



U.S. Securities and Exchange Commission
Office of Inspector General
Office of Audits

The SEC Has Processes To Manage Information
Technology Investments But Improvements Are
Needed



September 19, 2019
Report No. 555

REDACTED FOR PUBLIC RELEASE



OFFICE OF
INSPECTOR GENERAL

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

M E M O R A N D U M

September 19, 2019

TO: Kenneth Johnson, Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General 

SUBJECT: *The SEC Has Processes to Manage Information Technology Investments But Improvements Are Needed, Report No. 555*

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) fiscal year 2018 information technology (IT) investments. The report contains five recommendations that should help improve the SEC's management of IT investments.

On August 21, 2019, we provided management with a draft of our report for review and comment. In its September 5, 2019, response, management concurred with our recommendations. We have included management's 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 management 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: Jay Clayton, Chairman
Sean Memon, Chief of Staff, Office of Chairman Clayton
Bryan Wood, Deputy Chief of Staff, Office of Chairman Clayton
Peter Uhlmann, Managing Executive, Office of Chairman Clayton
Kimberly Hamm, Chief Counsel/Senior Policy Advisor, Office of Chairman Clayton
Robert J. Jackson Jr., Commissioner
Prashant Yerramalli, Counsel, Office of Commissioner Jackson
Hester M. Peirce, Commissioner
Jonathan Carr, Counsel, Office of Commissioner Peirce
Elad Roisman, Commissioner
Matthew Estabrook, Counsel, Office of Commissioner Roisman

REDACTED FOR PUBLIC RELEASE

Allison Herren Lee, Commissioner
Andrew Feller, Counsel, Office of Commissioner Lee
Gabriel Benincasa, Chief Risk Officer
John Nester, Director, Office of Public Affairs
Robert B. Stebbins, General Counsel
Holli Heiles Pandol, Director, Office of Legislative and Intergovernmental Affairs
Charles Riddle, Acting Chief Information Officer, Office of Information Technology
Jeffrey Stagnitti, Associate Director and Managing Executive, Office of
Information Technology
Vance Cathell, Director, Office of Acquisitions
Gregory Steigerwald, Competition Advocate, Office of Acquisitions

Executive Summary

The SEC Has Processes To Manage Information Technology Investments But Improvements Are Needed

Report No. 555
September 19, 2019

Why We Did This Audit

In fiscal year (FY) 2018, the U.S. Securities and Exchange Commission (SEC or the agency) spent about \$307 million on 515 information technology (IT) investments (for the purpose of this report, “spent” includes amounts obligated in FY 2018 to related contracts). This represented about 18 percent of all funding available to the SEC that year. The Government Accountability Office (GAO) has reported that Federal IT investments have too often failed, incurred cost overruns and schedule slippages, or contributed little to mission-related outcomes. Since 2015, GAO has included “Improving the Management of IT Acquisitions and Operations” in its list of government-wide high-risk areas needing attention by the executive branch and Congress.

We conducted this audit to assess the SEC’s management of its FY 2018 IT investments, and to determine whether the agency used funds allocated to those investments for their intended purposes, selected investments for funding in accordance with established processes, and had effective controls for ensuring investments meet established cost, schedule, and performance goals.

What We Recommended

We made four recommendations to improve the SEC’s management of IT investments, including recommendations to update the SEC’s capital planning and investment control policies and procedures and to provide training to personnel with investment oversight and program management responsibilities. We also made one recommendation to improve the SEC’s contract management by establishing documentation requirements for thoroughly supporting independent Government cost estimates. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action. This report contains non-public information about the SEC’s information technology program. As a result, the SEC OIG redacted the non-public information to create this public version.

What We Found

We determined that the SEC increased its funding for IT initiatives over the FY 2017 level as required by the Consolidated Appropriations Act, 2018. In addition, the agency used funds allocated to the 11 IT investments we judgmentally selected for review for their intended purposes.

However, the SEC’s management of steady state investments (investments to maintain and operate IT assets in a production environment) needs improvement, because the SEC’s Office of Information Technology (OIT) did not view such investments as IT investments for the purposes of capital planning and investment control. The SEC’s spending on steady state investments has gradually increased in recent years and, in FY 2018, steady state investments represented 71 percent of the agency’s total IT investment expenditures (that is, \$217 million of the \$307 million spent that year). Improving agency management of steady state investments could promote more effective decision-making and provide greater assurance that such investments (1) deliver value, (2) do not unnecessarily duplicate or overlap with other investments, and (3) continue to meet the SEC’s needs.

In addition, the SEC can better manage and document deviations from approved plans for investments to develop, modernize, and enhance IT assets (referred to as DME investments). Five of the six DME investments we reviewed were rebaselined in FY 2018; however, we could not always determine compliance with aspects of the SEC’s capital planning and investment control policy that address managing and documenting deviations from approved investment plans. This occurred because OIT had not established detailed formal rebaselining procedures. Without procedures that ensure a complete and accessible audit trail of each investment’s lifecycle, the SEC’s rebaselining processes may lack the transparency needed to ensure effective oversight of its DME investments.

Also, 5 of the 11 IT investments we reviewed involved purchases of hardware assets. We found that OIT needs to improve the documentation of hardware assets investment planning and to demonstrate investment outcomes because OIT had not established processes to do so. Without such processes, the SEC risks hardware assets in use reaching their end-of-life/end-of-service, thereby increasing the risk of equipment failure and the potential for data loss.

Finally, the SEC’s Office of Acquisitions extended on a sole-source basis two contracts for IT acquisitions we reviewed without adequate documentation to support independent government cost estimates used for the estimated extension prices. This occurred, in part, because guidance that urged personnel to document any and all methods used to complete independent government cost estimates was “for informational purposes” and contracting officials did not use it.

During our audit, two other matters of interest that did not warrant recommendations came to our attention. These matters related to the SEC’s selection of its enterprise IT project and portfolio management system, and contract actions impacting the SEC’s data centers. We discussed these matters with agency management for their consideration.

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

TABLE OF CONTENTS

Executive Summary i

Abbreviations iii

Background and Objectives 1

 Background 1

 Objectives 6

Results 8

 Finding 1. The SEC Increased Funding for IT Initiatives as Required, and Used Funds Allocated to the IT Investments We Reviewed for Their Intended Purposes 8

 Finding 2. The SEC’s Management of Steady State Investments Needs Improvement..... 9

 Recommendation, Management’s Response, and Evaluation of Management’s Response 12

 Finding 3. The SEC Can Better Manage and Document Deviations From Approved DME Investment Plans 13

 Recommendations, Management’s Response, and Evaluation of Management’s Response 16

 Finding 4. The SEC Can Better Plan and Manage Investments in Hardware Assets To Achieve Expected Outcomes or Goals 18

 Recommendation, Management’s Response, and Evaluation of Management’s Response 20

 Finding 5. The SEC Can Improve Its Support for Independent Government Cost Estimates..... 21

 Recommendation, Management’s Response, and Evaluation of Management’s Response 24

Other Matters of Interest..... 25

Figures and Tables

 Figure 1. Fundamental Phases of the IT Investment Approach..... 5

 Figure 2. SEC IT Investment Spending Between FY 2014 and FY 2018 (in Millions)... 6

 Table 1. Summary of CPIC Governance Authorities 30

 Table 2. Summary of IT Investments Reviewed..... 31

Appendices

 Appendix I. Scope and Methodology 27

 Appendix II. SEC CPIC Governance Authorities 30

 Appendix III. SEC IT Investments Reviewed 31

 Appendix IV. Management Comments 32

ABBREVIATIONS

CCA	Clinger-Cohen Act of 1996
CIO	Chief Information Officer
COR	Contracting Officer’s Representative
CPIC	capital planning and investment control
DME	development, modernization, and enhancement
EOL/EOS	end of life/end of service
FAR	Federal Acquisition Regulation
FITARA	Federal Information Technology Acquisition Reform Act
FY	fiscal year
GAO	Government Accountability Office
IGCE	independent government cost estimate
IOC	Information Officers’ Council
IT	information technology
ITCPC	Information Technology Capital Planning Committee
OA	Office of Acquisitions
OFM	Office of Financial Management
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PRB	Project Review Board
Rev.	Revision
SEC or agency	U.S. Securities and Exchange Commission
SECR	SEC Administrative Regulation

Background and Objectives

Background

The Office of Management and Budget (OMB) defines an information technology (IT) investment as “an expenditure of information technology resources to address mission delivery and management support.”¹ OMB has stated that such IT resources are critical to the U.S. social, political, and economic well-being and enable the Federal Government to provide citizens with quality services, among other things. Nevertheless, the U.S. Government Accountability Office (GAO) has reported that Federal IT investments have too often failed, incurred cost overruns and schedule slippages, or contributed little to mission-related outcomes.² Since 2015, GAO has included “Improving the Management of IT Acquisitions and Operations” in its list of Government-wide high-risk areas needing attention by the executive branch and Congress.³

The U.S. Securities and Exchange Commission (SEC or agency) is increasingly harnessing and investing in technology to better identify risks, uncover frauds, sift through large volumes of data, inform policymaking, and streamline operations.⁴ In fiscal year (FY) 2018, the SEC spent about \$307 million on IT investments, including significant investments to modernize its IT infrastructure and improve its cybersecurity risk profile.⁵ This amount represented about 18 percent of all funding available to the agency that year.⁶

¹ Office of Management and Budget, Circular No. A-130, *Managing Information as a Strategic Resource*, July 28, 2016 (OMB Circular No. A-130).

² U.S. Government Accountability Office, *Information Technology – Continued Implementation of High-Risk Recommendations Is Needed to Better Manage Acquisitions, Operations, and Cybersecurity* (GAO-18-566T, May 23, 2018).

³ U.S. Government Accountability Office, *High Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas* (GAO-19-157SP, March 6, 2019).

⁴ U.S. Securities and Exchange Commission, *Fiscal Year 2017 Congressional Budget Justification, Fiscal Year 2017 Annual Performance Plan, and Fiscal Year 2015 Annual Performance Report* (February 9, 2016).

⁵ For the purpose of this report, “spent” includes amounts obligated in FY 2018 to related contracts.

⁶ The Consolidated Appropriations Act, 2018 (P.L. 115-141, 132 Stat. 578, March 2018) provided \$1.652 billion for the programs and operations of the SEC. Notably, the Act stated that the SEC’s “funding for information technology initiatives shall be increased over the fiscal year 2017 level by not less than \$45,000,000.” The SEC’s Reserve Fund (established in Section 991(e) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 [the Dodd-Frank Act, P.L. 111-203, 124 Stat. 1376, July 2010]), provided the SEC an additional \$77 million in FY 2018, which the agency allocated to IT investments.

Federal Laws, Guidance, and Regulation. Federal laws, guidance, and regulation, including the Clinger-Cohen Act of 1996 (CCA),⁷ the Federal Information Technology Acquisition Reform Act (FITARA),⁸ OMB circulars and other guidance, and the Federal Acquisition Regulation (FAR), address the Federal IT acquisition process, including IT investment management. Each of these is discussed further below.

CCA. Recognizing the significance of IT investments, the CCA requires executive agencies to establish clearly defined IT capital planning and investment control (CPIC) processes to focus more on the results achieved through IT investments while streamlining the IT acquisition process. According to the CCA, each executive agency shall design and implement a process for maximizing the value and assessing and managing the risks of the agency’s IT acquisitions. The CCA further states that such process shall:

1. provide for the selection, management, and evaluation of the results of IT investments;
2. be integrated with the processes for making budget, financial, and program management decisions within the agency;
3. include minimum criteria to be applied in considering whether to undertake a particular investment in information systems;
4. provide for identifying information systems investments that would result in shared benefits or costs for other Federal agencies or state or local governments;
5. provide for identifying for a proposed investment quantifiable measurements for determining the net benefits and risks of the investment; and
6. provide the means for agency senior management to obtain timely information about information systems investments, including milestones for measuring cost, ability to meet specified requirements, timeliness, and quality.

FITARA. Enacted in 2014, FITARA establishes specific requirements related to Federal IT acquisition, including requirements for reviews of agency IT investment portfolios, enhanced transparency, and improved risk management in IT investments. Although the SEC is not a “covered agency” for the purposes of FITARA, the SEC’s

⁷ The Information Technology Management Reform Act of 1996, together with the Federal Acquisition Reform Act of 1996, became known as the Clinger-Cohen Act of 1996 (P.L. 104-106, division D, 110 Stat. 642 and division E, 110 Stat. 679; February 10, 1996).

⁸ Federal Information Technology Reform provisions of the Carl Levin and Howard P. ‘Buck’ McKeon National Defense Authorization Act for Fiscal Year 2015 (P.L. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450; December 19, 2014).

administrative regulation (SECR) for introducing new technology into the agency refers to FITARA as an authoritative source.⁹

OMB Circulars and Other Guidance. OMB Circular No. A-130, which applies to the information resources management activities of all executive branch agencies, including the SEC, establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services. According to the Circular, agencies shall establish a comprehensive approach to improve the acquisition and management of their information resources by:

- performing information resources management activities in an efficient, effective, economical, secure, and privacy-enhancing manner;
- focusing information resources planning to support their missions;
- implementing an IT investment management process that links to and supports budget formulation and execution; and
- rethinking and restructuring the way work is performed before investing in new information systems.

OMB has also issued and annually updates Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, (OMB Circular No. A-11), which applies to all executive departments and establishments, including the SEC. Section 55 of OMB Circular No. A-11, *Information Technology Investments*, provides the policy and requirements associated with Federal IT budget, IT investment, and IT portfolio management. In addition, the accompanying annual IT Budget – Capital Planning Guidance includes technical requirements and more details related to the requirements. Collectively, the required information allows each agency and OMB to review and evaluate agency IT spending and to compare IT spending across the Federal Government.

Moreover, OMB’s Capital Programming Guide (a supplement to OMB Circular No. A-11) provides guidance on the principles and techniques for effective capital programming to ensure that capital assets successfully contribute to the achievement of agency strategic goals and objectives. According to Version 3.0 of the Guide, capital assets include IT hardware and software used by the Federal Government that have an estimated useful life of two years or more and may or may not be capitalized (that is, recorded on an entity’s balance sheet). With respect to IT, the Guide states, among other things, agency CPIC processes should lead to overall reductions or stabilization in costs during the management-in-use phase.¹⁰

⁹ SECR 24-1.2, *Introduction of New Technology Into the Agency* (Rev. 1; September 15, 2017).

¹⁰ The management-in-use phase begins after an investment’s acquisition. A key objective during the management-in-use phase is to demonstrate that existing investments meet agency needs and deliver expected value.

Finally, OMB Memorandum M-10-27, *Information Technology Baseline Management Policy* (June 28, 2010) (OMB Memorandum M-10-27), defines a common structure for Federal IT investment baseline management policies with the goal of improving transparency, performance management, and effective investment oversight. According to the memorandum, IT investments enable “efficient operation of agency missions by closing critical performance gaps. . . . If IT investments are not planned well, then cost and schedule overruns occur and expected benefits are jeopardized.”

FAR. The FAR was established to codify uniform policies for acquisition of supplies and services by executive agencies. FAR 39, *Acquisition of Information Technology*, prescribes policies and procedures for acquiring IT, consistent with OMB Circular No. A-130. IT acquisitions are also subject to other FAR requirements, including fair opportunity requirements when agencies use multiple award contracts to purchase IT products and services.

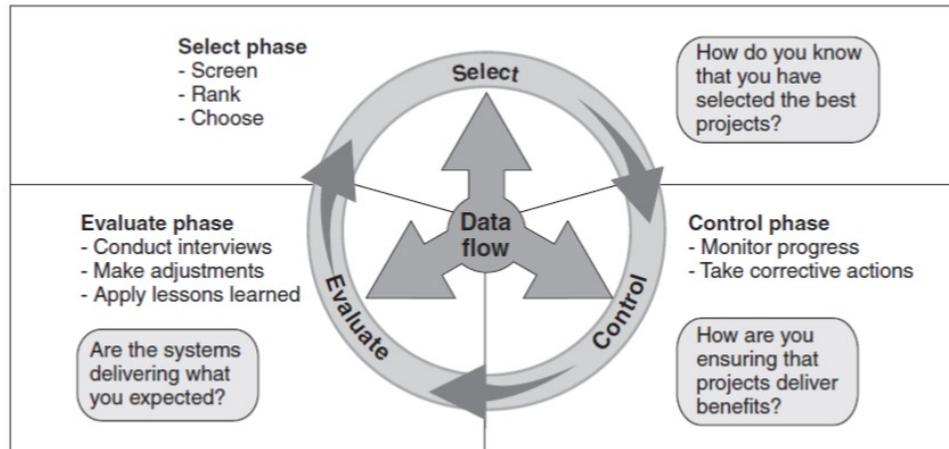
SEC Administrative Regulation, Roles, and Responsibilities. The SEC defines its CPIC policy and processes and the responsibilities for complying with key provisions of the CCA and other relevant mandates in SECR 24-02, *Information Technology Capital Planning and Investment Control* (Rev. 2.2; July 25, 2018) (SECR 24-02). According to SECR 24-02, the goal of the agency’s CPIC process is “to promote effective decision-making with respect to IT investments throughout the agency’s systems development life cycle (SDLC), without an undue burden on the delivery process.” SECR 24-02 further states that, “The CPIC process applies to all IT investments within the SEC and all stages of capital programming, including planning, budgeting, acquisition, management, and assessment.” The document also notes that, while all major investments shall follow a management process that conforms in practice to OMB Circular No. A-11, the SEC’s Chief Information Officer (CIO) may establish separate procedures for “smaller investments” that “match the rigor of the selection, control, and evaluation processes to the scale of the proposed investment.”¹¹ However, SECR 24-02 makes clear that the SEC’s IT resources strategic and capital plans and CPIC processes and procedures shall conform, to the maximum extent possible, to the general approach and processes established in OMB Circulars No. A-130 and A-11 “with modification as necessary to recognize the smaller scope of the SEC’s operations.”

As described in SECR 24-02, the SEC’s CPIC process conforms to the select-control-evaluate model championed by OMB and GAO. Figure 1 illustrates the fundamental phases of the model, which provides a systematic method for agencies to minimize risks while maximizing the returns of investments. The model’s selection phase includes activities to prepare, submit, evaluate, and approve an investment proposal or plan, including the baseline investment cost, schedule, scope, benefits, goals, and risks.

¹¹ According to OMB guidance, a major investment is a system or acquisition requiring special management attention because of its importance to the mission or function of the agency, a component of the agency, or another organization; is for financial management and obligates more than \$500,000 annually; has significant program or policy implications; has high executive visibility; has high development, operating, or maintenance costs; is funded through other than direct appropriations; or is defined as major by the agency’s CPIC process.

The control phase encompasses processes and activities to track the investment’s progress against a series of verifiable milestones to ensure the investment meets established cost, schedule, and performance goals. Lastly, the model’s evaluation phase includes processes to validate whether business objectives were met and to ensure that IT systems remain necessary and cost-effective.

Figure 1. Fundamental Phases of the IT Investment Approach



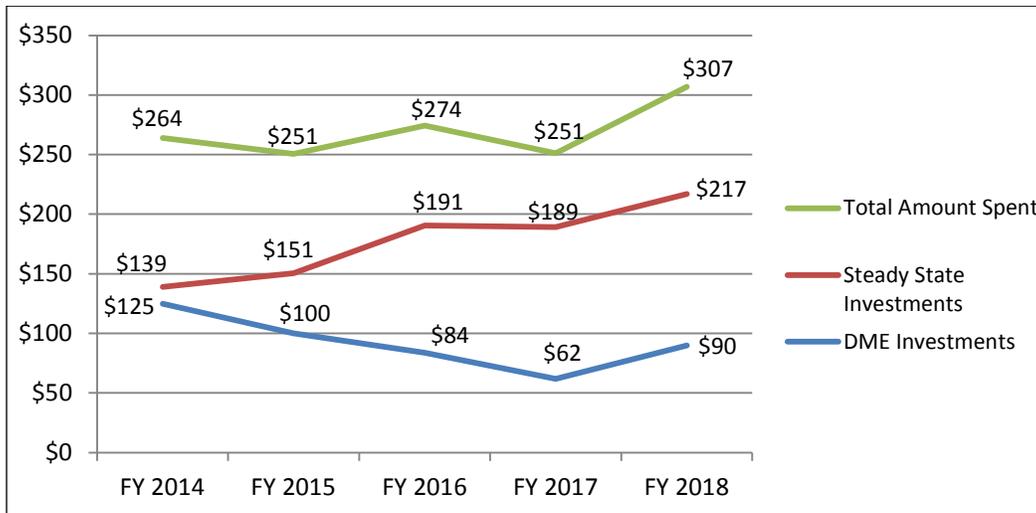
Source: U.S. Government Accountability Office, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (GAO-04-394G, March 1, 2004).

According to SECR 24-02, the SEC’s Office of Information Technology (OIT) is responsible for managing the agency’s CPIC policy and processes as they relate to IT. In addition, OIT funds the majority of the SEC’s IT investments. The agency’s Office of Acquisitions (OA) and Office of Financial Management (OFM) also share responsibility for overseeing the SEC’s IT investments. While OA develops and executes programs for procurement and contract administration, including IT acquisition, OFM administers the agency’s financial management and budget functions. Finally, with the support of the CIO, the SEC’s CPIC process is controlled by three governance authorities responsible for selecting, overseeing, and evaluating IT investments within their purview. These governance authorities (further described in Appendix II) are OIT’s Project Review Board (PRB), the Information Officers’ Council (IOC), and the Information Technology Capital Planning Committee (ITCPC).

Types of IT Investments and SEC Funding. As described in OMB Circular No. A-130, IT investments include investments to develop, modernize, and enhance a single IT asset or group of assets with related functionality (referred to as DME investments), and investments to maintain and operate such assets in a production environment (referred to as steady state or operations and maintenance investments). DME investments lead to new IT assets or systems, or change or modify existing IT assets to substantively improve capability or performance. Steady state investments sustain existing information systems at their current capability and performance levels, and include costs for software or equipment support, maintenance, and replacing IT equipment.

As shown in Figure 2, the SEC’s IT investment spending, as tracked through OIT, increased from about \$264 million in FY 2014 to about \$307 million in FY 2018. The portion of these amounts spent on DME investments steadily declined from about \$125 million in FY 2014 to about \$62 million in FY 2017, with an increase to about \$90 million in FY 2018. In contrast, the SEC’s spending on steady state investments gradually increased from about \$139 million in FY 2014 to about \$217 million in FY 2018.

Figure 2. SEC IT Investment Spending Between FY 2014 and FY 2018 (in Millions*)



Source: Office of Inspector General (OIG) analysis of IT spending reports provided by OIT. Amounts shown do not include IT investments funded by other SEC offices and divisions. *We rounded the amounts spent to the nearest million using normal rounding. As a result, annual amounts shown may not total.

Of the nearly \$307 million spent on IT investments in FY 2018, about \$244 million was from the SEC’s General Fund (and included about \$29 million for DME investments and about \$215 million for steady state investments). The remaining nearly \$63 million was from the SEC’s Reserve Fund (and included about \$61 million for DME investments and about \$2 million for steady state investments). In total, the SEC funded through OIT 515 IT investments in FY 2018.

Objectives

Our overall objective was to assess the SEC’s management of IT investments funded in FY 2018 through the Consolidated Appropriations Act, 2018 (that is, the agency’s General Fund) and the agency’s Reserve Fund as a part of OIT’s budget. Specifically, we sought to determine whether the SEC (1) increased funding for IT initiatives over the FY 2017 level, as required, and used funds allocated to IT investments for their intended purposes; (2) selected IT investments for funding in accordance with established processes; and (3) had effective controls for ensuring IT investments meet established cost, schedule, and performance goals.

To address our objectives, among other work performed, we (1) interviewed OIT, OA, and OFM officials and personnel; (2) reviewed applicable Federal laws, guidance, and regulations, and SEC policies and procedures; (3) performed a walkthrough of OIT's system for tracking IT spending; and (4) selected and assessed a nonstatistical sample of 11 of the 515 IT investments funded as part of OIT's budget in FY 2018, including each sampled item's investment and contractual documents.

Appendix I includes additional information about our scope and methodology, including our sampling methodology; our review of relevant internal controls; and prior coverage. Appendix II describes the SEC's CPIC governance authorities. Appendix III provides details about the 11 IT investments we reviewed.

Results

Finding 1. The SEC Increased Funding for IT Initiatives as Required, and Used Funds Allocated to the IT Investments We Reviewed for Their Intended Purposes

The Consolidated Appropriations Act, 2018 required the SEC to increase its funding for IT initiatives over the FY 2017 level by not less than \$45 million. We reviewed reports of the SEC's IT funding levels through the General Fund in FY 2017 and FY 2018 and determined that, in FY 2017, the agency's funding for IT initiatives was about \$199 million. In comparison, the agency's funding for FY 2018 IT initiatives was about \$244 million. As a result, we determined that the SEC complied with the IT investment funding requirement of the Consolidated Appropriations Act, 2018.

In addition, we determined that, for each of the 11 FY 2018 IT investments we reviewed, the SEC used funds allocated for their intended purposes. We also verified that, for those FY 2018 IT investments funded through the agency's Reserve Fund, the SEC notified Congress as required by the Dodd-Frank Act.¹²

We are not making recommendations for corrective action in these areas at this time.

¹² Section 991 of the Dodd-Frank Act states that, within 10 days after the date on which the SEC obligates funds from the Reserve Fund, the agency shall notify Congress of the date, amount, and purpose of the obligation.

Finding 2. The SEC's Management of Steady State Investments Needs Improvement

The CCA requires agencies to establish effective and efficient capital planning processes for selecting, managing, and evaluating IT investments. According to OMB, IT investments include DME and steady state investments. To comply with the CCA, the SEC established and implemented its CPIC process for selecting, controlling, and evaluating DME investments. However, the SEC did not apply the same process to its steady state investments, and its overall management of steady state investments needs improvement. Specifically, OIT did not (1) establish investment proposals or plans to document and manage steady state investments' baseline cost, schedule, benefits, and risks; or (2) periodically analyze steady state investments to ensure they continued to meet agency needs. This occurred because OIT officials did not view the SEC's steady state investments as IT investments for the purposes of capital planning and investment control. The SEC's spending on steady state investments has gradually increased in recent years. In FY 2018, steady state investments represented 71 percent of the agency's total IT investment expenditures (that is, \$217 million of the \$307 million spent that year). Improving agency management of steady state investments could promote more effective decision-making and provide greater assurance that such investments (1) deliver value, (2) do not unnecessarily duplicate or overlap with other investments, and (3) continue to meet the SEC's needs.

Requirements for Managing Steady State Investments. As previously discussed, OMB Circular No. A-130 includes in the definition of IT investments both DME investments and investments for the maintenance and subsequent operation of those assets in a production environment (that is, steady state investments). OMB has directed agencies to periodically examine the performance of steady state investments against, among other things, established cost, schedule, and performance goals by performing operational analyses.

For example, with regard to investment planning and control, OMB Circular No. A-130 states that agencies are responsible for establishing a decision-making process "that shall cover the life of each system" and include explicit criteria for analyzing the projected and actual costs, benefits, and risks. OMB's Capital Programming Guide also emphasizes that developmental costs are only a fraction of total lifecycle costs, and operations is a critical area where improved effectiveness and productivity can have the greatest net measurable benefit in terms of cost, performance, and mission accomplishment. The Guide concludes that 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," and to determining whether an IT investment should be retained, modified, replaced, or retired. With respect to steady state investments, the Guide states:

Regardless of performance of operational indicators, a formal operational analysis is warranted for every steady-state project. Recommendations and evaluations will be consolidated into the project's operational analysis plan. This plan will continuously be reviewed and updated as future operational analyses will be conducted yearly or on an as-needed basis.

OMB's FY 2018 IT Budget – Capital Planning Guidance 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.” The guidance further states that such analysis should trigger considerations of how an investment's objectives could be better met, how costs could be reduced, and whether the organization should continue performing a particular function.

Finally, OMB Memorandum M-10-27 states that agencies “shall establish a policy for performing operational analysis on operational/steady state investments to measure how well the investment is achieving expected cost, schedule, technical and customer performance goals.”

OIT Did Not Establish Steady State Investment Baselines or Periodically Analyze Such Investments. Unlike DME investments, which have investment proposals and plans for documenting and managing baseline information and deviations, including expected cost, schedule, benefits, and risks, OIT did not establish proposals or plans for the SEC's steady state investments. In addition, OIT did not periodically analyze the SEC's steady state investments (that is, perform operational analyses) to ensure a positive return on those investments or to determine whether the investments continued to meet agency needs.

For example, in FY 2018, the SEC continued to fund consolidated operations and maintenance support of SEC applications (an investment known as “Application Maintenance Support”) at a cost of about \$16 million without an investment proposal or plan and without performing an operational analysis of the investment. The agency entered into the investment's original contract in December 2013. At that time, the contract had an anticipated value of about \$30 million. As of December 2018, however, the SEC had spent about \$71 million on the contract.¹³ Although the SEC has spent about \$41 million more than planned, because “Application Maintenance Support” is categorized as a steady state investment, the agency does not manage the investment according to established capital planning and investment control processes.

OIT Did Not View Steady State Investments as IT Investments Subject to the CPIC Process. According to responsible OIT personnel, steady state investments did not require investment proposals or plans and were not considered IT investments for the purposes of capital planning and investment control. Guidance, forms, and other

¹³ The SEC modified the Application Maintenance and Support contract over the period of performance to add resources and funding to support additional initiatives such as SEC systems and applications support.

information maintained on the SEC's CPIC and OIT Budget and Analysis Branch internal websites corroborated this view, indicating that the SEC's DME investments are subject to the agency's CPIC process, including potential designation as major investments and scrutiny by the agency's governance authorities, but steady state investments are not. One presentation intended to answer frequently asked questions about OIT's budget (dated September 6, 2017) stated that "DME projects change to [steady state] once the project is in production and maintenance expenses begin," at which time funding changes from DME to steady state.

Notably, the SEC's CPIC policy, SECR 24-02, does not specifically address DME or steady state investments, although the document broadly defines an IT investment as, "An expenditure of resources for IT or IT-related products and services for which there are expected benefits to the organization's performance, either in terms of the efficiency of operations or effectiveness of services." SECR 24-02 includes requirements for IT investment post-implementation reviews and periodic evaluations that generally appear to meet OMB's guidance for conducting operational analyses. However, SECR 24-02 states that such reviews and evaluations are applicable to the SEC's major investments, which inherently excludes the SEC's steady state investments because of the manner in which OIT chooses to manage steady state investments.

Although the SEC did not apply the same rigor to steady state investments as to DME IT investments and its CPIC policy does not address management of steady state investments, according to OIT's Managing Executive and calendars and meeting minutes we reviewed, the SEC's ITCP and CIO reviewed the agency's overall FY 2018 steady state budget.

Improving Management of Steady State Investments Could Promote More Effective Decision-Making and Assurance Over Those Investments. OMB Circular No. A-130 states that agencies are to execute investment planning and control processes "commensurate with the size, scope, duration, and delivery risk of the investment." In October 2012, GAO reported that agencies needed to strengthen oversight of steady state investments given the size and magnitude of those investments relative to total IT spending.¹⁴ The SEC's spending on steady state investments has gradually increased in recent years and, as of FY 2018, represented 71 percent of the agency's total IT investment expenditures (that is, \$217 million of the \$307 million spent that year). Improving agency management of steady state investments could promote more effective decision-making and provide greater assurance that such investments (1) continue to meet the SEC's needs, (2) deliver value, and (3) do not unnecessarily duplicate or overlap with other investments.

¹⁴ U.S. Government Accountability Office, *Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments* (GAO-13-87, October 16, 2012).

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

To improve the SEC’s management of its steady state investments, we recommend that the Office of Information Technology:

Recommendation 1: Update its capital planning and investment control policies and procedures and implement processes for selecting, managing, and evaluating steady state investments in accordance with the Clinger-Cohen Act of 1996 and with applicable Office of Management and Budget circulars and other guidance. These processes should match the rigor of the selection, control, and evaluation processes to the scale of the proposed investment, and include:

- (a) completing an investment proposal or plan for each steady state investment documenting baseline information (such as the expected cost, schedule, benefits, and risks) to determine whether resource allocations meet business needs, and to track deviations from approved plans; and
- (b) performing and documenting a periodic operational analysis of each steady state investment to measure, among other things, that the investment is continuing to meet business and customer needs and is contributing to meeting the SEC’s strategic goals.

Management’s Response. Management concurred with the recommendation. The Office of Information Technology will revise its policies and procedures to establish more specific guidance and coverage of steady state requirements. Management’s complete response is reprinted in Appendix IV.

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

Finding 3. The SEC Can Better Manage and Document Deviations From Approved DME Investment Plans

At times, a project's cost, schedule, and performance goals—known as its baseline—are modified to reflect changes in circumstances. According to OMB Memorandum M-10-27, "When plans change, it's critically important to understand and document the reasons for the change because of the potential mission impact." Five of the six DME investments we reviewed were rebaselined in FY 2018 (that is, there were changes to the investments' cost, schedule, and/or scope). However, for four of these investments, we could not determine compliance with SECR 24-02, which states that changes to investment baselines (1) should be documented, (2) require additional CPIC governance authority review and approval, and (3) must include an evaluation of alternatives. This occurred because OIT had not established detailed formal rebaselining procedures, including expectations for documenting governance authority review and approval and alternatives analyzed. Without detailed procedures that ensure a complete and accessible audit trail of each investment's lifecycle, the SEC's rebaselining processes may lack the transparency needed to ensure effective oversight of its DME investments.

Requirements for Managing and Documenting Deviations From Approved Investment Plans. Consistent with applicable OMB guidance, SECR 24-02 states that, once approved, IT investments must be managed within the constraints of their defined cost, schedule, and scope. The policy also states that any changes to an investment's cost, schedule, or scope "shall require additional CPIC governance authority review and approval prior to implementation." SECR 24-02 further states that, for major investments, the control phase of the SEC's CPIC process shall, among other things:

Establish and track corrective actions to address any deviations from approved investment plans. Ensure that proposed changes to investment baselines fully and properly evaluate alternatives and give consideration to recovery plans, impacts to the [enterprise architecture], and the investment delivery process.¹⁵

Finally, SECR 24-02 makes clear that investment teams are responsible for maintaining current information, together with required CPIC documentation, in the agency's enterprise system until the investment has been approved for closure.

¹⁵ According to SECR 24-02, the terms "major information system," "major investment," "major project," or "major system" are used interchangeably and mean a system or investment that requires special management attention because, among other things, it is important to the agency's mission or has significant program or policy implications. Based on this guidance and the descriptions of the DME investments we reviewed, we viewed all six DME investments in our sample as "major" when evaluating compliance with the SEC's CPIC process.

OIT's Business Management Office maintains a comprehensive internal site that provides links and information related to each CPIC phase (select, control, and evaluate) and serves as informal guidance. The "control" phase of the site refers to project change requests, which are required when there are changes to a project's approved funding, scope, baseline completion date, official name, and overall status. According to the site's general instructions for submitting a change request, the PRB Chair can approve requests for additional funding of \$50,000 or less. However, requests for additional funding of more than \$50,000 or requests for other changes to a project must be presented to OIT's PRB. As further discussed in Appendix II, the PRB serves as an advisory body with the authority to recommend budget action on the selection of IT investments throughout the investment lifecycle to ensure the agency's business needs are effectively and efficiently met.

We Could Not Always Determine Compliance With SECR 24-02. Five of the six DME investments we reviewed were rebaselined in FY 2018 (that is, there were changes to the investments' cost, schedule, and/or scope). However, for four of these investments, we could not determine compliance with the SECR 24-02 requirements related to deviations from approved investment plans. Specifically, agency officials did not maintain or provide documentation, such as meeting minutes or project change requests, demonstrating the PRB's review and approval of changes to the investments' baselines or the alternatives analyzed.¹⁶

For example, the cost of the investment related to the SEC's National Exam Program enhancement contract increased from about \$4.7 million to about \$5.7 million, while the investment for (b)(7)(E) increased from about \$1.3 million to about \$6.8 million. However, OIT did not provide detailed documentation demonstrating that the PRB reviewed and recommended the additional funding for either investment as required.

In addition, the cost, schedule, and scope of the investment for migrating and expanding the (b)(7)(E) system to a new architecture changed in FY 2018. According to the investment proposal, the project had a start date of April 15, 2018, and an expected end date of May 31, 2019. As of May 2019, the investment was not complete, and OIT had not submitted a project closure report. Although the investment was not intended to span multiple years, in FY 2019, the project manager submitted a new investment request for an additional \$1 million to expand the (b)(7)(E) system and establish a new completion date of May 2020. The new investment request also included a change in scope to address the possibility of future expansions. Despite these changes, OIT did not submit a change request to document the revised cost, schedule, and scope and the reasons for the changes.

Finally, to address persistent physical and environmental control deficiencies and other concerns at the SEC's D1 data center, the agency approved an investment for D1 data center improvements and risk mitigation. Subsequently, it was determined that the best

¹⁶ We were able to obtain adequate documentation for the fifth DME investment we reviewed that was rebaselined in FY 2018.

course of action to mitigate the risks would be to relocate the data center to a new facility (referred to as D3). Through an August 2017 request for information, the SEC sought to identify vendors capable of meeting the agency’s data center needs. In addition, the SEC pursued inter-agency agreements with other Federal agencies to share data center services. Ultimately, however, the SEC modified the contract for its D2 data center to provide for D3 data center services in a new location. Through reviews of emails, change request forms, meeting minutes, and other documents, we were able to track and understand the changes in the investment’s cost, schedule, and scope. However, OIT did not provide documentation to demonstrate how the investment team met the SECR 24-02 requirement that they “fully and properly” evaluated alternatives before relocating the data center.

Establishing Detailed Formal Rebaselining Procedures Could Improve Oversight of the SEC’s DME Investments. As previously stated, SECR 24-02 includes high-level requirements for documenting and managing deviations from approved investment plans. In addition, OIT maintains an internal site that provides informal guidance, including guidance related to change request forms and processes. However, OIT had not established detailed formal rebaselining procedures, including expectations for documenting governance authority review and approval and alternatives analyzed.

In July 2008, GAO reported that Federal agencies needed to establish comprehensive policies to address changes to projects’ baselines and to establish new baselines.¹⁷ Subsequently, OMB issued OMB Memorandum M-10-27, which defines a common structure for IT investment baseline management policies with the goal of improving transparency, performance management, and effective investment oversight. The memorandum states that agencies should create or update existing IT investment baseline management policies and ensure those policies address the following items for revising investment baselines:

- a description of changes to performance goals and measures;
- a summary of the changes in the investment’s scope and/or capabilities;
- identification of contributing problems, why the current plan is not feasible, and remediation plans to prevent problem recurrence, if applicable;
- the chronology of changes to an investment’s work breakdown structure and cost estimate detailing variance from the most recently approved baseline; and
- a description of any contract implications or necessary actions assuring that the baseline accurately reflects contracting constraints and risks.

For major investments, OMB Memorandum M-10-27 also states that agency rebaselining policies shall address the need for an updated “Analysis of Alternatives of

¹⁷ U.S. Government Accountability Office, *Agencies Need to Establish Comprehensive Policies to Address Changes to Projects’ Cost, Schedule, and Performance Goals* (GAO-08-925, July 31, 2008).

the chosen alternative’s cost data at a minimum (or new analysis if any of the original alternatives are no longer valid) and related recommendation.”

GAO acknowledges that, when managed effectively, rebaselining can improve performance management of IT projects. Moreover, OMB emphasizes that baseline management demonstrates that a project is under financial and managerial control. Formal rebaselining procedures, including expectations for documenting governance authority review and approval and alternatives analyzed, could help ensure a complete and accessible audit trail of each investment’s lifecycle. Without such procedures, the SEC’s rebaselining processes may lack the transparency needed to ensure effective oversight of its DME investments.

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

To better manage and document deviations from approved investment plans, we recommend that the Office of Information Technology:

Recommendation 2: Ensure its capital planning and investment control policies meet the intent of Office of Management and Budget guidance on information technology investment baseline management policies, to include procedures that:

- (a) clarify the specific information needed to support change requests for deviations from approved investment baselines;
- (b) specify the minimum documentation necessary to demonstrate the analysis of alternatives performed to support decisions to improve, enhance, or modernize existing information technology investments, or to implement changes to investment baselines; and
- (c) establish the circumstances under which a new investment proposal is warranted in lieu of a change request.

Management’s Response. Management concurred with the recommendation. The Office of Information Technology will revise its policies and procedures as recommended. Management’s complete response is reprinted in Appendix IV.

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: Provide training to personnel with investment oversight and program management responsibilities that, at a minimum, addresses the SEC’s information technology investment baseline management policies and procedures.

Management’s Response. Management concurred with the recommendation. The Office of Information Technology will implement training for personnel with investment oversight and program management responsibilities that addresses the

SEC's information technology investment baseline management policies and procedures. Management's complete response is reprinted in Appendix IV.

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

Finding 4. The SEC Can Better Plan and Manage Investments in Hardware Assets To Achieve Expected Outcomes or Goals

The CCA, OMB, and SECR 24-02 each emphasize achievement of performance goals and the importance of planning and managing IT investments, including using documents that demonstrate investment outcomes. In addition, OMB has stated agencies must effectively plan for the replacement of hardware assets. However, we reviewed five IT investments that involved purchasing hardware assets and found that OIT needs to improve the documentation of hardware assets investment planning and to demonstrate investment outcomes. This occurred because OIT had not established processes to effectively plan for the replacement of hardware assets, and processes to track related investments' outcomes or achievement of goals. Without such processes, the SEC risks hardware assets in use reaching their end-of life/end-of-service (EOL/EOS), thereby increasing the risk of equipment failure and the potential for data loss.

Requirements for Effectively Planning IT Investments and Adequately Tracking Investment Outcomes. According to OMB Circular No. A-11, agencies should maintain documents used to manage the planning of IT investments and documents that demonstrate investment outcomes and achievement of goals. OMB states that agencies should explain what outcomes or desired results the agency expects to achieve with the requested funding. Specifically, during the planning phase, agencies should establish the investment cost, schedule, and performance goals that can be measured (or evaluated) throughout the acquisition process. Such evaluations are to assess how well a specific strategy or an aspect of a program is working to achieve intended results or outcomes, and may address questions related to the overall performance of the program, or questions related to measurement of progress.

In addition, OMB Memorandum M-16-02 addresses the need to effectively plan for the replacement of hardware assets.¹⁸ The memorandum discusses management practices such as adopting uniform refresh cycles, and states that “agencies shall develop and implement policies and procedures in which only a portion of the laptops and desktops are at the end of their useful life and need to be replaced each year.”

Furthermore, according to the *GAO IT Investment Management Framework*, providing investment oversight is a pivotal process whereby the organization monitors investments against anticipated benefits. GAO also states that investment oversight should evaluate the benefits delivered to-date and the relationship of the investment to specific business objectives. Within the SEC, SECR 24-02 states that the agency's

¹⁸ Office of Management and Budget, Memorandum M-16-02, *Category Management Policy 15-1: Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops*, October 16, 2015.

CPIC process is to “assess achievement of performance measures and compare investment performance against stated requirements.”

OIT Needs To Improve the Documentation of Hardware Assets Investment Planning and To Demonstrate Investment Outcomes or Achievement of Goals. Of the 11 FY 2018 IT investments we reviewed, 5 involved the purchase of hardware assets, including laptops, desktops, servers, and other network and storage devices. Generally, these investments aimed to replace hardware in use that:

1. had reached its EOL/EOS,
2. was not capable of providing (b)(7)(E), and/or
3. had started to show signs of age to the point of failing.

OIT did not adequately document its planning of these five investments, including the processes used to (1) track hardware warranties and/or the expected useful life of hardware assets in use, and (2) determine the cost, type, and quantities of hardware assets OIT needed to purchase. According to an OIT official, most of the SEC’s (b)(7)(E) in use in FY 2018 were more than 7 years old, were no longer serviceable, and were not capable of providing (b)(7)(E). OIT personnel also stated that funding to replace EOL/EOS hardware was an annual set-aside based on a goal or strategy to replace about 30 percent of the agency’s hardware assets annually, although this goal/strategy was not formally established. In addition, OIT personnel stated that the five investments in question were for hardware acquisition, therefore, OIT focused on purchasing and receiving the hardware assets. Although OIT tracked the receipt of the hardware assets purchased, OIT did not maintain adequate planning or implementation documentation to demonstrate that the investments’ achieved expected outcomes or goals.

For example, for one investment, the SEC spent about \$6.8 million to replace aging and EOL hardware and software with assets capable of supporting (b)(7)(E). The established investment outcome or goal was to protect (b)(7)(E). Although OIT tracked the receipt of the assets it purchased, OIT could not demonstrate that the SEC deployed the assets (b)(7)(E).

For another investment, the SEC spent about \$1.4 million to upgrade laptops and desktops to be compatible with (b)(7)(E). OIT personnel stated that the investment outcome or goal was for all SEC computers to be compatible with (b)(7)(E) by the end of November 2019. At the end of FY 2018, however, OIT could not demonstrate the number of SEC computers compatible with (b)(7)(E) and, therefore, the investment’s progress toward meeting its stated goal.

¹⁹ According to a July 2019 report, OIT had replaced or refreshed “about 53 to 58 percent” of the SEC’s computers.

OIT Had Not Established Processes To Effectively Plan for the Replacement of Hardware Assets and To Track Investments' Outcomes. The conditions we observed occurred because OIT had not established processes to effectively plan for the replacement of hardware assets, or to track related investments' outcomes beyond the receipt of the hardware purchased. Without such processes, the SEC risks hardware assets in use reaching their EOL/EOS, thereby increasing the risk of equipment failure and the potential for data loss.

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

To further improve its planning and management of investments in hardware assets, we recommend that the Office of Information Technology:

Recommendation 4: Update its capital planning and investment control policies and procedures and implement processes to:

- (a) establish a uniform refresh plan or a strategic approach for the replacement of hardware assets, and document performance against planned cost, quantities, and type of hardware assets to be replaced annually; and
- (b) monitor investments in hardware asset purchases beyond receipt of the assets to ensure the assets are efficiently and effectively deployed and the investments achieve expected outcomes or goals and provide requested capabilities.

Management's Response. Management concurred with the recommendation. The Office of Information Technology will revise its policies and procedures as recommended. Management's complete response is reprinted in Appendix IV.

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

Finding 5. The SEC Can Improve Its Support for Independent Government Cost Estimates

Mandated by FAR 16.505(b), the concept of fair opportunity is intended to level the playing field so that Federal agencies cannot give an unfair advantage to one contractor over another. Federal agencies purchasing IT products and services must follow the FAR's fair opportunity requirements when using multiple award contracts, including Government-wide acquisition contracts. During FY 2018, OA extended contracts for two IT investments we reviewed, and documented justifications to support the use of the logical follow-on exception to fair opportunity for both extensions. However, responsible personnel did not maintain adequate documentation to support the independent Government cost estimates (IGCE) used for the estimated extension prices. While the FAR does not specify the documentation required to support IGCEs or determinations about the fairness and reasonableness of extension prices, GAO has issued guidance addressing the need for adequate documentation as part of an effective internal control system. In addition, OA established guidance emphasizing "practical lessons learned" and urging responsible personnel to document any and all methods used to complete IGCEs. However, OA's guidance was "for informational purposes," and contracting officials did not use it. Moreover, the OA operating procedure that established required actions did not address the need for documentation. Without adequate documentation, the SEC has less assurance that anticipated prices for contract extensions—including the extensions we reviewed—are fair and reasonable, and that the extensions will provide the best return on investment.

Fair Opportunity Requirements and Related Considerations. FAR 16.505(b)(2) requires contracting officers to provide awardees a fair opportunity to be considered for each order exceeding \$3,500 issued under multiple delivery-order contracts or multiple task-order contracts, unless an exception applies. One such exception (known as the logical follow-on exception) applies in the case of an order that must be issued on a sole-source basis in the interest of economy and efficiency because it is a logical follow-on to an order already issued under the contract, provided that all awardees were given a fair opportunity to be considered for the original order. The FAR requires a written justification for using the logical follow-on exception, including a determination that the anticipated cost to the Government of the extension will be fair and reasonable. FAR 15.402 also states that contracting officers shall obtain the type and quantity of data necessary to establish a fair and reasonable price.

IGCEs are the Government's best estimate of a contractor's potential costs and are an important tool for both program and contracting officials to provide information when planning for and awarding contracts. IGCEs support efforts to ensure that the cost of meeting the Government's requirements for the goods or services being acquired are known. Contracting officials also use IGCEs to (1) compare offerors' proposed prices,

(2) determine whether proposed contract prices are reasonable, and (3) support contract price negotiations.

The FAR does not specify the documentation required to support IGCEs or the contracting officer’s determination that, when using the logical follow-on exception to fair opportunity requirements, extension prices will be fair and reasonable. However, GAO has issued guidance addressing the need for documentation. Specifically, according to GAO’s *Standards for Internal Control in the Federal Government*, documentation is a necessary part of an effective internal control system, and is required for the effective design, implementation, and operating effectiveness of an entity’s internal control system.²⁰ In addition, GAO’s *Cost Estimating and Assessment Guide* states that a well-documented cost estimate includes source data and significance, clearly detailed calculations and results, and explanations of why particular methods and references were chosen.²¹ GAO has also reported that, “The usefulness of an IGCE to a contracting officer depends in part on its supporting documentation . . .”²²

The SEC Did Not Maintain Adequate Documentation To Support the IGCEs. OA used the follow-on exception to fair opportunity requirements to extend existing contracts for two IT investments we reviewed, but responsible personnel did not maintain adequate documentation to support the IGCEs used for the estimated extension prices. Contracting officials based the IGCE for one of the two extensions on the contractor’s cost/price estimate, and did not fully document the data sources and methodology used to develop either extensions’ IGCE. Descriptions of both extensions follow.

Application Maintenance Support. Using the follow-on exception to fair opportunity, OA extended on a sole-source basis an existing contract for application and maintenance support for various SEC applications. According to the written justification, the extension was for 12-months with two 3-month options and the anticipated value of the extension was about \$89 million. The contracting officer’s representative (COR) who developed the IGCE for the extension price explained that she relied, in part, on the contractor’s price and technical proposal for a portion of the IGCE that totaled about \$26 million. The COR also used the contractor’s current labor rates to develop the extension price for the additional \$63 million in funding, which included a \$10 million buffer for potential projects. However, the COR did not document the detailed calculations, methodology, or data sources used to arrive at the IGCE. In addition, the COR did not provide evidence that the program office scrutinized the contractor’s proposal to validate the contractor’s price.

²⁰ U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 10, 2014).

²¹ U.S. Government Accountability Office, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs* (GAO-09-3SP, March 2, 2009).

²² U.S. Government Accountability Office, *Service Contracts: Agencies Should Take Steps to More Effectively Use Independent Government Cost Estimates* (GAO-17-398, May 17, 2017).

National Exam Program Enhancement Contract. OA also used the follow-on exception to fair opportunity to extend on a sole-source basis an existing contract for the enhancement, operation, and maintenance of the SEC's National Exam Program systems, and for the pilot migration of these systems to another platform. According to the written justification, the extension was for 20 months (including all options) and the anticipated value of the extension was about \$12.6 million. The COR provided the IGCE used for the extension price and the contracting officer provided worksheets showing the labor rate and labor hours needed to arrive at part of the extension activities totaling about \$5.6 million. The IGCE labor rate reflected the contractor's current labor rates; however, contracting officials did not provide documentation showing how they arrived at (1) the number of hours needed, or (2) the extension price for the remaining extension activities totaling about \$6.9 million.

Although responsible personnel documented written justifications for these two contract extensions, including a determination that the anticipated cost of the extensions would be fair and reasonable, they did not maintain adequate documentation to support these determinations. In both cases, the contracting officers stated that their determinations about the fairness and reasonableness of the extension prices were based on labor rates determined to be fair and reasonable at the time the base or original contracts were awarded (in 2013 and 2014, respectively). The contracting officers also stated that they relied on a technical review performed by the program office—OIT—to determine that the estimated labor mix and number of hours for the extension periods were appropriate for the level of effort, and confirmed with OIT that the anticipated extension prices would be fair and reasonable. However, program office personnel did not provide documentation supporting their review.

OA Did Not Establish IGCE Documentation Requirements, Which Could Improve Agency Assurance Over Price Reasonableness Determinations. The conditions we observed occurred because OA did not establish documentation requirements for IGCEs. For example, in May 2013, OA issued an *Independent Government Cost Estimate Guide* (IGCE Guide) based on “practical lessons learned” that, if followed, would help meet GAO guidance related to IGCEs. The IGCE Guide states, “Caution: Do not to base the IGCE on a contractor’s cost/price estimate. Pricing history from previous awards can be used but a vendor quote should not be used.” The IGCE Guide also states:

Using cost/price data from a single contractor, without scrutiny, invalidates the ‘independence’ that makes your IGCE useful in contract negotiations . . . Even unique requirements and sole source acquisitions require research into previous contracts, similar requirements, and the use of technical judgment to ensure that the data in the IGCE is unbiased.

Finally, the IGCE Guide contains an IGCE template and advises responsible personnel to provide a brief narrative with the completed IGCE explaining how contracting officials developed costs and what reference material they used. In multiple places, the IGCE Guide urges SEC personnel to “Document any and all methods used to reach the IGCE” and to “REMEMBER TO DOCUMENT ALL ASSUMPTIONS!” However, the IGCE

Guide is “for informational purposes,” and its usage is not required. As such, the contracting officials responsible for the contract extensions we reviewed did not use it.

In addition, in May 2019, OA issued an operating procedure that prescribes the organization’s policies, responsibilities, and procedures, including procedures for other than full and open competition.²³ Unlike the IGCE Guide, compliance with the operating procedure is not optional. However, the operating procedure does not address the process or documentation needed to thoroughly support IGCEs.

Without adequate documentation, the SEC has less assurance that anticipated prices—including those for the extensions we reviewed—are fair and reasonable, and that the extensions will provide the best return on investment.

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

To further improve the SEC’s contract management, we recommend that the Office of Acquisitions:

Recommendation 5: Establish documentation requirements for thoroughly supporting independent Government cost estimates.

Management’s Response. Management concurred with the recommendation. The Office of Acquisitions will revise the *Independent Government Cost Estimate Guide* to include minimum required supporting documentation for independent government cost estimates. Management’s complete response is reprinted in Appendix IV.

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.

²³ OA Operating Procedure 1, *Acquisition*, (May 21, 2019). This operating procedure replaced SECR 10-23, *Other than Full and Open Competition* (Rev. 1; November 2015).

Other Matters of Interest

During our audit, the following other matters of interest that did not warrant recommendations came to our attention. We discussed these matters with agency management for their consideration.

The SEC Selected (b)(7)(E) as the Agency's Enterprise IT Project and Portfolio Management System Although the System Did Not Meet Agency Requirements.

In May 2015, the SEC's former CIO selected (b)(7)(E) as the agency's enterprise IT project and portfolio management system, although the system did not meet or exceed most of the SEC's project and portfolio management requirements. According to the investment proposal, the SEC sought to replace its previous IT project and portfolio management system because the system did not support the agency's future strategic and critical requirements, and a new system was needed to address OIG and GAO recommendations. The agency considered four alternatives, including (b)(7)(E) and a system called (b)(7)(E). OIT prepared a vendor selection business case which showed that (b)(7)(E) met more project and portfolio management requirements, and (b)(7)(E) "cannot support project management" and "may provide limited functionality." Nevertheless, the SEC selected (b)(7)(E) without providing a justification or rationale in the investment or contract files.

About 2 years after implementing (b)(7)(E), the SEC decided to replace the system with (b)(7)(E). Had the SEC selected a system that met or exceeded most of the agency's project and portfolio management requirements in 2015, the agency may not have needed to replace the system 2 years later, and could have saved about \$390,000 (that is, the cost of migrating data to (b)(7)(E)).²⁴

To improve IT investment decision-making in the future, we encourage OIT to assess and, as needed, revise its processes for (1) conducting alternatives analyses leading to investment selection, and (2) documenting management decisions.

The Use of a Single Vendor for the SEC's Data Center Services Increases Certain Risks.

As discussed in Finding 3, in FY 2018, the SEC modified the contract for its D2 data center to provide for data center services in a new location, referred to as D3. This action successfully addressed persistent physical and environmental control deficiencies and other concerns at D1, the SEC's former data center location.²⁵ However, by using a single vendor for its data center services, the SEC is in a vendor lock-in position. According to OMB Memorandum M-16-21, *Federal Source Code Policy* (August 2016), "vendor lock-in" refers to a situation in which the customer depends on a single supplier for a product and cannot easily move to another vendor

²⁴ The (b)(7)(E) project was ongoing at the time of our audit and we could not determine whether the agency will incur additional costs to migrate data from (b)(7)(E) to (b)(7)(E).

²⁵ U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Management of Its Data Centers* (Report No. 543; September 29, 2017).

without sustaining substantial cost or inconvenience. National Institute of Standards and Technology Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (April 2015), also states that use of a diverse set of suppliers reduces the possibility of single point of failure or threat.

We also noted that, under the new contract modification, the D2 and D3 data centers' periods of performance expire at the same time.

We encourage agency management to (1) consider actions necessary to mitigate the risks associated with its data center vendor lock-in and contract periods of performance, and (2) timely implement those actions deemed necessary and appropriate.

Appendix I. Scope and Methodology

We conducted this performance audit from November 2018 through September 2019 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 and Objective. The audit covered the SEC's IT investments funded in FY 2018 (between October 1, 2017, and September 30, 2018) through the Consolidated Appropriations Act, 2018 (that is, the agency's General Fund) and the agency's Reserve Fund as a part of OIT's budget.²⁶ Our overall objective was to assess the SEC's management of those IT investments and determine whether the agency (1) increased funding for IT initiatives over the FY 2017 level, as required, and used funds allocated to IT investments for their intended purposes; (2) selected IT investments for funding in accordance with established processes; and (3) had effective controls for ensuring IT investments meet established cost, schedule, and performance goals.

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

Methodology. To address our objectives, among other work performed, we:

- interviewed OIT, OFM, and OA personnel;
- reviewed applicable Federal laws, guidance, and regulation, and relevant SEC policies and procedures;
- clarified with OMB the definition of "IT investments," as described in OMB Circular No. A-130; and
- performed a walkthrough of OIT's system for tracking IT spending.

We also obtained information about the agency's IT investments funded through OIT's budget in FY 2018, and we selected a nonstatistical sample of 11 of the 515 IT investments funded that year (or about 2 percent). We ensured that the sample included DME and steady state investments and represented at least 10 percent of the agency's overall FY 2018 OIT-approved budget.²⁷ For each sampled investment, we reviewed corresponding investment and contractual documents and focused our review on those controls intended to ensure that the agency (1) used funding for its intended

²⁶ OIT funds the majority of the SEC's IT investments. We did not review IT investments funded by other SEC offices and divisions.

²⁷ As of the end of FY 2018, the SEC had spent \$306,922,925 on IT investments funded through OIT, of which \$41,826,334 was spent on the IT investments we reviewed, as shown in Appendix III. These amounts include amounts obligated in FY 2018 to related contracts.

purposes, (2) selected IT investments for funding in accordance with established processes, and (3) monitored IT investments to ensure they met their established cost, schedule, and performance goals, including through rebaselining. Appendix III provides details about the 11 IT investments we reviewed.

Internal Controls. To assess internal controls related to our objectives, we reviewed the FY 2018 risk control matrices and management assurance statements for OIT, OA, and OFM. In addition, we gained an understanding of the SEC's controls for managing IT investments funded through the Consolidated Appropriations Act, 2018, and the Reserve Fund, and identified and tested key internal controls related to our objectives. Specifically, we assessed the SEC's processes for (1) selecting IT investments for funding; (2) controlling IT investments, including through rebaselining, to ensure the agency used funds allocated to these investments for their intended purposes and investments met established cost, schedule, and performance goals; and (3) evaluating IT investments to ensure they met established goals and agency needs. To do so, as previously described, we performed walkthroughs of established processes, compared SEC policy and processes to relevant Federal mandates, and reviewed a nonstatistical sample of 11 judgmentally selected IT investments funded in FY 2018.

We determined that the SEC's controls for selecting, controlling, and evaluating DME investments were generally effective. However, as noted in this report, we identified internal control weaknesses that affected how the SEC (1) manages steady state investments; (2) manages and documents changes to approved DME investment plans; (3) plans and manages investments in hardware assets; and (4) documents IGCEs. 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 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 FY 2018 IT investment reports from OIT's system for tracking IT spending, contractual documents from the SEC's procurement system, and IT investment records from the SEC's enterprise IT project and portfolio management system. We did not perform extensive testing of the systems as such testing was not part of our objectives. However, to assess the reliability of the

computer-processed data we relied on, we interviewed OIT, OA, and OFM personnel to gain an understanding of the data sources; corroborated information from OIT's system for tracking IT spending with information in the SEC's financial reporting system; and reviewed individual investment and contractual records. Based on our assessments, we determined that the computer-processed data we reviewed was sufficiently reliable in the context of our objectives.

Prior Coverage. Between 2008 and 2019, the SEC OIG and GAO issued the following reports of particular relevance to this audit.

SEC OIG:

- *Audit of the SEC's Management of its Data Centers* (Report No. 543, September 29, 2017).
- *Audit of the SEC's Information Technology Requirements-Gathering Process* (Report No. 538, September 30, 2016).
- *Audit of the SEC Budget Execution Cycle* (Report No. 488, March 29, 2011).
- *Assessment of the SEC Information Technology Investment Process* (Report No. 466, March 26, 2010).

GAO:

- *High Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas* (GAO-19-157SP, March 6, 2019).
- *Information Technology – Continued Implementation of High-Risk Recommendations Is Needed to Better Manage Acquisitions, Operations, and Cybersecurity* (GAO-18-566T, May 23, 2018).
- *Information Technology: Opportunities for Improving Acquisitions and Operations* (GAO-17-251SP, April 11, 2017).
- *Federal Agencies Need to Address Aging Legacy Systems* (GAO-16-696T, May 25, 2016).
- *Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments* (GAO-13-87, October 16, 2012).
- *U.S. Government Accountability Office, Agencies Need to Establish Comprehensive Policies to Address Changes to Projects' Cost, Schedule, and Performance Goals* (GAO-08-925, July 31, 2008)

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

Appendix II. SEC CPIC Governance Authorities

The following table describes the roles and responsibilities of the SEC’s three CPIC governance authorities.

Table 1. Summary of CPIC Governance Authorities

Governance Authority	Roles and Responsibilities
PRB	<p>OIT's PRB is the first level of governance in the SEC's CPIC process. It serves as an advisory body with the authority to recommend budget action on the selection of IT investments throughout the investment lifecycle to ensure the agency's business needs are effectively and efficiently met. The PRB's primary role is to inform and advise senior management on IT investment proposals generated by OIT and other business sponsors and then make recommendations to senior management regarding the viability of such proposals for budget action. The PRB is also involved in the control and evaluate phases of the IT investment lifecycle, and it assists the ITCPC and the IOC in the prioritization of investment-related activities based on their relative importance to the SEC's overall mission. While the PRB generally serves as an advisory body, the Chair has the authority to approve IT investments up to \$50,000 without Board review. According to the PRB's March 2019 charter, the PRB meets weekly and is composed of 19 voting members and 2 advisory members from OIT, OA, and OFM.</p>
ITCPC	<p>The ITCPC is a decision-making body with the authority to approve, continue, modify, or terminate all IT programs and recommend the overall allocation of budget resources for IT. The ITCPC provides high-level strategic direction and governance to IT management and is the agency's highest IT investment decision-making body. OIT's operating budget and the allocation of budget resources across IT programs, projects, or IT investments are subject to ITCPC approval. As part of the CPIC process, the ITCPC provides agency-wide, executive-level direction on the selection, control, and evaluation of IT investments. The ITCPC is composed of 12 members who are senior executives from various enterprise IT and business units.</p>
IOC	<p>The IOC is a decision-making body with the authority to approve all IT investments that fall within the budgetary guidelines set by the ITCPC for the FY. The IOC scales its IT investment oversight commensurate with an investment's dollar value. Generally, only those investments costing more than \$2 million within any given FY are brought before the IOC for consideration. As part of the CPIC process, the IOC: (i) reviews investment proposals and ensures resource allocations meet business needs; (ii) periodically reviews the performance of selected IT investments; and (iii) periodically reviews the results of completed IT investments to ensure they provide expected business results, deliver the expected value, and ensure that IT systems remain necessary and cost-effective. The IOC is composed of 18 members who are senior officers from various SEC divisions and offices including OIT, OA, and OFM.</p>

Source: OIG-generated based on governance authorities' charters.

Appendix III. SEC IT Investments Reviewed

The following table provides details about the five steady state and six DME investments we reviewed, including each investment's name and purpose and the amount the SEC spent on each investment in FY 2018 (including amounts obligated to related contracts).

Table 2. Summary of IT Investments Reviewed

Investment Name	Investment Purpose	Amount Spent in FY 2018
1. Security Compliance and Monitoring Support - Supplemental	To secure (b)(7)(E) practices and expand the agency's ability to (b)(7)(E).	\$1,500,000
2. Application Maintenance Support	To provide funding for consolidated operations and maintenance support of SEC applications.	\$15,660,340
3. Replacement of EOL/EOS and Growth of Computing Hardware	To replace EOL/EOS infrastructure and add capacity to support existing steady state services.	\$4,147,419
4. Governance Support	To provide additional staff to assist in handling IT investments subject to OIT's service delivery framework processes.	\$1,026,442
5. (b)(7)(E) Admin and Support	To provide for (b)(7)(E) on-premise perpetual licenses for SEC staff's unlimited usage, and for other technical support.	\$1,162,520
Subtotal: FY 2018 Spending for Steady State Investments Reviewed		\$23,496,721
6. Data Center 1 Relocation	To relocate the D1 data center to a new facility.	\$3,434,161
7. CF Workload Tracking System	To modernize nine existing (b)(7)(E) applications and develop a major system to support the business requirements of the Division of Corporation Finance.	\$0 ²⁸
8. (b)(7)(E)	To acquire computing and storage resources to migrate and expand the (b)(7)(E) system to a new architecture.	\$986,440
9. Laptop/Desktop Refresh	To acquire new workstations to replace old equipment incompatible with (b)(7)(E), and to upgrade the remaining equipment (b)(7)(E).	\$1,400,000
10. Encryption (b)(7)(E)	To protect (b)(7)(E) by replacing (b)(7)(E).	\$6,837,178
11. National Exam Program Enhancement Contract	To continue developing and enhancing systems supporting the SEC's National Exam Program.	\$5,671,834
Subtotal: FY 2018 Spending for DME Investments Reviewed		\$18,329,613
Total FY 2018 Spending for All Investments Reviewed		\$41,826,334

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

²⁸ Although CPIC governance authorities approved about \$2.8 million in funding for this investment, the SEC did not obligate any of those funds in FY 2018.

Appendix IV. Management Comments

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

FROM: Kenneth A. Johnson, Chief Operating Officer

KENNETH JOHNSON Digitally signed by
KENNETH JOHNSON
Date: 2019.09.05
18:15:31 -04'00'

DATE: September 5, 2019

SUBJECT: Response to Draft Report entitled “The SEC Has Processes to Manage Information Technology Investments but Improvements Are Needed”

Thank you for the opportunity to review and comment on the draft report entitled “The SEC Has Processes to Manage Information Technology Investments but Improvements Are Needed. We take very seriously our obligation to effectively manage the SEC’s IT investments, and our obligation to be good stewards of agency resources.

As we note below, we concur with all the recommendations in the draft report and intend to continue to work swiftly and diligently to address them.

A response to each of the recommendations is provided below.

Recommendation 1: Update its capital planning and investment control policies and procedures and implement processes for selecting, managing, and evaluating steady state investments in accordance with the Clinger-Cohen Act of 1996 and with applicable Office of Management and Budget circulars and other guidance. These processes should match the rigor of the selection, control, and evaluation processes to the scale of the proposed investment, and include:

- (a) completing an investment proposal or plan for each steady state investment documenting baseline information (such as the expected cost, schedule, benefits, and risks) to determine whether resource allocations meet business needs, and to track deviations from approved plans; and
- (b) performing and documenting a periodic operational analysis of each steady state investment to measure, among other things, that the investment is continuing to meet business and customer needs and is contributing to meeting the SEC’s strategic goals.

Management Response: Management concurs with this recommendation. OIT will revise its policies and procedures to establish more specific guidance and coverage of IT Steady State requirements, as recommended.

Recommendation 2: Ensure its capital planning and investment control policies meet the intent of Office of Management and Budget guidance on information technology investment baseline management policies, to include procedures that:

- (a) clarify the specific information needed to support change requests for deviations from approved investment baselines;
- (b) specify the minimum documentation necessary to demonstrate the analysis of alternatives performed to support decisions to improve, enhance, or modernize existing information technology investments, or to implement changes to investment baselines; and
- (c) establish the circumstances under which a new investment proposal is warranted in lieu of a change request.

Management Response: Management concurs with this recommendation. OIT will revise its policies and procedures, as recommended.

Recommendation 3: Provide training to personnel with investment oversight and program management responsibilities that, at a minimum, addresses the SEC's information technology investment baseline management policies and procedures.

Management Response: Management concurs with this recommendation. OIT will implement training for personnel with investment oversight and program management responsibilities that addresses the SEC's information technology investment baseline management policies and procedures, as recommended.

Recommendation 4: Update its capital planning and investment control policies and procedures and implement processes to:

- (a) establish a uniform refresh plan or a strategic approach for the replacement of hardware assets, and document performance against planned cost, quantities, and type of hardware assets to be replaced annually; and
- (b) monitor investments in hardware asset purchases beyond receipt of the assets to ensure the assets are efficiently and effectively deployed and the investments achieve expected outcomes or goals and provide requested capabilities.

Management Response: Management concurs with this recommendation. OIT will revise its policies and procedures, as recommended.

Recommendation 5: Establish documentation requirements for thoroughly supporting independent Government cost estimates.

Management Response: Management concurs with this recommendation. OA will revise the Independent Government Cost Estimate Guide to include minimum required supporting documentation for IGCEs.

In addition, while not formal recommendations, the OIG encouraged: OIT to assess and, as needed, revise its processes for (1) conducting alternatives analyses leading to investment selection, and (2) documenting management decisions; and, agency management to (1) consider actions necessary to mitigate the risks associated with its data center vendor lock-in and contract periods of performance, and (2) timely implement those actions deemed necessary and appropriate. Management concurs with these suggestions.

Finally, we would like to express our appreciation for the courtesy you and your staff extended to us during this audit. If you have any questions or would like to discuss any of our comments, please let us know.

cc: Vance Cathell, Director, Office of Acquisitions
 Charles Riddle, Acting Director/Chief Information Officer, Office of Information Technology

Major Contributors to the Report

Kelli Brown-Barnes, Audit Manager

Sara Tete Nkongo, Lead Auditor

John Dettinger, Auditor

Leann Harrier, Assistant Counsel

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

Web: <https://www.sec.gov/oig>

Telephone: 1-833-SEC-OIG1 (833-732-6441)

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