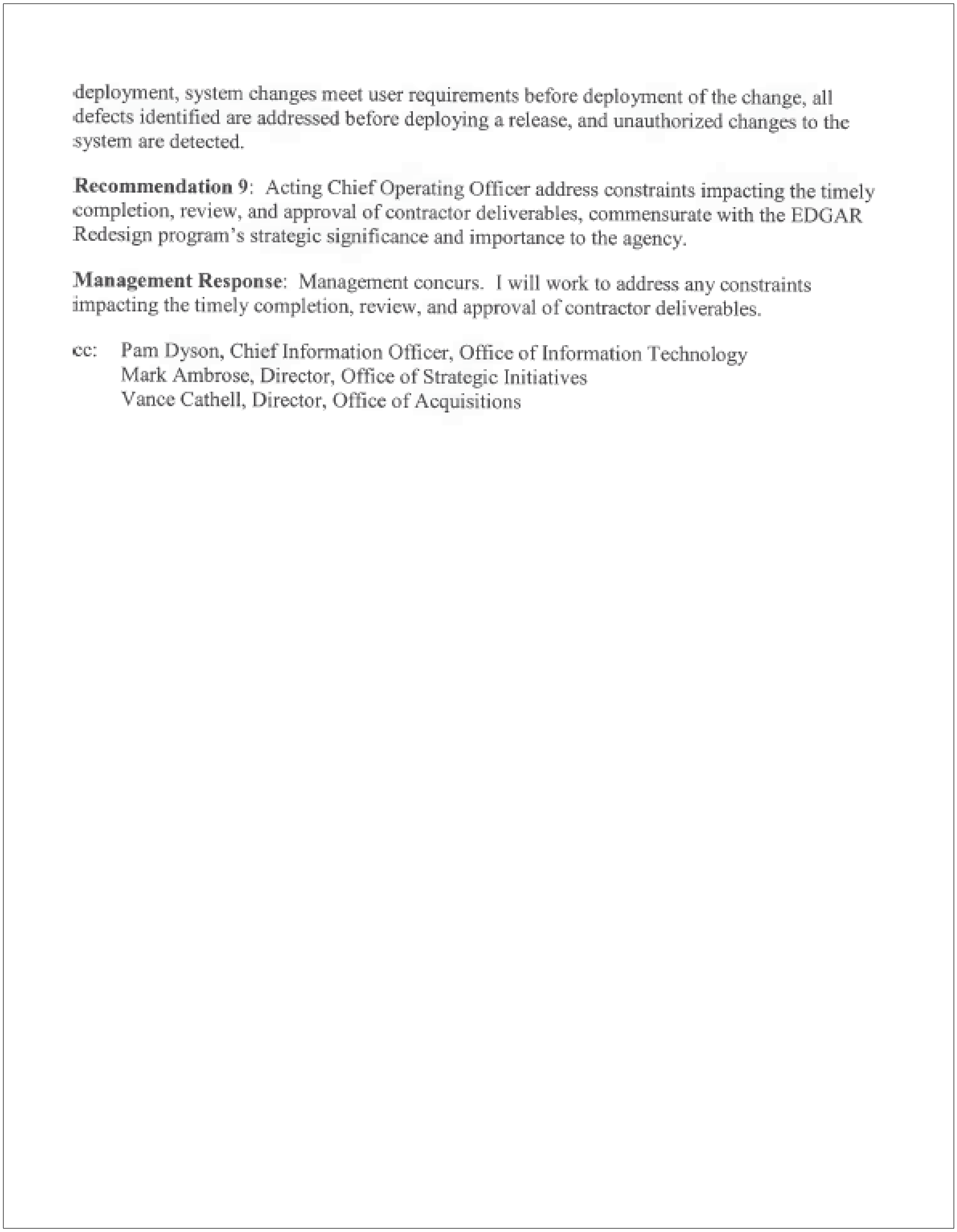
Management Response: Management concurs. OA, OIT, and OSI will work together to improve the current process for tracking the EDGAR system engineering contractor's performance to ensure it includes all releases deployed during the period of performance; consistently tracks on-time delivery of release documentation; utilizes original, expected, and actual dates to track adherence to the release schedule; and includes documentation of the fee-based incentive to maintain system response times.

Recommendation 7: Acting Chief Operating Officer ensure that the Office of Acquisitions and the Office of Information Technology coordinate to consistently define the expected EDGAR system response time in agency contracts to operate, maintain, and enhance the EDGAR system.

Management Response: Management concurs. OIT and OA will coordinate to ensure consistency in the stated requirements for system response time across SEC contracts to operate, maintain, and enhance the EDGAR system.

Recommendation 8: Office of Information Technology update its EDGAR change management policies and procedures to include a (a) configuration change control process for emergency releases, (b) process to ensure that system performance has not degraded following each release deployment, (c) process to ensure EDGAR system changes meet user requirements before deployment of the change, (d) process to ensure all defects identified are addressed before deploying a release, and (e) process to ensure detection of unauthorized changes to the EDGAR system.

Management Response: Management concurs. OIT will review and update the EDGAR change management policies and procedures to improve configuration change control for emergency releases and ensure that system performance has not degraded following each release



deployment, system changes meet user requirements before deployment of the change, all defects identified are addressed before deploying a release, and unauthorized changes to the system are detected.

Recommendation 9: Acting Chief Operating Officer address constraints impacting the timely completion, review, and approval of contractor deliverables, commensurate with the EDGAR Redesign program's strategic significance and importance to the agency.

Management Response: Management concurs. I will work to address any constraints impacting the timely completion, review, and approval of contractor deliverables.

cc: Pam Dyson, Chief Information Officer, Office of Information Technology
Mark Ambrose, Director, Office of Strategic Initiatives
Vance Cathell, Director, Office of Acquisitions

Major Contributors to the Report

Kelli Brown-Barnes, Audit Manager

Michael Burger, Lead Auditor

Sara Tete Nkongo, Auditor

Sumeer Ahluwalia, Auditor

To Report Fraud, Waste, or Abuse, Please Contact:

Web: www.reportlineweb.com/sec_oig

Telephone: (877) 442-0854

Fax: (202) 772-9265

Address: U.S. Securities and Exchange Commission
Office of Inspector General
100 F Street, N.E.
Washington, DC 20549

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, evaluations, or reviews, please send an e-mail to OIG Audit Planning at AUDplanning@sec.gov. Comments and requests can also be mailed to the attention of the Deputy Inspector General for Audits, Evaluations, and Special Projects at the address listed above.