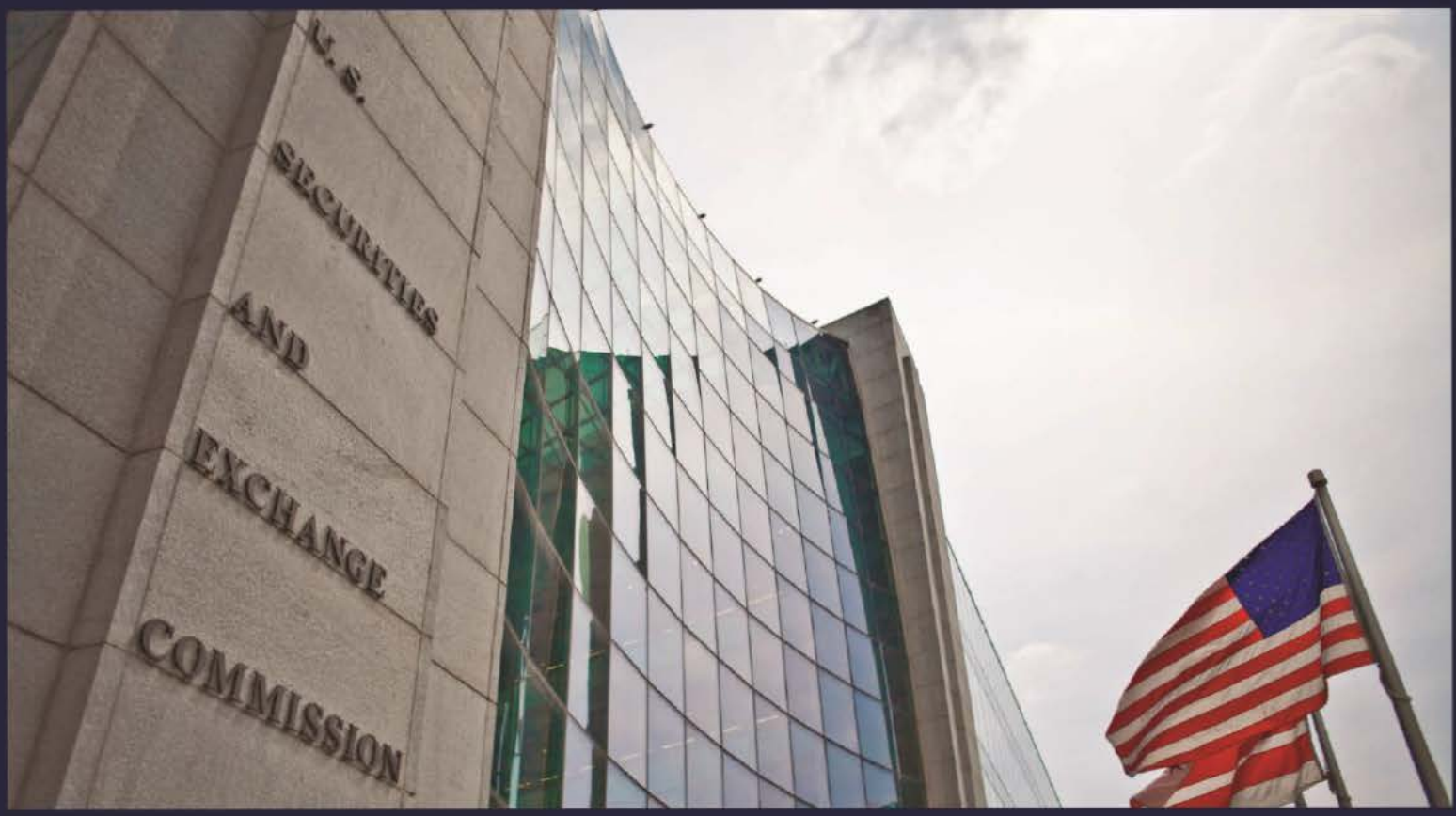
U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Audit of the SEC's Information Technology Requirements-Gathering Process



September 30, 2016
Report No. 538

REDACTED FOR PUBLIC RELEASE

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

OFFICE OF
INSPECTOR GENERAL

M E M O R A N D U M

September 30, 2016

TO: Jeffery Heslop, Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General

SUBJECT: *Audit of the SEC's Information Technology Requirements-Gathering Process*, Report No. 538

Attached is the Office of Inspector General (OIG) final report detailing the results of our audit of the U.S. Securities and Exchange Commission's (SEC or agency) information technology requirements-gathering process. The report contains seven recommendations that should help improve the SEC's information technology requirements-gathering process and oversight of information technology acquisitions.

On September 19, 2016, we provided management with a draft of our report for review and comment. In its September 27, 2016, response, management concurred with our recommendations. We have included the response as Appendix IV 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 Offices of Information Technology and Acquisitions 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: Mary Jo White, Chair
Andrew Donohue, Chief of Staff, Office of the Chair
Michael Liftik, Deputy Chief of Staff, Office of the Chair
Nathaniel Stankard, Deputy Chief of Staff, Office of the Chair
Michael S. Piwowar, Commissioner
Jaime Klima, Counsel, Office of Commissioner Piwowar
Kara M. Stein, Commissioner

Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein
Anne K. Small, General Counsel
Keith Cassidy, Director, Office of Legislative and Intergovernmental Affairs
Rick Fleming, Investor Advocate
John J. Nester, Director, Office of Public Affairs
Pamela C. Dyson, Chief Information Officer, Office of Information Technology
Vance Cathell, Director, Office of Acquisitions
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

REDACTED FOR PUBLIC RELEASE

Executive Summary

Audit of the SEC's Information Technology Requirements-Gathering Process
Report No. 538
September 30, 2016

Why We Did This Audit

According to the Government Accountability Office (GAO), Federal Government information technology (IT) projects frequently incur cost overruns and schedule slippages and contribute little to mission-related outcomes, in part, because of ineffective management, including poor requirements gathering. In 2011, GAO identified requirements management as a leading practice to manage IT modernization efforts, stating that disciplined processes for developing and managing IT requirements can improve the likelihood that systems will meet user needs and perform as intended. Between October 1, 2013, and November 25, 2015, the U.S. Securities and Exchange Commission (SEC or agency) obligated more than $521 million for 692 IT investments, including investments to modernize the agency's systems. If the SEC does not have a disciplined process for developing and managing IT requirements, the SEC risks cost overruns and schedule delays in its efforts to maintain and modernize its IT systems. Moreover, agency IT investments may not meet user needs.

What We Recommended

We made seven recommendations, including that management continue its efforts to design and implement an IT requirements-gathering process or framework; define roles and responsibilities for IT requirements-gathering; assess the potential risks and benefits, including potential cost savings, from the Oracle consolidation effort; and update existing policies and procedures. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action. We redacted sensitive information contained in this report.

What We Found

The SEC's Office of Information Technology (OIT) has overall management responsibility for the agency's IT capital planning and investment control process, which includes the IT requirements-gathering process. In September 2015, OIT initiated efforts to establish a Requirements Center of Excellence. By August 2016, OIT had rolled out the Requirements Center of Excellence framework. However, OIT has not fully designed and implemented the SEC's IT requirements-gathering process, and opportunities exist to improve OIT's oversight of the SEC's IT investments and their underlying requirements.

Specifically, we reviewed a sample of 17 development, modernization, and enhancement (DME) investments and 8 steady state investments and found that, although OIT policies and procedures addressed elements of IT requirements-gathering, OIT did not consistently document or validate detailed, measurable requirements, particularly for DME investments. In addition, OIT did not always ensure that investments were managed by integrated project teams and certified individuals, where necessary, or define project team members' roles and responsibilities for IT requirements-gathering. We also found that investment documents did not always demonstrate that OIT integrated security requirements into DME investment planning and initiation phases. Furthermore, OIT did not consistently review and coordinate IT investments—particularly steady state investments, investments to acquire technology equipment, and Oracle support services investments—to prevent redundancy; and for two investments, governance authorities did not review and approve changes to investments' baselines before implementation.

As a result, OIT did not always comply with Federal regulations, Federal and industry guidelines, and its own policies and procedures. In addition, two IT investments we reviewed were delayed between 6 and 15 months from their initial completion dates (one of them incurred about $1.9 million in additional costs to further define requirements and continue project development and implementation); and the SEC may not realize any cost savings from an effort to consolidate some contracts for Oracle support services. Furthermore, the SEC may not have optimized its technology equipment purchases. We also question $24,230 paid to a contractor hired to gather requirements during a period when the corresponding project had no specific requirements-gathering activity. Finally, we determined that the SEC spent about $1 million to develop requirements that, according to the business sponsor, may in part need to be re-worked once a dependency (a separate system component) is completed, and about $600,000 for a project that was put on hold. We encourage management to leverage the results of our audit as OIT continues its efforts to fully design and implement the SEC's requirements-gathering process and improve the oversight of the SEC's IT investments.

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

TABLE OF CONTENTS

ABBREVIATIONS

CPIC	Capital Planning and Investment Control
DME	development, modernization and enhancement
EDGAR	Electronic Data Gathering and Retrieval
eFAP	electronic Filing for Administrative Proceedings
ESC	Enterprise Services Center
FAC-P/PM	Federal Acquisition Certification for Program and Project Managers
FDM	Financial Data Mart
FY	fiscal year
GAO	Government Accountability Office
IOC	Information Officers' Council

IT	information technology
ITCPC	Information Technology Capital Planning Committee
NIST	National Institute of Standards and Technology
(b) (7)(E)	(b) (7)(E)
O&M	operations and maintenance
OA	Office of Acquisitions
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PRB	Project Review Board
RCoE	Requirements Center of Excellence
Rev.	Revision
SDLC	System Development Life Cycle
SEC or agency	U.S. Securities and Exchange Commission
SECR	SEC Administrative Regulation
SP	Special Publication
TCR	Tips, Complaints, and Referrals Intake and Resolution System
TRB	Technical Review Board

Background and Objective

Background

According to the Government Accountability Office (GAO), Federal Government information technology (IT) projects "can—and have—become risky, costly, unproductive mistakes," that "too frequently incur cost overruns and schedule slippages while contributing little to mission-related outcomes" because of ineffective management, including poor requirements-gathering and management.[1] IT requirements establish what an IT system will do, how well the system will do it, and how the system will interact with other systems. Typically, IT requirements-gathering includes eliciting, analyzing, validating, and documenting end users' and stakeholders' detailed, measurable requirements and controlling changes to those requirements in documents such as a requirements traceability matrix or a requirements management plan. In 2011, GAO identified requirements management as a leading practice to manage IT modernization efforts, stating that defining and implementing disciplined processes for developing and managing requirements can improve the likelihood that systems will meet end user needs and perform as intended.[2] Furthermore, in 2015, GAO identified "Improving the Management of [IT] Acquisitions and Operations" as a new high-risk area needing attention by Congress and the executive branch.[3]

The U.S. Securities and Exchange Commission's (SEC or agency) Office of Information Technology (OIT) is responsible for aligning technology with agency business needs. OIT provides the SEC with project management and oversight for all enterprise-wide IT investments or projects.[4] OIT is also responsible for the agency's IT requirements-gathering process. The SEC's Office of Acquisitions (OA) is responsible for overseeing agency acquisitions, including soliciting, evaluating, and awarding contracts for new or revised IT systems, or contracts to operate and maintain existing systems. Between October 1, 2013, and November 25, 2015, the SEC obligated more than $521 million for 692 IT investments. OIT has engaged contractors to manage many of these IT investments, as discussed further in this report.

Federal Laws and Guidance. Congress has enacted legislation that addresses the IT acquisition process, including developing and managing IT requirements. For example,

[1] U.S. Government Accountability Office, *Information Technology – Critical Factors Underlying Successful Major Acquisitions* (GAO-12-7, October 2011).

[2] U.S. Government Accountability Office, *USDA Systems Modernization – Management and Oversight Improvements Are Needed* (GAO-11-586, July 2011).

[3] U.S. Government Accountability Office, *High-Risk Series – An Update* (GAO-15-290, February 2015).

[4] OIT's *Project Life Cycle Framework – Project Manager Resource Guide*, February 2015, defines "IT project" as "an IT investment for which there is an expenditure of resources for IT or IT-related products and services, and for which there are expected benefits to the organization's performance, either in terms of the efficiency of operations or effectiveness of services." Thus, we use the terms "investment" and "project" interchangeably throughout this report.

Congress enacted the Clinger-Cohen Act of 1996, which requires Federal agencies to establish clearly defined IT capital planning and investment control (CPIC) processes.[5] In 2014, Congress enacted the Federal Information Technology Acquisition Reform Act,[6] which aims to improve Federal IT acquisitions and operations. Moreover, according to the Federal Information Security Modernization Act of 2014, "each Federal agency shall develop, document, and implement an agency-wide information security program to provide information security for information and information systems."

The Office of Management and Budget (OMB) has issued policy and guidance for implementing these Federal laws. The Federal Acquisition Regulation establishes additional requirements for the Federal IT acquisition process. Also, the National Institute of Standards and Technology (NIST) publishes Federal guidelines for agencies' information systems. NIST Special Publication (SP) 800-64[7] states that organizations should document detailed security requirements in measurable terms, and integrate security steps throughout the system development life cycle (SDLC).[8]

Industry Guidelines. Industry guidelines also address IT requirements-gathering and management. Specifically, OIT recognizes the Project Management Institute's *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*[9] as a professional standard for project management. The guide emphasizes the need to elicit, analyze, and document project requirements in enough detail to be measurable. Also, the Software Engineering Institute's *Capability Maturity Model® Integration for Development*[10] (cited as an industry standard in OIT documents) addresses the need to establish and maintain a defined requirements development process that includes analyzing and validating requirements, and tracking and controlling changes to requirements. OIT's policies, procedures, and documents refer to and, in some cases, require compliance with these industry guidelines.

SEC Regulations, Policies, and Procedures. As discussed further in this report, the SEC did not have a requirements-gathering process or framework including activities to consistently document and validate detailed, measurable requirements. However, SEC regulations, policies, and procedures that describe the agency's CPIC process and SDLC include elements of IT requirements-gathering and management. For example,

[5] CPIC processes include identifying, selecting, controlling, and evaluating IT investments to determine which investments make the best use of agency resources. The rigor of CPIC processes varies depending on the complexity and risk of each investment.

[6] The Federal Information Technology Acquisition Reform Act (as part of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015); December 19, 2014.

[7] NIST SP 800-64, *Security Considerations in the System Development Life Cycl*e, Revision (Rev.) 2; October 2008.

[8] As Table 1 in Appendix II demonstrates, the SDLC is a series of phases through which all IT investments pass, beginning with the initial identification of a need to the retirement of the investment.

[9] Project Management Institute: *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Fifth Edition, Project Management Institute, Inc. (PMI), 2013.

[10] Carnegie Mellon Software Engineering Institute, *Capability Maturity Model® Integration (CMMI) for Development*, Version 1.3, CMU/SEI-2010-TR-033 (Hanscom AFB, Massachusetts: November 2010).

SEC Administrative Regulation 24-02, Rev. 2, *Information Technology Capital Planning and Investment Control* (April 2015) (SECR 24-02), prescribes the policies, requirements, and responsibilities for the SEC's CPIC process and states that the process will include re-assessing "business cases in the light of changing requirements and improved knowledge of costs and risks." SECR 24-02 also assigns responsibilities for developing business requirements and for preparing business cases for IT investments. In addition, OIT's *Project Manager Resource Guide* describes the phases of the SEC's SDLC for a repeatable, enterprise-wide approach to managing all agency IT projects and ensuring IT projects meet agency requirements and priorities. Appendix II includes a summary of the SEC's SDLC phases including, where applicable, the elements of IT requirements-gathering that the agency's SDLC addresses.

In addition, the SEC's CPIC process includes three phases that integrate with the SDLC. First, the selection phase includes activities to prepare, submit, evaluate, and approve the investment business case (which serves as the investment proposal), including the rationale, approach, budget, and related issues. Second, the control phase encompasses processes and activities to track the investment's progress against verifiable milestones, re-assess risks facing the investment, and establish and track corrective actions to address any deviations from the approved investment proposal. Third, the evaluation phase includes processes to validate whether business objectives were met, and re-assess the business cases, as needed, in light of changing requirements.

Investment Boards and Oversight Structures. CPIC boards (also called governance authorities) and SDLC oversight structures govern the SEC's IT investments and are responsible for selecting, overseeing, and evaluating SEC IT investments within their purview. The SEC's investment boards (further described in Appendix II) are the Information Technology Capital Planning Committee (ITCPC), the Project Review Board (PRB), and the Information Officers' Council (IOC). The SEC's SDLC oversight structures are OIT's Transition Management Branch, the Enterprise Architecture (through its Technical Review Board [TRB]), and the Configuration Management and Quality Assurance organizations.

IT Investment Categories. IT investments fall within two categories: (1) development, modernization, and enhancement (DME) investments, and (2) steady state investments. DME investments include new investments and changes to existing systems to improve their performance, implement legislative or regulatory requirements, or meet agency leadership requests. In contrast, steady state investments sustain existing information systems at their current capability and performance levels, and include costs for voice and data communications maintenance and service, and costs to replace broken IT equipment. Of about $521 million the SEC obligated between October 2013 and November 2015 for IT investments, about $226 million (or 43 percent) was for DME investments. The remaining $295 million (or 57 percent) was for steady state investments.

Plans To Improve IT Service Delivery and Establish a Requirements Center of Excellence (RCoE). In 2011, the Boston Consulting Group completed a study and issued a report that noted, among other things, gaps in the SEC's delivery of IT services, including insufficient understanding of business needs (or business requirements) and limited oversight of IT investments.[11] The report also noted a limited and inconsistent use of tools and methodologies, stating that "OIT lacks a comprehensive tool to manage [IT] project requirements." According to the report, OIT has initiated efforts to address these gaps. Specifically, in September 2015, OIT hired a contractor to assess the SEC's IT requirements management maturity level and to establish an RCoE because, according to OIT management, some SEC IT projects experienced schedule, scope, and budget challenges because of inadequate requirements development. In addition, OIT management realized that the agency did not have standardized requirements documents or requirements management processes. According to the contract, the objective of the RCoE is:

> to equip the Commission to meet customer expectations, deliver projects on time, and within budget. The [RCoE] will establish a framework for full requirements management, quality control, and implement a standard requirements tool that will be used to capture and manage requirements throughout the project lifecycle.

By August 2016, OIT had rolled-out a SharePoint site, defined requirements documents and templates, and conducted trainings on the RCoE framework. OIT anticipates implementing a policy mandating the use of the RCoE framework by December 2016.

Objective

Our overall objective was to evaluate the SEC's IT requirements-gathering process. Specifically, we sought to determine whether the SEC's IT requirements-gathering process was:

1. sufficiently designed and complied with applicable Federal laws, regulations, and industry guidelines; and

2. consistently applied in accordance with Federal and agency policies and facilitated the effective and efficient procurement or development of IT projects.

To address our objectives, we reviewed applicable Federal laws and guidance, Federal and industry guidelines, and SEC regulations, policies, and procedures. We also reviewed a nonstatistical sample of 25 of the SEC's 692 IT investments funded between October 1, 2013, and November 25, 2015, as recorded in OIT's financial system. We

[11] The Boston Consulting Group, Inc., *U.S. Securities and Exchange Commission Organizational Study and Reform*; March 10, 2011. Section 967 of the Dodd-Frank Wall Street Reform and Consumer Protection Act directed the SEC to engage an independent consultant to examine the internal operations, structure, and the need for reform at the SEC. The Boston Consulting Group was selected for this study, which focused on four matters: organizational structure, personnel and resources, technology and resources, and relationships with self-regulatory organizations.

focused our review on the SEC's activities to identify, validate, and document detailed, measurable IT requirements. Our sample included 17 DME investments and 8 steady state investments sponsored by various SEC divisions and offices throughout the period reviewed. As of November 2015 (the time of our sample selection), the SEC had obligated about $83 million for the 25 IT investments we reviewed. Appendix I includes additional information on our scope and methodology, including a summary of the IT investments we reviewed, our review of internal controls, and prior audit coverage.

Results

Finding 1: OIT Has Not Fully Designed and Implemented the SEC's IT Requirements-Gathering Process

OIT initiated efforts to establish the RCoE by hiring a contractor to assess the SEC's IT requirements management maturity level and rolling-out an RCoE framework to standardize requirements documents and requirements management processes. However, based on the IT investments we reviewed, we determined that OIT has not fully designed and implemented the requirements-gathering process. Specifically, OIT did not consistently document or validate detailed, measurable IT requirements for DME investments. In addition, OIT did not always ensure that integrated project teams, including individuals with the required level of certification, managed investments, or defined in project documents, including charters, project team members' roles and responsibilities for IT requirements-gathering. As a result, OIT did not always comply with applicable Federal regulations, Federal and industry guidelines, and OIT's own policies and procedures. In addition, two DME investments we reviewed were delayed between 6 and 15 months from their initial completion dates, with one of the DME investments incurring about $1.9 million in additional costs to further define requirements and continue project development and implementation.

OIT Did Not Consistently Document or Validate Detailed, Measurable IT Requirements for DME Investments

For each of the 17 DME investments we reviewed,[12] OIT developed and documented high-level requirements (that is, business requirements or project ideas) in an investment proposal or plan. In addition, for 10 of the 17 DME investments reviewed, OIT documented and validated detailed, measurable functional and nonfunctional requirements, although the documents describing these requirements varied by investment. However, for the remaining seven DME investments we reviewed, OIT either did not develop detailed requirements documents or did not have business sponsors validate or formally accept (that is, sign-off on) requirements documents as baselines.

For example, we reviewed an investment to develop requirements for the Division of Investment Management's workflow system (referred to as the *Investment Management Workflow System Requirements Gathering* project) and determined that, aside from

[12] We did not review investment proposals documenting high-level requirements for the eight steady state investments included in our sample because steady state investments are costs to sustain IT assets (that were once DME) at their current capability and performance levels. Finding 2 addresses issues related to the annual operational analysis of steady state investments.

high-level requirements, OIT did not document detailed, measurable requirements. We reviewed another investment (referred to as the *electronic Filing for Administrative Proceedings [eFAP] II* project) and determined that, although OIT documented detailed, measurable requirements, OIT did not have the business sponsor (the Office of the Secretary) validate or formally accept the requirements documents. In its 2011 report, the Boston Consulting Group also found that "OIT and its internal clients [SEC divisions and offices] are not tightly aligned," noting that "divisions and offices typically do not engage in formal sign-offs" at project development milestones.

When acquiring supplies or services, the Federal Acquisition Regulation requires agencies to state requirements, including functions to be performed and the performance required, in requirements documents.[13] In addition, GAO has reported that agencies' IT requirements management processes should include documenting, validating, and managing requirements throughout the system life cycle.[14] Industry guidelines established by the Project Management Institute also state that, "before being baselined, requirements need to be unambiguous (measurable and testable), traceable, complete, consistent, and acceptable to key stakeholders."[15] Finally, SEC policies and procedures require that "All [SEC] IT investments, regardless of dollar value, shall be supported and justified by an approved investment plan" that summarizes the business case and initial requirements for the investment, and state that the SEC's SDLC planning phase should include requirements documents.[16]

OIT did not document or validate detailed, measurable requirements for 7 of the 17 DME investments we reviewed, in part, because OIT has not fully designed and implemented the SEC's IT requirements-gathering process. Although OIT initiated efforts to establish the RCoE and, in August 2016, rolled-out the RCoE framework, OIT has not implemented a policy mandating the use of this framework. OIT officials told us that they anticipate implementing a policy mandating the use of the RCoE framework by December 2016. As a result, OIT did not always comply with Federal regulations or Federal and industry guidelines addressing the need to establish management processes to document and validate requirements. In addition, OIT did not always develop requirements documents in accordance with its own policies and procedures. Moreover, the following two DME investments we reviewed were delayed between 6 and 15 months from their initial completion dates with one of them incurring an additional $1.9 million to further define requirements and continue project development and implementation:

[13] Federal Regulations, *Federal Acquisition Regulations System* (Revised); March 2005.

[14] U.S. Government Accountability Office, *United States Coast Guard: Improvements Needed in Management and Oversight of Rescue System Acquisition* (GAO-06-623, May 2006).

[15] Project Management Institute: *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Fifth Edition, Project Management Institute, Inc. (PMI), 2013.

[16] OIT Implementing Instruction II 24-02.01.01 (01.0), *Information Technology Investment Initiation*, May 2005; and *OIT Project Life Cycle Framework Project Manager Resource Guide, February 2015*.

Analytic Tools and Platform Investment. An investment called *Analytic Tools and Platform* was part of a multiyear project to (b) (7)(E) [redacted] The multiyear project initially had a December 2014 baseline completion date and $5.9 million in approved funding. According to the Division of Enforcement (the project's business sponsor), before 2014, the project team documented high-level requirements. In 2014, the Division of Enforcement determined that it needed to either refine the requirements by defining detailed requirements or end the project. Communications between the Division of Enforcement and OIT state that using the high-level, broad requirements was not the best option to accomplish the project's objective and that a short term extension to develop new competitive requirements would be more applicable to keep the project going. The Division of Enforcement requested a 6-month extension and incurred about $1.9 million in additional costs to further define requirements and continue project development and implementation.

Investment Management Workflow System—Requirements Gathering Investment. As previously discussed, the objective of this investment was to develop requirements for the Division of Investment Management's workflow system. However, the project requirements (included in the contract deliverables) were generic in nature and not tied to specific business needs because such needs had not been established. As a result, OIT postponed the investment's baseline completion date by 15 months while the Division of Investment Management clarified its business needs. This investment is further discussed in Finding 2.

OIT Did Not Always Ensure Investments Were Managed by Integrated Project Teams and Certified Individuals, or Define Roles and Responsibilities for IT Requirements-Gathering

Less than half of the IT investments we reviewed (12 out of 25) were managed by integrated project teams, including appropriate subject matter experts such as a business owner, business lead, technical lead, and IT project manager.[17] Moreover, only a third of the investments we reviewed that were managed by integrated project teams (4 out of 12) had project charters or other investment documents that defined project team members' roles and responsibilities for IT requirements-gathering. Finally, although the SEC identified 4 of the 25 investments we reviewed as projects within the SEC's major IT investments reported to OMB,[18] OIT personnel managing 3 of those 4 projects did not hold a Federal Acquisition Certification for Program and Project Managers (FAC-P/PM), an equivalent level certification, or an extension or waiver as

[17] The remaining 13 investments we reviewed were not managed by integrated project teams.

[18] According to OMB Circular A-130, Revised, *Transmittal Memorandum No. 4*, *Management of Federal Information Resources*, November 2000; and OMB Memorandum M-10-27, *Information Technology Investment Baseline Management Policy*; June 28, 2010: A major [IT] investment is a system or acquisition requiring special management attention because of its importance to the mission or function to the Government; because it has significant program or policy implications, high executive visibility, high development, operating, or maintenance costs; because it uses an unusual funding mechanism; or because it is defined as such by the agency.

required by OMB and an SEC administrative regulation. According to OIT management, one of the three investments (the *Expanded Telework Hardware Requirements* project) was managed by an executive committee; however, OIT did not define a project charter describing the executive committee's composition, role, responsibilities, and authority.[19]

OMB's *Capital Programming Guide* states that agencies should establish integrated, dedicated project teams to maintain continuity and team accountability. Appendix 2 to the *Capital Programming Guide* also states that agencies should develop, maintain, and update as necessary project charters defining project teams' responsibilities and the authority and accountability for accomplishing project objectives.[20] Furthermore, OMB has stated that having skilled, competent, and professional program and project managers is essential to the success of critical agency missions, as project managers lead integrated project teams and ensure that requirements are appropriately written.[21] OMB further requires that program managers assigned to major acquisitions (as designated by the agency) hold a senior level certification or, at a minimum, be mid-level FAC-P/PM certified, unless the agency grants an extension or waiver. OMB also requires project managers assigned to lead projects within these major acquisitions to be, at a minimum, mid-level certified. In addition, the Software Engineering Institute recommends that organizations define the roles, responsibilities, and authority for the requirements-gathering or management process.[22] Finally, GAO has identified assigning responsibility for requirements-gathering as one of the key factors contributing to the successful completion of IT acquisitions.[23]

The SEC has also established administrative regulations requiring integrated project teams and FAC-P/PM certification. For example, according to SECR 24-02, SEC project teams shall be assigned appropriate subject matter experts such as a business sponsor, business lead, technical lead, and IT project manager (that is, project teams shall be integrated). In addition, SECR 10-29 (Rev. 1), *Federal Acquisition Certification for Program and Project Managers (FAC-P/PM) Program*, January 2015 (SECR 10-29) states that program managers for major investments "must have the FAC-P/PM senior level certification" and "project managers assigned to lead projects within these major acquisitions must have at a minimum the FAC-P/PM mid-level certification."

[19] OIT officials told us that, in July 2013, the Chairman's Deputy Chief of Staff established a committee of SEC senior officers to implement the newly negotiated Collective Bargaining Agreement. This committee was comprised of five sub-committees including the Information Technology subcommittee, chaired by the Chief Information Officer, and was charged with developing the standards and deploying the equipment issued to users of the expanded telework program.

[20] OMB Circular A-11, Revised, *Transmittal Memorandum No. 89, Preparation, Submission, and Execution of the Budget* (Appendix 2 of *Capital Programming Guide*); June 30, 2015.

[21] OMB Memorandum *Revisions to the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM)*; December 16, 2013.

[22] Carnegie Mellon Software Engineering Institute, *Capability Maturity Model® Integration (CMMI) for Development*, Version 1.3, CMU/SEI-2010-TR-033 (Hanscom AFB, Massachusetts: November 2010).

[23] U.S. Government Accountability Office, *Information Technology: Critical Factors Underlying Successful Major Acquisitions* (GAO-12-7, October 2011).

We determined that the SEC IT investments we reviewed were not consistently managed by integrated project teams because OIT did not have a mechanism in place to ensure that investments were staffed with integrated teams. In addition, although OIT policies and procedures indicated that subject matter experts shall be assigned to project teams and given responsibility to develop business requirements, OIT policies and procedures did not sufficiently define the roles and responsibilities for developing detailed, measurable requirements. Finally, OIT policies and procedures did not require project charters or include a mechanism to ensure that project managers assigned to lead projects within major IT investments hold a FAC-P/PM certification, equivalent level certification, or an extension or waiver.

By not ensuring that integrated project teams and, where necessary, certified individuals, managed the SEC's IT investments, OIT may not maintain continuity and team accountability in accordance with Federal guidance. In addition, not defining project teams' roles and responsibilities for requirements-gathering in documents such as project charters, in accordance with Federal and industry guidance, could adversely affect the SEC's ability to successfully complete agency IT investments as planned.

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

We encourage management to leverage the results of our audit as OIT continues its efforts to fully design and implement the SEC's requirements-gathering process, including the RCoE. We recommend that the Office of Information Technology:

Recommendation 1: Continue its efforts to design and implement a requirements-gathering process or framework that requires detailed, measurable requirements documents.

> **Management's Response.** The Office of Information Technology concurred with the recommendation and will continue its efforts towards the establishment of a robust Requirements Center of Excellence.
>
> **Office of the Inspector's (OIG) 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: Update applicable policies and procedures to reflect the new requirements-gathering process or framework referred to in Recommendation 1.

> **Management's Response.** The Office of Information Technology concurred with the recommendation and, as part of the Requirements Center of Excellence initiative, will take action to update applicable policies and procedures.
>
> **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 3: Establish documents, including project charters, to formally define and communicate the roles and responsibilities for the agency's information technology requirements-gathering process; and a mechanism to ensure that information technology investments are managed by integrated project teams with appropriate competencies and required certifications or waivers.

Management's Response. The Office of Information Technology concurred with the recommendation. The Office of Information Technology will ensure their Project Management Office establishes a Project Charter template that will be used to formally define and identify project roles and responsibilities, which can be leveraged for requirements-gathering tasks and to identify the integrated project teams. Further, the Office of Information Technology will continue to work with the Office of Acquisitions to ensure that project managers have the required certifications or waivers.

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: Opportunities Exist To Improve OIT's Oversight of the SEC's IT Investments and Their Underlying Requirements

We determined that opportunities exist to improve OIT's oversight of the SEC's IT investments and their underlying requirements. Specifically, we found that investments documents did not always demonstrate that OIT integrated security requirements into DME investment planning and initiation phases. In addition, OIT did not consistently review and coordinate IT investments—particularly steady state investments, investments to acquire technology equipment, and investments in Oracle support services—to prevent redundancy. Furthermore, aside from two investments we reviewed, governance authorities generally reviewed and approved changes to investments' baselines before implementation. As a result, OIT did not always comply with applicable Federal guidelines and its own policies and procedures. In addition, the SEC may not realize any cost savings from an effort to consolidate some contracts for Oracle support services, and may not have optimized its technology equipment purchases. We also question $24,230 paid to a contractor hired to gather requirements during a period when the corresponding project had no specific requirements-gathering activity.[24] Finally, we determined that the agency spent about $1 million to develop requirements that, according to the business sponsor, may in part need to be re-worked once a dependency (a separate system component) is completed, and about $600,000 for a project that was put on hold.

Investment Documents Did Not Always Demonstrate That OIT Integrated Security Requirements Into DME Investment Planning and Initiation Phases

Documents we reviewed supporting 11 of the 17 DME investments demonstrated that OIT addressed security requirements early in the investment planning and initiation phases in accordance with Federal guidelines and OIT policies and procedures.[25] However, for the remaining six DME investments we reviewed, investment documents did not demonstrate that OIT had integrated security requirements into the investment planning and initiation phases (which align with the selection phase of the CPIC process). Although OIT officials were able to demonstrate that they had addressed security requirements for these six DME investments at later stages in the process, Federal guidelines and OIT policies and procedures require OIT to address security requirements in all phases of the SDLC and CPIC process, including during investment planning and initiation.

[24] According to the Inspector General Act, as amended, "questioned costs" include costs questioned by the OIG because the expenditure of funds for the intended purpose is unnecessary or unreasonable.

[25] Documents reviewed included meeting minutes and materials from TRB open house meetings, completed TRB questionnaires, and e-mails from OIT Security personnel.

For example, NIST SP 800-64 describes the activities and outputs to integrate security considerations in each phase of the SDLC and throughout the CPIC process.[26] According to this guidance, incorporating security early on typically costs less than acquiring technologies that may later need to be reconfigured or customized, or that may provide more or fewer security controls than required. NIST further states that security should be included during the requirements-generation phase of any project, and that security requirements should be documented in specific and measurable terms to ensure that security controls are in place and functioning effectively. In accordance with this guidance, OIT's *Information Security Controls Manual* states that IT security requirements must be integrated into all stages of the SEC's system and services development and acquisition processes, or the SEC's CPIC processes. The *Information Security Controls Manual* also states that information system owners ensure that IT investment proposals taken to the PRB or the ITCPC are technically supportable and meet security requirements. Moreover, according to OIT's *Project Manager Resource Guide*, the selection phase of the CPIC process—which aligns with the SDLC planning and initiation phases—includes preparing a TRB questionnaire and identifying security requirements; in addition, the selection phase may include conducting a TRB open house review of projects for alignment with the SEC's enterprise architecture during that phase.

OIT did not consistently identify or document security requirements during investment planning and initiation phases for six of the DME investments we reviewed, in part, because OIT did not establish a mechanism or process to ensure that OIT personnel did so. By not consistently identifying or documenting security requirements during DME investment planning and initiation phases, OIT did not comply with those Federal guidelines and OIT policies and procedures that address the integration of security requirements in all phases of the SDLC. In addition, if project teams do not complete the TRB questionnaire, or if projects do not go through the TRB open house reviews during the SDLC planning and initiation phases, the SEC may be unaware whether the projects align with the agency's enterprise architecture until late in the acquisition. According to NIST 800-64, this could result in additional costs, delays, or unmet security requirements and vulnerabilities.

OIT Did Not Consistently Review and Coordinate IT Investments To Prevent Redundancy

We reviewed 25 IT investments and determined that OIT did not consistently review and coordinate IT investments to prevent redundancy. Specifically, we found that (1) OIT did not perform formal operational analyses of the eight steady state investments we reviewed to assess their continued need or ability to meet agency requirements, (2) OIT

[26] NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, Rev. 2; October 2008.

did not consistently coordinate and effectively monitor IT investments, and (3) IT investment documents did not consistently contain quality information impacting the investments.[27]

OIT Did Not Perform Formal Operational Analyses of Steady State Investments. Although OIT performed regular budget reviews of the SEC's IT investments, OIT did not perform formal operational analyses[28] for any of the eight steady state investments we reviewed to ensure that these investments continued to meet agency needs. In addition, investment boards' meeting minutes (specifically, ITCPC meeting minutes), did not demonstrate that governance authorities reviewed any of these eight steady state investments before funding, and the IOC did not review any of these steady state investments, as required by its charter. As of November 2015 (the time of our sample selection), the SEC had obligated about $49 million to these eight investments. For example, the SEC obligated and spent about $3 million for BlackBerry services in fiscal year (FY) 2015 without documented monitoring of device usage to minimize the risk of paying for unused or underused IT equipment.[29]

According to OMB's *Capital Programming Guide*, a formal operational analysis is warranted for every steady state project. Specifically, in describing operational analyses, the *Capital Programming Guide* states:

> A periodic, structured assessment of the cost, performance, and risk trends over time is essential to minimizing costs in the operational life of the asset. Beyond the typical developmental performance measures of cost and schedule performance, an operational analysis should seek to answer more subjective questions in the specific areas of: Customer Satisfaction; Strategic and Business Results; Financial Performance; and Innovation.

According to the *Capital Programming Guide,* in addressing customer satisfaction, an operational analysis should focus on whether an investment supports customer processes as designed and on how well the investment is delivering the goods or services it was designed to deliver. Strategic and Business Results from an operational analysis measure the effect an investment has on the organization itself and should provide a measure of how well the investment contributes to achieving the

[27] U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014), defines "quality information" as "information from relevant and reliable data that is appropriate, current, complete, accurate, accessible, and provided on a timely basis, and meets identified information requirements."

[28] Appendix 2 of *Capital Programming Guide*, *Supplement to Office of Management and Budget Circular A-11: Planning, Budgeting, and Acquisition of Capital Asset*s (June 2015) defines an operational analysis as a method of examining the ongoing performance of an operating asset investment and measuring that performance against an established set of cost, schedule, and performance goals.

[29] According to OIT officials, they received and reviewed monthly usage reports for BlackBerry services to identify and terminate devices that exceeded 90 days of non-usage. However, OIT management's detailed budget reviews, and OIT's reviews of monthly usage reports were not formal or documented to verify that investments continued to meet agency needs.

organization's strategic goals. In measuring the Financial Performance of an operating asset, the operational analysis should compare current performance with a pre-established cost baseline. Finally, the *Capital Programming Guide* states that addressing Innovation in the operational analysis is "an opportunity to conduct a qualitative analysis of the investment's performance in terms of the three previously mentioned areas. It also demonstrates that the agency has revisited alternative methods for achieving the same mission needs and strategic goals."

OMB further requires executive branch agencies to establish a policy for performing operational analyses of steady state investments.[30] Moreover, Executive Order 13589, *Promoting Efficient Spending* (November 2011), states that agencies should assess current device inventories and usage to ensure that they are not paying for unused or underused IT equipment, installed software, or services.

OIT did not perform and document formal operational analyses of the eight steady state investments we reviewed, in part, because OIT did not develop and implement a policy to periodically perform such analyses and ensure that each steady state investment continues to meet agency needs. In addition, OIT did not document the detailed reviews that were performed as part of the annual budgeting process, or other reviews performed to align steady state funding with current agency needs.

According to GAO, developing a policy and performing annual operational analyses ensures that steady state investments continue to meet agency needs.[31] GAO has also stated that it is important that agencies effectively manage steady state investments to ensure that the investments deliver value and do not unnecessarily duplicate or overlap other investments. Without periodic formal operational analyses of steady state investments, OIT may be unable to determine whether or how well steady state investments continue to meet agency needs.

OIT Did Not Consistently Coordinate and Effectively Monitor IT Investments. Of the 25 IT investments we reviewed, we found that OIT did not consistently coordinate 4 investments and effectively monitor 1 investment to align the investments with business needs and/or agency requirements. Federal and industry guidance and SECR 24-02 emphasize the need for portfolio management to provide an overall view of similar projects, prevent redundancy, consolidate activities, and optimize project costs, risks, and resources.[32]

---

[30] OMB M-10-27, *Information Technology Investment Baseline Management Policy*; June 28, 2010.

[31] U.S. Government Accountability Office, *Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments* (GAO-13-87, October 2012).

[32] Executive Order 13589, *Promoting Efficient Spending*; November 15, 2011.

OMB Circular A-130, Revised, *Management of Federal Information* Resources, November 2000.

Project Management Institute: *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Fifth Edition, Project Management Institute, Inc. (PMI), 2013.

According to SECR 24-02, the SEC's IT investment selection criteria should establish whether and "how the proposed IT investment has been evaluated to determine its benefits and risks from both business and technical perspectives," and cost benefit analysis may be used to perform this evaluation.

Coordinating IT Investments. OIT did not coordinate four IT investments we reviewed. Specifically, we found that OIT did not effectively coordinate the planning of the following two projects to acquire technology equipment such as printers, copiers, and computers: the *Equipment Inventory Restock* project and the *Expanded Telework Hardware Requirements* project. Each of the two projects cost about $1.5 million in FY 2014. However, OIT did not coordinate the equipment needs of the Equipment Inventory Restock project with the needs established as part of the *Expanded Telework Hardware Requirements* project. [33]

Similarly, OIT did not coordinate two Oracle-related multiyear investments we reviewed (the *Oracle Delivery Center* investment and the *Oracle Database Support Services* investment), with other existing Oracle-related investments. Based on our review of contracts supporting these investments and a contract supporting an existing Oracle-related investment (the *Oracle Platform Support Initiative*), we determined that the contracts had a similar scope of work. Specifically, the contracts are to provide OIT "with software engineering services to define, design, develop, integrate, test, deploy, maintain, troubleshoot, and enhance the functionality of applications using the Oracle platform."

According to OA officials, OIT coordinated the Oracle-related contracts, and it is not uncommon to establish contracts with the same or similar scope of work. OIT officials also stated that the contracts with similar language served similar tasks for different systems and did not overlap in scope. In addition, OIT officials told us that they coordinated the Oracle-related investments through the budget review process, which includes a consolidated management review of the steady state and DME requests. However, OIT budget reviews were not documented. Furthermore, we determined that an Oracle portfolio management effort is underway to consolidate four of the SEC's investments in the Oracle Fusion Middleware platform. Moreover, the Oracle portfolio management effort may not provide an overall view of the SEC's Oracle-related investments because it does not cover all Oracle Fusion Middleware investments and, according to OIT, it does not cover investments in Oracle legacy systems. OIT officials stated that these investments will be integrated at a future date.

The acquisition plan for the Oracle portfolio management effort states that the SEC seeks to combine its investments in the Oracle Fusion Middleware Platform "into one unified Oracle Portfolio Management requirement for efficiency and effectiveness." The acquisition plan also states that the annual independent Government cost estimate of the unified contract is about $12 million. OIT officials explained that they did not project any cost savings from the Oracle portfolio management effort, and the $12 million estimate covers the following:

- about $6 million for the four Oracle Fusion Middleware contracts to be consolidated;

[33] According to OIT management, the *Expanded Telework Hardware Requirements* project was driven by the SEC Chair's strategic priorities and OIT had a very short timeframe to address the project equipment needs, and limited opportunity to coordinate this project with similar equipment purchase projects.

- about $2 million in additional Oracle application O&M, break-fix, and portfolio management services;
- about $1 million in additional costs for projects going into production in FY 2017 using the Oracle Fusion Middleware Platform; and
- a "25-percent margin" (or about $2.3 million for cost overruns).

OIT did not coordinate investments to purchase technology equipment or investments in Oracle support services in accordance with Federal guidelines and its own policies and procedures, in part, because OIT did not have a process or mechanism to coordinate similar IT investments before funding, including a process to validate reported equipment inventory levels before making significant investments in IT systems. As a result, the SEC may not have optimized its technology equipment purchases. In addition, the SEC may not realize the anticipated efficiencies and effectiveness, or any cost savings from the Oracle portfolio management effort because OIT did not formally assess the potential cost benefits of this effort. In its 2011 report on the SEC's internal operations and structure, the Boston Consulting Group also noted that the agency's IT projects were "typically evaluated individually, without considering the full breadth of IT demand."

Monitoring IT Investment Activities. We also found that OIT did not effectively monitor the activities of one project we reviewed. The project (the *Investment Management Workflow System Requirements Gathering* project) included work performed by a contractor to elicit, analyze, and validate detailed requirements for the Division of Investment Management's workflow system. In FY 2014, the SEC obligated $575,000 for the project. We determined that, for 9 months (between March and November 2015), monthly status reports indicated that there was no specific requirements gathering activity under this contract. Nonetheless, OIT paid the contractor $24,230 during this period. According to OIT management, the contract task order was based on labor hours, and there were billable hours between March and November 2015 resulting from meetings and conversations between SEC and contractor staff and other "pre-work" that was necessary but did not result in contract deliverables. However, we question the payment of $24,230 because the project's scope was to gather requirements and no requirements-gathering activity occurred during that period.

OIT Implementing Instruction *Information Technology Investment Control* states that governance authorities conduct periodic reviews of the SEC's IT investments to ensure that investments continue to meet the agency's needs; identify areas where corrective actions may be needed; and determine whether to continue, change, or terminate an investment.[34] Furthermore, SECR 24-02 states that IT investments greater than $2 million with more than 6 months to complete from time of contract award "shall be subject to greater scrutiny and oversight."

[34] OIT Implementing Instruction II 24-02.01.02 (01.0), *Information Technology Investment Control*; January 9, 2008.

OIT did not effectively monitor the *Investment Management Workflow System Requirements Gathering* project in part because OIT did not have a mechanism or process in place to periodically review investments below the $2 million threshold, such as the *Investment Management Workflow System Requirements Gathering* project, to ensure those investments continue to meet the SEC's needs. In addition, OIT Implementing Instruction *Information Technology Investment Control* is outdated and does not specify criteria to determine whether to continue, change, or terminate an investment. As a result, the agency unnecessarily paid $24,230 to a contractor hired to gather requirements during period of no requirements-gathering activity.

IT Investment Documents Did Not Consistently Contain Quality Information Impacting the Investments. We found that the investment documents (including investment proposals and investment boards' meeting minutes) for 5 of the 17 DME investments we reviewed did not contain quality information impacting the investments. Such quality information included significant internal and external dependencies, changes, issues, or risks related to the investments.

For example, we reviewed the *electronic Filing for Administrative Proceedings* (*eFAP) II* project, which is a project to develop capabilities for uploading and distributing legal documents related to agency administrative proceedings. The project is dependent on completion of *eFAP I*, a separate project for the electronic submission of documents related to administrative proceedings.[35] We found that *eFAP II* investment documents reviewed by the PRB did not include evidence that the project team assessed the risks arising from a significant change in the *eFAP I* schedule. Specifically, before the PRB approved the *eFAP II* investment proposal, OIT postponed the completion of *eFAP I* from August 30, 2013, to November 7, 2014 (a period greater than 1 year). Nonetheless, the PRB approved the *eFAP II* investment proposal, including the project's high level requirements or business case, in November 2013, and beginning in September 2014, the agency began paying a contractor to develop *eFAP II* requirements.

Officials from the Office of the Secretary (the project's business sponsor) explained that, at the time of the *eFAP II* investment approval, the PRB knew of *eFAP I* delays and the Office of the Secretary did not deem the delays significant. In addition, OIT officials indicated that they noted the impact of the delays in monthly status reports (after *eFAP II* was approved), and they realized that they needed to "solidify the [*eFAP II*] requirements before development can start." On January 14, 2015, OIT officials reduced the *eFAP II* initial project scope to focus on requirements-gathering and transferred about $1.9 million from *eFAP II* to *eFAP I* to complete *eFAP I*. Between September 2014 and September 2015, the contractor completed the *eFAP II* requirements-gathering activity, for which the SEC paid about $1 million. However, according to the Office of the Secretary, the *eFAP II* requirements developed may in

[35] In February 2014, the SEC awarded a contract to design, develop, and implement the eFAP solution, including contract line items for *eFAP I* and an optional line item for *eFAP II*. The agency executed the *eFAP II* optional line item in September 2014.

part need to be re-worked or re-validated once *eFAP I* is completed. As of August 2016, *eFAP I* was still not complete and was scheduled to be completed at the end of October 2016.

For another project (the *Financial Data Mart [FDM]* project), the investment proposal reviewed by the PRB did not include evidence that the project team identified a significant project dependency and assessed the potential impact of the dependency on the project before the PRB approval. Between February and July 2014, the contractor for this project invoiced the agency about $600,000 for requirements gathered to consolidate data from multiple systems into a single platform (known as the *FDM*), including data from the Enterprise Services Center (ESC), operated by the Department of Transportation. The goal of the *FDM* project was to strengthen the SEC's ability to generate financial statements and other financial reports more efficiently. More than 80 percent of the data that the *FDM* project planned to centralize came from ESC by a daily transaction file. In FY 2014, the Department of Transportation initiated its own financial data mart project and told the SEC's Office of Financial Management (the *FDM* project business sponsor) that the daily transaction file would no longer be available at a future unspecified date.

We found that the *FDM* project documents (including the investment proposal and the PRB meeting minutes) did not identify ESC or the receipt of daily transaction files as a dependency or risk to the *FDM* project, or include an analysis or assessment of the potential impact of this dependency on the *FDM* project before the PRB approval. However, the Chief Financial Officer told us that the risk resulting from potential changes in the data structure of the feed from ESC was indeed realized, resulting in the project being put on hold until the ESC data mart structure becomes clear. Although OIT did not capture or include the dependency or risk in the investment proposal presented to the PRB, OIT considered the risk in the project's contractual documents (after investment approval).

According to OMB Circular A-11, agencies should identify key external factors that may significantly affect the achievement of the agency goal, and describe significant risks that may impact program delivery or outcome. Furthermore, according to GAO, oversight authorities should receive quality information such as significant matters relating to changes, issues, or risks impacting the entity or subject being overseen to ensure effective oversight.[36] Also, the *GAO IT Investment Management Framework* states that organizations should identify and analyze each project's risks and returns before committing significant funds to the project.[37] GAO has further stated that it is essential that all performance data including cost, schedule, benefits, risks, and system functionality (both expected and actual) are collected and distributed to investment

[36] U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO/AIMD-00-21.3.1, November 1999). In September 2014, GAO revised the Standards for Internal Control in the Federal Government (GAO-14-704G, September 2014). The revised standards were not effective until FY 2016, although agency management could have adopted them earlier.

[37] U.S. Government Accountability Office, *Information Technology Investment Management – A Framework for Assessing and Improving Process Maturity*, Version 1.1 (GAO-04-394G, March 2004).

boards. Finally, according to SECR 24-02, the CPIC process includes criteria to ensure that investments selected for funding have been evaluated to determine their benefits and risks from both business and technical perspectives.

IT investment documents did not consistently contain quality information impacting investments because OIT policies and procedures did not establish a mechanism to ensure that project teams consistently identify, analyze, and report to investment boards quality information related to IT investments before funding. Without early assessment and communication to the investment boards of the potential impact of issues, risks, and dependencies on IT projects, the agency spent about $1 million to develop requirements that may in part need to be re-worked or re-validated, and about $600,000 for a project that was put on hold. In its 2011 report, the Boston Consulting Group also noted that the SEC's governance authorities often evaluated IT investment proposals without sufficient information.

Governance Authorities Generally Reviewed and Approved Changes to Investments' Baselines Before Implementation, But Did Not for Two Investments We Reviewed

We determined that for 23 of the 25 investments we reviewed, CPIC governance authorities reviewed and approved changes in project baselines before the SEC implemented these changes. However, as further described below, governance authorities did not review and approve scope, cost, or schedule changes for the remaining two investments before implementation in accordance with OIT policies and procedures.

(b) (7)(E) In FY 2015, the contractual amount for the SEC's investment in (b) (7)(E) (b) (7)(E) (b) (7)(E) —was almost $2 million higher than the funding approved by the PRB. Specifically, according to the investment proposal and PRB meeting minutes, the PRB approved about $1.5 million for this project. However, OA (in collaboration with OIT) later executed a $3.4 million contract to purchase (b) (7)(E) (b) (7)(E) without documented evidence of CPIC governance authorities' approval of the increased cost. According to OA and OIT officials, the $3.4 million contract combined various requisitions for (b) (7)(E).

In addition, OIT changed the project scope without a documented governance authority's approval. OIT changed the scope by redirecting part of the equipment planned for SEC's (b) (7)(E) as a short-term solution to provide new (b) (7)(E) to meet that office's needs. (b) (7)(E) specifications were not provided to the project team at project initiation. However, OIT officials did not view redirecting equipment from the (b) (7)(E) as a change in project scope even though the approved investment proposal explicitly stated that the intended purpose of the equipment was to replace (b) (7)(E)

Investment Management Workflow Requirements-Gathering Project. Similarly, before obtaining approval from CPIC governance authorities, OA in collaboration with OIT executed a zero-cost contract extension that changed the project schedule for the *Investment Management Workflow Requirements-Gathering* project. The zero-cost extension postponed the project completion date by 6 months from January to July 2016. According to OA and OIT officials, OA and OIT were in constant communication throughout the procurement process, and governance authorities approved the change in project schedule within 1 month after the contract extension.

According to OMB, agency policies should include a baseline validation process and address acceptable reasons for revising a baseline, including significant changes in investment goals (scope, requirements, or objectives) resulting from internal or external management decisions, or changes in funding level or availability of funds.[38] In addition, the GAO IT *Investment Management Framework* states that the relationship between investment boards and management must be documented and agreed upon by all parties. Finally, SECR 24-02 states "any changes to an investment's scope, cost, or schedule, shall require additional CPIC governance authority review and approval prior to implementation." In addition, OIT policies and procedures state that the Chief Information Officer has the authority to approve investments costing $2 million or less.

OA executed contractual actions for the (b) (7)(E) (b) (7)(E) project and *Investment Management Workflow Requirements-Gathering* project without the appropriate CPIC governance authorities' approval, in part, because a mechanism did not exist to ensure that investment boards' approvals were obtained before executing contract actions. In addition, OIT policies and procedures did not address acceptable reasons for revising project baselines.

By implementing changes to investments' baselines without prior approval from CPIC governance authorities, including, where applicable, the Chief Information Officer, OIT did not comply with applicable Federal guidelines and OIT policies and procedures. In addition, by redirecting (b) (7)(E) OIT postponed the replacement of (b) (7)(E) (b) (7)(E) As a result, the SEC risked a potential increase in its operational and security risk exposure.

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

We encourage management to leverage the results of our audit as OIT continues to improve the oversight of the SEC's IT investments. We recommend that the Office of Information Technology:

[38] OMB M-10-27, *Incorporating and Funding Security in Information Systems Investments*, June 2010.

Recommendation 4: Formally assess the Oracle consolidation effort and identify any anticipated efficiencies, effectiveness, and cost savings.

Management's Response. The Office of Information Technology concurred with the recommendation and will take action to formally assess the Oracle consolidation effort.

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: In coordination with the Office of Acquisitions, develop and implement a process or mechanism to coordinate similar information technology investments as part of the approval and funding process.

Management's Response. The Office of Information Technology concurred with the recommendation and will work with the Office of Acquisitions to develop and implement a process or mechanism to coordinate similar technology investments as part of the approval and funding process.

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: Develop and implement a policy to periodically perform and document formal operational analyses of steady state investments in accordance with Office of Management and Budget requirements, and clarify investment boards' relationships and responsibility to review steady state investments to minimize overlaps or gaps in steady state investments.

Management's Response. The Office of Information Technology concurred with the recommendation and will update applicable policies and procedures to clarify roles and responsibilities of oversight bodies. Management's response also indicates that the Office of Information Technology will implement a policy to periodically perform and document formal operational analyzes of steady state investments.

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: Update its policies and procedures to:

(a) require that security requirements are defined and documented during the planning and initiation phases of every project;

(b) consider implementing a process to periodically review information technology investments that fall below the $2 million threshold;

(c) implement a mechanism so that project teams consistently identify, assess, and report to investment boards quality information (such as risks, issues, changes, and dependencies) impacting information technology investments before funding; and

(d) specify acceptable reasons for revising project baselines (or implementing project changes), including criteria to determine whether to continue, change, or terminate an investment;

(e) define a process to ensure that changes to project baselines are approved by investment boards before executing contractual actions, and coordinate this activity with the Office of Acquisitions.

Management's Response. The Office of Information Technology (OIT) concurred with the recommendation and will assess the need to ensure that security requirements are further documented to augment the SEC's information security control manual. In addition, OIT will make adjustments to the criteria as needed to ensure that it addresses investments under the $2 million threshold. Furthermore, OIT will assess the current investment proposal information required to ensure that project teams consistently identify, assess, and report to investment boards quality information impacting information technology investments before funding. OIT will also assess the current change request information required to ensure that they specify acceptable reasons for revising project baselines. Moreover, OIT will coordinate the Office of Acquisitions and assess applicable processes to ensure they adequately address steps necessary to ensure that changes to project baselines are approved by investment boards before executing contractual actions.

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.

Appendix I. Scope and Methodology

We conducted this performance audit from November 2015 through September 2016 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. The audit covered the SEC's IT investments funded between October 1, 2013, and November 25, 2015. We conducted fieldwork at the SEC's Headquarters in Washington, DC, focusing on the SEC's activities to identify, validate, and document detailed, measurable IT requirements. Our overall objective was to evaluate the SEC's IT requirements-gathering process. Specifically, we sought to determine whether the SEC's IT requirements-gathering process was:

1. sufficiently designed and complied with applicable Federal laws, regulations, and industry guidelines; and

2. consistently applied in accordance with Federal and agency policies, and facilitated the effective and efficient procurement or development of IT projects.

Methodology. To address our objectives, we reviewed Federal laws and guidance; SEC regulations, policies, and procedures, and industry guidelines that address IT requirements-gathering. The documents we reviewed included:

Federal Laws and Guidance:

- Clinger-Cohen Act of 1996 (also called National Defense Authorization Act for Fiscal Year 1996), Pub. L. No. 104-106; February 10, 1996.
- Federal Information Technology Acquisition Reform Act (as part of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015); December 19, 2014.
- Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, December 2014.
- E-Government Act of 2002, Pub. L. No. 107-347; December 17, 2002.
- Federal Acquisition Regulation, Volume 1, Parts 1-51, March 2005.
- Executive Order 13589, *Promoting Efficient Spending*; November 15, 2011.
- OMB Circular A-11, Revised, *Transmittal Memorandum No. 89, Preparation, Submission, and Execution of the Budget*; June 30, 2015.
- OMB Circular A-130, Revised, *Transmittal Memorandum No. 4, Management of Federal Information Resources*, November 2000.

- OMB Memorandum, *The Federal Acquisition Certification for Program and Project Managers*; April 25, 2007.
- OMB Memorandum, *Revisions to Federal Acquisition Certification for Program and Project Managers (FAC-P/PM)*; December 16, 2013.
- OMB Memorandum M-15-14, *Management and Oversight of Federal Information Technology*; June 10, 2015.
- OMB Memorandum M-10-27, *Information Technology Investment Baseline Management Policy*; June 28, 2010.
- U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO/AIMD-00-21.3.1, November 1999), and its revised version, GAO-14-704G, September 2014.
- NIST SP 800-64, S*ecurity Considerations in the System Development Life Cycle*, Rev. 2; October 2008.

SEC Regulations, Policies, and Procedures:

- SECR 24-1.6, *Enterprise Architecture*, Rev. 1; April 23, 2015.
- SECR 24-02, *Information Technology Capital Planning and Investment Control*, Rev. 2, April 2015.
- SEC OIT Implementing Instruction 24-02.01.01 (01.0), *Information Technology Investment Initiation*, May 2005.
- SEC OIT Implementing Instruction 24-02.01.02 (01.0), *Information Technology Investment Control*; January 9, 2008.
- SEC OIT *Project Life Cycle Framework – Project Manager Resource Guide*, February 2015.
- SECR 24-04A *Information Security Controls Manual*, Rev 2.1; November 10, 2015.
- SECR 10-29 (Rev.1.0) *Federal Acquisition Certification For Program and Project Managers (FAC-P/PM) Program*, January 2015.

Industry Guidance

- Carnegie Mellon Software Engineering Institute, *Capability Maturity Model® Integration (CMMI) for Development,* Version 1.3, CMU/SEI-2010-TR-033 (Hanscomb AFB, Massachusetts: November 2010).
- Project Management Institute: *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Fifth Edition, Project Management Institute, Inc. (PMI), 2013.

We also selected a nonstatistical sample of 25 of the SEC's 692 IT investments funded between October 1, 2013, and November 25, 2015, as recorded in OIT's financial

system. As of November 2015 (the time of our sample selection), the SEC had spent about $83 million for the 25 IT investments selected for review. We selected our sample by FY and across SEC divisions and offices, and we included investments managed by different contractors. We also selected a variety of investments including those related to IT infrastructure, office automation, telecommunication, application design and supporting platforms, EDGAR, and IT security. For each of the 25 IT investments selected for review, we (1) interviewed OIT staff, project managers, and business stakeholders; and (2) reviewed project and procurement documents, including investment approval documents, contracts, and documentation of project team composition, roles, responsibilities, and qualifications, as applicable. Because we selected a nonstatistical sample, we did not project our results and conclusions to the total population of SEC IT investments funded during the period reviewed. Appendix III shows the 25 IT investments included in our sample.

Internal Controls. Consistent with our objectives, we reviewed the SEC's controls over its IT requirements-gathering process. We did not assess OIT's overall internal control structure. We relied on interviews with OIT personnel and information requested from and supplied by OIT staff, including OIT's 2015 management assurance statement and Risk and Control Matrix. We reviewed OIT's 2015 management assurance statement and Risk and Control Matrix to identify and evaluate management's assessment of internal controls and any material weaknesses relevant to our audit objectives, consistent with GAO's *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014). As discussed in this report, we identified internal control weaknesses related to the SEC's IT requirements-gathering process and OIT's oversight and monitoring of the SEC's IT investments. Our recommendations, if implemented, should correct the weaknesses we identified.

Computer-processed Data. GAO's *Assessing the Reliability of Computer-Processed Data* (GAO-09-680G, July 2009) states, "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 your 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 investment reports from OIT's financial system, documents from the SEC's procurement system, and IT investment records from OIT's portfolio management system. We did not test these systems as such testing was not part of our objectives. However, we assessed

the reliability of the computer-processed data we relied on by (1) interviewing OIT management knowledgeable about the data source, (2) reconciling the amounts reported in OIT's financial system with the SEC's financial reporting system, and (3) reviewing individual procurement and investment records. Based on our assessment, we determined that the data were sufficiently reliable to support our conclusions.

Prior Coverage. During the last 6 years, the SEC OIG issued one report related to IT investment oversight and acquisition: *Assessment of the SEC Information Technology Investment Process*, Report No. 466; March 26, 2010. The report identified inconsistencies in implementing the SEC's CPIC policies and procedures and a lack of effective project management, and stated that significant decisions were made about SEC IT investments without meaningful reviews by appropriate boards. The report made nine recommendations intended to improve the SEC's CPIC process and oversight of agency IT investments. Although the recommendations are closed, we found that oversight of the SEC's IT investments was not always effective, as discussed in this report.

In addition, in May 2015, the OIG issued a management letter related to the SEC's Tips, Complaints, and Referrals Intake and Resolution System (TCR system): *Final Management Letter: Observations Noted During TCR System Audit Support Engagement*; May 20, 2015. The letter identified various factors that led to schedule delays and cost increases in the agency's project to (1) elicit requirements, (2) design, and (3) deploy a redesigned TCR system. Such factors included unacceptable contractor performance, ineffective project management and control, and a lack of adequate contractor and Government resources to timely address project concerns. The letter requested that the SEC provide the OIG information about its plans to implement the redesigned TCR system. As of the date of this report, the redesigned TCR system is scheduled to go live in November 2016 (more than 2 years after its original go-live date of July 21, 2014).

Unrestricted SEC OIG reports can be accessed at: http://www.sec.gov/about/offices/oig/inspector_general_audits_reports.shtml.

GAO also issued the following reports of particular relevance to our objectives:

- *Information Technology Investment Management – A Framework for Assessing and Improving Process Maturity*, Version 1.1 (GAO-04-394G, March 2004).
- *Additional Actions and Oversight Urgently Needed to Reduce Waste, and Improve Performance in Acquisitions and Operations* (GAO-15-675T, June 2015).
- *Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments* (GAO-13-87, October 2012).
- *USDA Systems Modernization – Management and Oversight Improvements Are Needed* (GAO-11-586, July 2011).

- *Information Technology – Critical Factors Underlying Successful Major Acquisitions* (GAO-12-7, October 2011).
- *United States Coast Guard – Improvements Needed in Management and Oversight of Rescue System Acquisition* (GAO-06-623, May 2006).
- *High-Risk Series – An Update* (GAO-15-290, February 2015).

Unrestricted GAO reports can be accessed at: http://www.gao.gov/.

Appendix II. Summaries of the SEC's SDLC Phases and IT Investment Boards

Tables 1 and 2 provide summaries of the SEC's SDLC phases and IT Investment Boards.

Table 1. Summary of the SEC's SDLC Phases

SDLC Phase	Phase Description Including Requirements-Gathering Elements
Initiation	Activities to define the overall parameters of an IT project and to establish the appropriate project management and quality measures required to complete the project. Activities related to requirements-gathering include creating a project charter and defining the project's objectives, scope, purpose, and deliverables.
Planning	Activities to determine an approach for accomplishing the business need. Activities related to requirements-gathering include refining user requirements and developing plans for the overall technical solution and approach. Deliverables include requirements documents.
Design	Activities to demonstrate compliance with the SEC enterprise, data, and technical architecture, outline, and document-specific components of the technical solution and deployment strategy. Activities related to requirements-gathering include analyzing and refining requirements. Deliverables include the requirements traceability matrix and detailed architecture design document.
Development	Activities to transform the design blueprint into a working system that satisfies the requirements defined in earlier phases.
Independent Test	Activities to validate that the solution developed satisfies all defined requirements.
Deployment	Activities to confirm the operational readiness of the solution for deployment to the production environment.
Project Close	Activities necessary to close out the project, including analyzing the project to review successes and shortcomings and capture lessons learned.
Operations & Maintenance (O&M)	Activities for the ongoing monitoring of system performance in accordance with user requirements.
Retirement	Activities to initiate the retirement process when the business no longer needs the product or when OIT implements a replacement system.

Source: OIG generated based on *OIT Project Life Cycle Framework - Project Manager Resource Guide*.

Table 2. Summary of the SEC's IT Investment Boards

Boards and Sample of Boards' Roles and Responsibilities	Board Composition
ITCPC. Oversees the SEC's CPIC process and approves the method of prioritizing IT investments by their relative importance to the agency's overall mission; provides executive-level direction to ensure shared benefits or costs of inter-agency solutions are considered; and approves OIT's operating budget and recommends the allocation of budget resources across IT investments.	Composed of 11 senior executives who represent the enterprise IT and various agency business units.
PRB. Implements direction from the ITCPC; reviews and evaluates IT investments' progress against milestones and cost, schedule, and performance goals; and reviews investment plans (or proposals) and ensures that such plans accurately describe the investment scope, requirements, life costs, schedule, and risks.	Composed of 16 voting members and 2 advisory members, including the OA Assistant Director and assistant directors from various OIT branches.
IOC. Implements direction from the ITCPC; approves IT investments costing more than $2 million; determines whether investment proposals meet business needs, are appropriate, and maximize inter-office support; and reviews steady state funding for alignment with IT operating needs.	Composed of 15 senior officers from various SEC divisions and offices, including senior officers from OA and the Chief Information Officer.
TRB.[39] Reviews new technology solutions, existing technology upgrades, architecture changes, and other efforts impacting the SEC environment for alignment with the SEC's Enterprise Architecture; and identifies potential risks and provides recommendations to minimize impacts to current systems, infrastructure, and IT services.	Composed of the Chief Enterprise Architect, OIT branch chiefs, support staff, and subject matter experts from various OIT branches, including representatives from OIT Security.

Source: OIG-generated based on each investment board's charter.

[39] The TRB is not an investment board; however, we included the TRB in Table 2 because the TRB may be involved in selecting IT investments as part of the SEC's CPIC process.

Appendix III. SEC IT Investments Reviewed

Tables 3 and 4 provide details about the 25 SEC steady state and DME investments we reviewed.

Table 3. SEC Steady State Investments Reviewed

FY	Investment Name	Investment Purpose	Investment Funds Committed
2014	1. Data WAN Circuits	To support the agency wide area network, Metro Area Network, Internet services, and support provided under multiple contracts.	$5,494,323
	2. Enterprise Operations Maintenance & License Renewals	To provide maintenance support services and license renewals for OIT Servers and Storage Branch.	$6,942,614
FY 2014 Steady State Investments Total			**$12,436,937**
2015	3. ISS - Incremental Funding	To support agency-wide IT infrastructure services contracts such as the IT Help Desk.	$22,085,442
	4. Content Management Application Maintenance Support	To cover costs associated with the maintenance of various applications in production at the SEC.	$7,289,243
	5. BlackBerry Services	To provide BlackBerry devices and services to SEC employees.	$3,050,324
	6. Data Center O&M	To support the agency's New Jersey data center.	$2,030,000
FY 2015 Steady State Investments Total			**$34,455,009**
2016	7. Oracle database support services (or Sybase, SQL, Oracle DBA O&M Services)	To continue providing various database support services.	$1,267,661
FY 2016 (as of November 2015) Steady State Investments Total			**$1,267,661**
TOTAL FUNDS OBLIGATED FOR STEADY STATE INVESTMENTS REVIEWED			**$48,159,607**

Source: OIG-generated based on information from OIT's financial system.

Table 4. SEC DME Investments Reviewed

FY	Investment Name	Investment Purpose	Investment Funds Committed
2014	8. Equipment Inventory Restock	To cover costs associated with various IT equipment purchases.	$1,585,313
	9. Expanded Telework Hardware Requirements	To purchase equipment for telework purposes.	$1,527,553
	10. Investment Management Workflow System - Requirements Gathering	To provide requirements support services for the Division of Investment Management and the Office of Credit Ratings.	$575,000
	11. Financial Data Mart (or EDW & FDM Planning and Requirements-Gathering Services Only)	To gather requirements for a centralized financial database for the Office of Financial Management and Division of Enforcement.	$722,782
	12. Oracle Delivery Center	To establish an Oracle Delivery Center to align Oracle-based projects with the agency's enterprise architecture, and to handle small to medium Oracle-based projects.	$3,172,970
	13. Electronic Filing for Administrative Proceedings "eFAP" Phase II	To extend the Phase I functionality through a business process re-engineering effort and by consolidating legacy systems. The project was de-scoped to requirements-gathering.	$3,291,170[40]
	14. Next-Generation Threat Prevention: Intrusion Prevention Sensors Modernization	To consolidate two existing platforms and implement an intrusion prevention/intrusion detection solution.	$3,696,341
	15. Regional Office Relocation Upgrades	To relocate or renovate six SEC regional offices.	$767,407
	16. FY 2014 TRENDS Development and Enhancements	To develop and implement users' recommended enhancements and to address bugs identified in the current version of TRENDS used by the Office of Compliance, Inspections, and Examinations as a document management system.	$5,598,993
FY 2014 DME Investments Total			**$20,937,529**

[40] CPIC governance authorities initially approved $1.2 million for this project and subsequently increased the project funding by obligating about $3.3 million for the project in FY 2014.

FY	Investment Name	Investment Purpose	Investment Funds Committed
2015	17. Analytic Tools and Platform	To cover costs for a 6-month extension of a contract to provide training and support services for the Analytics Tools and Platform.	$1,888,609
	18. Storage Infrastructure FY 2015 Updates/ Enhancements	To replace storage infrastructure that reached its end of life, and to migrate an application to a clustered environment.	$3,537,552
	19. EDGAR Fee System Modernization	To cover costs for replacing EDGAR Momentum and improving the EDGAR filing system.	$3,768,565
	20. Enterprise Data Analytics Platform (EDAP) II	To cover costs for the operation and maintenance, training, and user support for EDAP II, with options for enhancements to the platform.	$1,668,800
	21. Broker-Dealer Risk Assessment Solution	To replace the broker-dealer risk assessment internal application being used by the Risk Management Program in the Division of Trading and Markets.	$413,465
	22. OHR Process Automation Phase 3	To add modules or functionalities to the Office of Human Resources' process automation platform.	$911,936
	23. SEC.gov Modernization FY 2014	To enhance SEC.gov based on requirements from the Office of Public Affairs.	$821,658
	24. OIDS - Requirements and Design	To develop requirements and design a solution to update the Division of Economic and Risk Analysis Application.	$491,590
FY 2015 DME Investments Total			**$13,502,175**
2016	25. Webcasting	To cover costs for continued content delivery services for SEC web sites such as SEC.gov.	$813,440
FY 2016 (as of November 2015) DME Investments Total			**$813,440**
TOTAL FUNDS OBLIGATED FOR DME INVESTMENTS REVIEWED			**$35,253,144**

Source: OIG-generated based on information from OIT's financial system.

Appendix IV. Management Comments

MEMORANDUM

September 27, 2016

To: Rebecca Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects, Office of Inspector General

From: Jeffery Heslop, Chief Operating Officer /s/

Subject: Management Response to Draft Report No. 538 – Audit of the SEC's Information Technology Requirements-Gathering Process

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft recommendations related to its audit of the SEC's Information Technology Requirements-Gathering Process (Report No. 538). We value the independent insights and opinions of our auditors and the perspective they provide.

The SEC is committed to ensuring its information technology (IT) projects are managed in a responsible, consistent, and effective manner consistent with Federal requirements and proven project-management best practices. The Office of Information Technology (OIT) is responsible for the development of IT solutions to provide the SEC's Offices and Divisions the tools they need to execute the Commission's regulatory mission. In April of 2015, prior to the OIG's initiation of this report, the OIT began its work to develop a Requirements Center of Excellence (RCoE). The goal of the RCoE is to enhance the OIT's requirements development capabilities through the implementation of a robust project management framework, the development of standardized templates and project reporting tools, and definition of performance metrics. OIT is on schedule to fully deploy the RCoE by December of 2016.We believe the RCoE will enable the SEC to enhance our project management practices, while helping to ensure OIT can continue to deliver quality and effective information technology solutions.

Report No. 538 contains seven recommendations with which the SEC concurs. Below, I have indicated the actions we have taken or intend to take for each recommendation.

I look forward to continuing our productive dialogue in the coming months on the SEC's efforts to address the areas noted in your report. I appreciate your continued support and the valuable assistance and guidance from your staff. If you have any questions, or you would like to discuss this response in more detail, please contact me at (202) 551-2105.

Recommendation 1: Continue its efforts to design and implement a requirements-gathering process or framework that requires detailed, measurable requirements documents.

Response: Concur. The OIT is working towards the establishment of a robust RCoE.

Recommendation 2: Update applicable policies and procedures to reflect the new requirements-gathering process or framework referred to in Recommendation 1.

Response: Concur. As part of the RCoE initiative, the OIT will take action to update applicable policies and procedures. OIT anticipates implementing a policy mandating the use of the RCoE.

Recommendation 3: Establish documents, including project charters, to formally define and communicate the roles and responsibilities for the agency's information technology requirements-gathering process; and a mechanism to ensure that information technology investments are managed by integrated project teams with appropriate competencies and required certifications or waivers.

Response: Concur. The OIT will ensure our Project Management Office establishes a Project Charter template that will be used to formally define and identify project roles and responsibilities, which can be leveraged for requirements-gathering tasks and to identify the integrated project teams. The OIT will continue to work with the Office of Acquisitions (OA) to ensure that project managers have the required certifications or waivers.

Recommendation 4: Formally assess the Oracle consolidation effort and identify any anticipated efficiencies, effectiveness, and cost savings.

Response: Concur. The OIT will take action to formally assess the Oracle consolidation effort.

Recommendation 5: In coordination with the Office of Acquisitions, develop and implement a process or mechanism to coordinate similar information technology investments as part of the approval and funding process.

Response: Concur. The OIT will work with the OA, and continue to utilize the IT Project Review Board, to develop and implement a process or mechanism to coordinate similar information technology investments as part of the approval and funding process.

Recommendation 6: Develop and implement a policy to periodically perform and document formal operational analyses of steady state investments in accordance with Office of Management and Budget requirements, and clarify investment boards' relationships and responsibility to review steady state investments to minimize overlaps or gaps in steady state investments.

Response: Concur. The OIT will take action to ensure applicable policies and/or procedures are updated to clarify roles and responsibilities for applicable oversight bodies and implement a policy to periodically perform and document formal operational analyses of steady state investments in accordance with Office of Management and Budget requirements.

2

Recommendation 7: Update its policies and procedures to:

(a) require that security requirements are defined and documented during the planning and initiation phases of every project;

(b) consider implementing a process to periodically review information technology investments that fall below the $2 million threshold;

(c) implement a mechanism so that project teams consistently identify, assess, and report to investment boards quality information (such as risks, issues, changes, and dependencies) impacting information technology investments before funding; and

(d) specify acceptable reasons for revising project baselines (or implementing project changes), including criteria to determine whether to continue, change, or terminate an investment;

(e) define a process to ensure that changes to project baselines are approved by investment boards before executing contractual actions, and coordinate this activity with the Office of Acquisitions.

Response: Concur. The OIT will assess the need to ensure that security requirements are further documented to augment the SEC's information security control manual, which is developed in accordance with NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

Specific to implementing a process to periodically review information technology investments that fall below the $2 million threshold, OIT currently holds recurring project review meetings and is finalizing an effort to formally expand that review for projects that fit specific criteria. OIT will make adjustments to the criteria as needed to ensure that it addresses investments under the $2 million threshold.

OIT will assess the current investment proposal information required to ensure that project teams consistently identify, assess, and report to investment boards quality information impacting information technology investments before funding. OIT will also assess the current change request information required to ensure that they specify acceptable reasons for revising project baselines.

OIT will coordinate the OA and assess applicable processes to ensure they adequately address steps necessary to ensure that changes to project baselines are approved by investment boards before executing contractual actions.

3

Major Contributors to the Report

Kelli Brown-Barnes, Audit Manager

Sara Tete Nkongo, Lead Auditor

Jacob Dull, 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.