U.S. SECURITIES AND EXCHANGE COMMISSION

REPORT NO. 568

SEPTEMBER 29, 2021

OFFICE OF INSPECTOR GENERAL

OFFICE OF AUDITS

Additional Steps Are Needed For the SEC To Implement a Well-Defined Enterprise Architecture

This report contains non-public information about the U.S. Securities and Exchange Commission's information technology program. We redacted the non-public information to create this public version. All redactions are pursuant to Freedom of Information Act exemption (b)(7)(E) unless otherwise stated.

REDACTED FOR PUBLIC RELEASE

OFFICE OF
INSPECTOR GENERAL

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

MEMORANDUM

September 29, 2021

TO: Kenneth Johnson, Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General

SUBJECT: *Additional Steps Are Needed For the SEC To Implement a Well-Defined Enterprise Architecture*, Report No. 568

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) implementation of an enterprise architecture. The report contains six recommendations that should help improve the SEC's implementation of a well-defined enterprise architecture, and one recommendation to improve the SEC's oversight of enterprise architecture support services contracts.

On August 26, 2021, we provided management with a draft of our report for review and comment. In its September 21, 2021, response, management concurred with our recommendations. We have included management's response as Appendix V 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 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: Gary Gensler, Chair
Prashant Yerramalli, Chief of Staff, Office of Chair Gensler
Heather Slavkin Corzo, Policy Director, Office of Chair Gensler
Kevin R. Burris, Counselor to the Chair and Director of Legislative and Intergovernmental Affairs
Scott E. Schneider, Counselor to the Chair and Director of Public Affairs
Lisa Helvin, Legal Counsel, Office of Chair Gensler
Hester M. Peirce, Commissioner

Benjamin Vetter, Counsel, Office of Commissioner Peirce
Elad L. Roisman, Commissioner
Matthew Estabrook, Counsel, Office of Commissioner Roisman
Allison Herren Lee, Commissioner
Frank Buda, Counsel, Office of Commissioner Lee
Andrew Feller, Counsel, Office of Commissioner Lee
Caroline A. Crenshaw, Commissioner
David Hirsch, Counsel, Office of Commissioner Crenshaw
John Coates, General Counsel
David Bottom, Director/Chief Information Officer, Office of Information Technology
Jeffrey Stagnitti, Associate Director/Managing Executive, Office of Information Technology
Michael McAdams, Assistant Director, Planning and Governance, Office of Information Technology
David Parrish, Assistant Director, Enterprise Platforms, Office of Information Technology
Bridget Hilal, Branch Chief, Cyber Risk and Governance Branch, Office of Information Technology
Vance Cathell, Director, Office of Acquisitions
Michael Whisler, Assistant Director, Office of Acquisitions
Nick Chung, Competition Advocate/Small Business Specialist, Office of Acquisitions
Caryn Kauffman, Chief Financial Officer and Acting Chief Risk Officer
Mathew Keeler, Management and Program Analyst, Office of Chief Risk Officer

EXECUTIVE SUMMARY

Additional Steps Are Needed For the SEC To Implement a Well-Defined Enterprise Architecture

REPORT NO. 568 | SEPTEMBER 29, 2021

WHY WE DID THIS AUDIT

The U.S. Securities and Exchange Commission's (SEC or agency) Office of Information Technology (OIT) has overall management responsibility for the agency's information technology (IT) program including enterprise architecture (EA). The objective of the SEC's EA program is to define strategic business capabilities and align SEC business functions and goals with both project level and enterprise wide IT systems and plans. As noted by the U.S. Government Accountability Office, EA can help organizations realize cost savings and/or cost avoidance, enhance information sharing, and optimize service delivery.

Attempting to modernize and evolve IT environments without an EA to guide and constrain investments often results in operations and systems that are duplicative, not well integrated, unnecessarily costly to maintain and interface, and ineffective in supporting mission goals.

We conducted this audit to determine the extent to which the SEC has implemented an effective EA program to guide and facilitate the modernization of the agency's IT environment.

WHAT WE RECOMMENDED

We made six recommendations to improve the SEC's implementation of a well-defined EA, and one recommendation to improve the SEC's oversight of EA support services contracts. Management concurred with our recommendations, which will be closed upon completion and verification of corrective action that is fully responsive to each recommendation. This report contains non-public information about the SEC's information technology program. We redacted the non-public information to create this public version.

WHAT WE FOUND

We found that the SEC established an EA policy and several governance boards that have a role in EA. In addition, OIT established an EA portal to maintain information on the agency's EA program and the program's functions. The SEC also relies on contractors to provide EA support services, including developing EA artifacts and performing the SEC's annual EA self-assessment. However, additional steps are needed for the SEC to implement a well-defined EA and to improve its oversight of EA support services contractors.

Although the SEC has efforts underway to develop an enterprise roadmap for future years, for fiscal years 2020 and 2021, the SEC did not (1) prepare and submit to the Office of Management and Budget (OMB) an up-to-date enterprise roadmap, and (2) fully develop or maintain a complete set of EA artifacts in accordance with OMB guidance. As a result, the SEC may not have an authoritative source to perform IT portfolio reviews, or may not be able to identify duplicate investments, gaps, and opportunities for collaboration within the SEC and across agencies.

In addition, OIT did not always document IT investments' alignment with the SEC's EA before approving investments' funding; and the SEC's governance boards did not always periodically review IT investments for EA alignment. The SEC has efforts underway to improve IT governance; however, without clearly defined EA governance, the agency risks (1) unwarranted overlap across IT investments, and (2) hindering its ability to ensure maximum systems interoperability and the selection and funding of IT investments with manageable risks and returns.

We also determined that the SEC's oversight of contracts for EA support services can be improved. Specifically, two EA support services contracts potentially overlapped. Moreover, OIT did not adequately oversee contracts for EA support services to mitigate the risk of bias that might arise from contractors' conflicting roles, and to ensure that the SEC's EA self-assessment results prepared largely by a contractor were adequately supported. As a result, between June and August 2020, the SEC spent more than $1 million on two contracts for potentially duplicative application and data rationalization tasks. In addition, agency officials may not have an accurate understanding of the design and operating effectiveness of EA core elements, which can result in organizational operations and supporting technology infrastructures and systems that are duplicative, poorly integrated, unnecessarily costly to maintain and interface, and unable to respond quickly to shifting environmental factors.

Lastly, OIT did not periodically assess IT investments in accordance with federal and SEC guidance, and did not document a formal strategy for the continued use and/or retirement of an enterprise platform that supports multiple critical SEC business applications despite known concerns. Without a periodic assessment of the cost, performance, and risk associated with IT investments, and a formal strategy for the continued use and/or retirement of this platform, the SEC may not be able to minimize unnecessary and poorly planned investments.

Contents

Tables

Abbreviations

ARM	Application Reference Model
BRM	Business Reference Model
CHEVO	Chevo Consulting LLC
CIO	Chief Information Officer
CP List	Contractor Personnel List
CPIC	capital planning and investment control
DME	development, modernization, and enhancement
DRM	Data Reference Model
EA	enterprise architecture
EAC	Enterprise Architecture Council
EAMMF	Enterprise Architecture Management Maturity Framework
FAR	Federal Acquisition Regulation
FEAF	Federal Enterprise Architecture Framework
FITARA	Federal Information Technology Acquisition Reform Act
FY	fiscal year
GAO	U.S. Government Accountability Office
IOC	Information Officer's Council
IRM	Infrastructure Reference Model
IT	information technology
ITCPC	Information Technology Capital Planning Committee
MITRE	MITRE Corporation
[redacted]	[redacted]
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PRB	Project Review Board

PRM	Strategy/Performance Reference Model
Procentrix	Procentrix Inc.
[redacted]	[redacted]
SEC or agency	U.S. Securities and Exchange Commission
SECR	SEC administrative regulation
SRA	SRA International Inc.
SRM	Security Reference Model
[redacted]	[redacted]
[redacted]	[redacted]
TMB	Technology Management Board
TRB	Technical Review Board
[redacted]	[redacted]

Background and Objective

BACKGROUND

As noted by the U.S. Government Accountability Office (GAO), an enterprise architecture (EA) is a blueprint for organizational change defined in models that describe (in both business and technology terms) how the entity operates today and how it intends to operate in the future, including a plan for transitioning to the future state. EA can help organizations realize cost savings and/or cost avoidance, enhance information sharing, and optimize service delivery.[1] Moreover, GAO has stated that:

- effective use of an EA is a hallmark of successful organizations;
- a well-defined EA is an essential tool for leveraging information technology (IT) to transform business and mission operations; and
- attempting to modernize and evolve IT environments without an EA to guide and constrain investments often results in operations and systems that are duplicative, not well integrated, unnecessarily costly to maintain and interface, and ineffective in supporting mission goals.[2]

Within the U.S. Securities and Exchange Commission (SEC or agency), the Office of Information Technology (OIT) has overall management responsibility for the agency's IT program including EA. According to the SEC EA portal, the mission of the SEC's EA program is to take a strategic approach to enterprise decision making, and its objective is to "define strategic business capabilities and align SEC business functions and goals with both project level and enterprise wide IT systems and plans."[3] Within OIT, the EA Branch (also called the EA team) supports the EA mission by performing key functions, including:

- ensuring OIT and SEC business alignment with the agency's mission;
- ensuring compliance with standards and policies; and

[1] U.S. Government Accountability Office, *Organizational Transformation: Enterprise Architecture Value Needs to Be Measured and Reported* (GAO-12-791; September 2012). This GAO report references the following federal agency financial benefits achieved as a result of EA: (1) the Department of the Interior used EA to modernize agency IT operations and avoid costs through enterprise software license agreements and hardware procurement consolidation, resulting in reported financial benefits of at least $80 million; (2) the Department of Health and Human Services, facilitated by its architecture program, moved to a new telecommunications contract, resulting in a savings of about $21 million; (3) the Nuclear Regulatory Commission avoided an estimated $1.3 million cost by eliminating duplicative staff planning systems; (4) the Department of Defense reported saving $179 million by streamlining Navy business operations, retiring legacy systems, and moving toward a real-time paperless business environment for processing vendor payments; and (5) the Department of Agriculture reported savings of $27 million by moving 120,000 e-mail users to a cloud-based solution.

[2] U.S. Government Accountability Office, *Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation* (GAO-06-831; August 2006).

[3] The SEC EA portal contains information about OIT's Office of Enterprise Architecture (or EA Branch) and its functions in addition to EA resources.

- allowing stakeholders to prioritize and justify technology decisions based on the "big picture," among other functions.

In fiscal year (FY) 2016 and with the assistance of an EA support services contractor, OIT began performing annual self-assessments of the SEC's EA program using GAO's EA Management Maturity Framework (EAMMF).[4] The EAMMF describes 59 core elements of EA management, which collectively represent the practices, structures, activities, and conditions that, when properly employed, can permit an organization to maximize its chances of realizing an EA's institutional value.[5] Based on the annual self-assessment, OIT assigns one of three values to each core element: fully met, partially met, or not met.

Table 1 summarizes the SEC's EA self-assessment results for FYs 2016 to 2020 and illustrates that the number of EA core elements assessed as fully met each year has gradually increased. However, in FY 2020, OIT concluded that the SEC fully met less than half (that is, 26 of 59) of the EAMMF core elements of EA management. We discuss in greater detail the SEC's annual EA self-assessments on page 17 of this report.

TABLE 1. SEC's EA Self-Assessment Results by FY (2016-2020)

FY	Number of EA Core Elements . . .			Total Number of EA Core Elements Assessed
	Fully Met	*Partially Met*	*Not Met*	
2016	9	19	31	59
2017	10	35	14	59
2018	14	35	10	59
2019	23	29	7	59
2020	26	28	5	59

Source: Office of Inspector General (OIG)-generated based on the SEC's EA self-assessments.

Federal Law and Guidance. Through the years, federal law and guidance have directed agencies to develop EA processes to assist in achieving agency strategic goals and information resources management goals. This includes the Clinger-Cohen Act of 1996 (Clinger-Cohen Act),[6] which calls for executive agencies[7] to develop, maintain, and facilitate the implementation of a sound and integrated IT architecture, and to monitor and evaluate the performance of agency IT systems. The Clinger-Cohen Act also states executive agencies shall ensure that performance measurements measure how well IT systems support agency programs, and requires agencies to monitor and evaluate the performance of IT

[4] U.S. Government Accountability Office, *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management* (Version 2.0) (GAO-10-846G; August 2010).

[5] According to the EAMMF, a core element is an EA practice or condition that should be performed or met.

[6] 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).

[7] For the purposes of the Clinger-Cohen Act, the SEC is an "executive" agency. In addition, SEC regulations (such as SECR 24-02, *Information Technology Capital Planning and Investment Control* [Rev 2.2]; July 2018) establish the Clinger-Cohen Act as authoritative guidance.

programs to determine whether to continue, modify, or terminate a program or project. In addition to the Clinger-Cohen Act, the Federal Information Technology Acquisition Reform Act (FITARA)[8] establishes specific requirements related to federal IT acquisition, including requirements for reviews of agency IT investment portfolios.[9]

The Office of Management and Budget (OMB) has also established guidance for developing and using EA in the federal government. For example, OMB's *Common Approach to Federal Enterprise Architecture* (Common Approach to Federal EA), released in May 2012, promotes "increased levels of mission effectiveness by standardizing the development and use of architectures within and between Federal Agencies."[10] In January 2013, OMB issued the *Federal Enterprise Architecture Framework Version 2* (FEAF), which describes a suite of tools to help government planners implement the Common Approach to Federal EA.[11] In addition, OMB Circular A-130[12] states that agencies shall develop an EA that describes the baseline architecture, target architecture, and a transition plan to get to the target architecture. Finally, OMB's Capital Programming Guide states that a complete EA consists of a set of interrelated "reference models" designed to facilitate cross-agency analysis and identification of duplicate investments, gaps, and opportunities for collaboration within and across agencies.[13] Collectively, the federal guidance issued by OMB establishes principles for using EA to help agencies eliminate waste and duplication, increase shared services, close performance gaps, and promote engagement among government, industry, and citizens.

SEC Policies and Procedures. The SEC has also established agency-specific EA policies and procedures. For example, in January 2018, OIT revised the SEC administrative regulation (SECR) governing the development, maintenance, and implementation of an EA at the SEC.[14] This SECR establishes the SEC EA policy pursuant to the Clinger-Cohen Act. OIT policy 24-01-CPIC, *Capital Planning and Investment Control* (CPIC policy) (June 2020), establishes the processes, roles, and responsibilities for the SEC's capital planning and investment control (CPIC) process. In addition, SECR 24-02, *Information Technology Capital Planning and Investment Control* (Revision 2.2; July 2018) (SECR 24-02), describes the CPIC process and states, "the CPIC process applies to all IT investments within the SEC." According to the SEC EA policy, EA is fully integrated with the SEC's capital planning process, and serves to inform, guide, and manage the agency's IT investment decisions. The SEC EA policy also states that EA is a practical description of the SEC systems using industry standard models. The SEC

---

[8] Federal Information Technology Acquisition 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).

[9] Although the SEC is not a "covered agency" for the purposes of FITARA, SEC regulations (such as SECR 24-1.2, *Introduction of New Technology into the Agency* [Rev 1]; September 2017) establish FITARA as authoritative guidance.

[10] Office of Management and Budget, *The Common Approach To Federal Enterprise Architecture* (May 2012).

[11] Office of Management and Budget, *Federal Enterprise Architecture Framework Version* 2 (January 2013).

[12] Office of Management and Budget, Circular No. A-130, *Managing Information as a Strategic Resource* (July 2016).

[13] Office of Management and Budget, Capital Programming Guide Version 3.1, *Supplement to Office of Management and Budget Circular No. A-11*: *Planning, Budgeting, and Acquisition of Capital Assets* (December 2020).

[14] U.S. Securities and Exchange Commission, SECR 24-1.6, *Enterprise Architecture* (Revision 2) (January 2018), referred to hereafter as "SEC EA policy."

also has several governance boards (also referred to as governance authorities) that have a role in EA, as we further discuss on page 10 of this report.

Prior OIG Work. Prior OIG reviews have identified EA-related deficiencies and potential concerns, including: (1) lack of accurate and up-to-date inventories; (2) limited performance monitoring processes; and (3) challenges in stabilizing the [redacted] platform. The OIG verified management implementation of corrective actions to address OIG recommendations related to these issues and, as of the date of this report, OIG recommendations related to these issues were closed for reporting purposes. Appendix I includes additional information about prior SEC OIG and GAO work relevant to our audit.

OBJECTIVE

Our overall objective was to determine the extent to which the SEC has implemented an effective EA program to guide and facilitate the modernization of the agency's IT environment. To achieve our objective, among other work performed, we:

- Met with SEC management and staff from OIT, the Office of Acquisitions, and the Office of the Chief Data Officer.
- Reviewed applicable federal law, guidance, and regulation, and relevant SEC policies and procedures.
- Reviewed the SEC's EA self-assessment reports for FYs 2016 to 2020.
- Reviewed investment documents and governance boards' meeting minutes.

The audit scope period included the SEC's EA program and performance processes in place as of FY 2021, including those relevant to the [redacted] platform and the critical systems it hosts. Appendix I includes additional information about our scope and methodology, including our review of internal controls and prior coverage. Appendices II and III provide the core elements of the SEC's EA program and the SEC IT investments that we reviewed in detail, respectively.

Results

FINDING 1. THE SEC DID NOT PREPARE AND SUBMIT TO OMB AN UP-TO-DATE ENTERPRISE ROADMAP, AND DID NOT FULLY DEVELOP OR MAINTAIN EA ARTIFACTS

According to OMB, agencies shall create an enterprise roadmap (which combines the artifacts developed for the EA) and submit an updated enterprise roadmap to OMB annually.[15] In addition, OMB defines required core artifacts, which serve to promote consistent views and interoperability within and between government organizations, and elective EA artifacts to support additional analysis if needed. The SEC has efforts underway to develop an enterprise roadmap for future years. However, for FYs 2020 and 2021, the SEC did not (1) prepare and submit to OMB an up-to-date enterprise roadmap, and (2) fully develop or maintain a complete set of EA artifacts in accordance with OMB guidance. This occurred, in part, because OIT did not define or establish processes, including roles and responsibilities, to develop and/or update an enterprise roadmap at regular intervals and submit the roadmap to OMB. In addition, the SEC had not defined or established processes, including roles and responsibilities, to develop and periodically update EA artifacts. As a result, the SEC may not have an authoritative source to perform IT portfolio review,[16] or may not be able to identify duplicate investments, gaps, and opportunities for collaboration within the SEC and across agencies. Additionally, the agency may not be in compliance with federal guidance.

Lack of Up-to-date Enterprise Roadmap

For FYs 2020 and 2021, the SEC did not prepare and submit to OMB an up-to-date enterprise roadmap in accordance with federal guidance. According to OMB's FEAF, "the agency will create an enterprise roadmap to document the current and future architecture states at a high level and presents the transition plan for how the agency will move from the present to the future in an efficient, effective manner." In addition, OMB's Common Approach to Federal EA states that the enterprise roadmap "documents and maps the organization's strategic goals to business services, integrating technology solutions across all of the Agency's lines of business." Moreover, the roadmap discusses the overall EA and identifies performance gaps, resource requirements, planned solutions, transition plans, and a summary of the current and future architecture. The roadmap combines artifacts developed for the EA and describes the EA governance process, the implementation methodology, and the documentation framework. OMB's Common Approach to Federal EA further states, "To support the annual Federal

OMB guidance directs agencies to annually create and submit an updated enterprise roadmap to facilitate IT portfolio review

[15] Office of Management and Budget, *The Common Approach To Federal Enterprise Architecture* (May 2012); and *Federal Enterprise Architecture Framework Version 2* (January 2013).

[16] OMB issues and annually updates Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, which states "portfolio reviews ensure the selection of IT investments that support the agency's strategic objectives or performance goals."

Budget process, each Federal Agency will submit an updated Enterprise Roadmap to OMB's Office of E-Government and IT on or before April 1st" so that it can serve as an authoritative reference for IT portfolio review. Submitting an enterprise roadmap annually to OMB is also included in OMB's Memorandum, *Increasing Shared Approaches to Information Technology Services* (May 2012), and in OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget* (June 2019).

When asked about the SEC's enterprise roadmap, OIT provided the *OIT Enterprise Architecture 2018-2019 Roadmap* (hereafter the *EA Roadmap 2018-2019*) and the *Technology Strategic Plan 2018-2020*. The *EA Roadmap 2018-2019* discusses topics such as EA primary focus, functions, and tasks for 2018-2019 and the principles for EA's emerging role in supporting digital transformation at the SEC. In addition, the *OIT Technology Strategic Plan 2018-2020* discusses strategic initiatives that address operating division priorities and their technology implications. However, the outdated *EA Roadmap 2018-2019* and *Technology Strategic Plan 2018-2020* do not reflect the SEC's current (as of FYs 2020 or 2021) and planned future architecture states at a high level or present the transition plan for how the agency will move from the present to the future.

Although these key documents are out of date, the SEC has efforts underway to develop an enterprise roadmap for future years. Specifically, the agency engaged a contractor to assist in developing and deploying "a new, responsive target architecture while reducing the operating risks of implementing a new architecture and ensuring operational continuity." The contractor deliverables include a 3-year operating plan. OIT provided the draft operating plan, which depicts a sequenced portfolio (or menu) of application and architecture investment choices that will inform the SEC's decision-making for capital planning activities through FY 2023.

The SEC did not have an up-to-date enterprise roadmap or submit a roadmap to OMB, in part, because OIT had not defined or established processes, including roles and responsibilities, to complete these actions in accordance with federal guidance. As a result, the agency may not have an authoritative source to perform IT portfolio reviews, and the SEC may not be able to ensure alignment of IT investments with the agency's strategic goals. Additionally, the agency may not be in compliance with federal guidance.

Lack of Complete and Current EA Artifacts

We also determined that the SEC did not fully develop or maintain a complete set of EA artifacts in accordance with OMB guidance. Although the type and depth of EA documentation used by an agency should be guided by the need for detail and answers to questions about requirements, applicable standards, timeframes, and available resources, OMB's FEAF and Common Approach to Federal EA consist of six interrelated "reference models" (also called sub-architecture domains or views). Collectively, the reference models are designed to facilitate cross-agency analysis and identification of duplicate investments, gaps, and opportunities for collaboration within and across agencies. Moreover, OMB's FEAF and Common Approach to Federal EA establish one required core EA artifact for each of the six reference models. These core artifacts also serve to promote consistent views and interoperability within and between government organizations. Table 2 lists the six reference models and each model's required core EA artifact.

TABLE 2. EA Reference Models and Required Core Artifacts

Reference Model	Required Core Artifact
Strategy/Performance Reference Model (PRM)	Concept Overview Diagram
Business Reference Model (BRM)	High-Level Business Process Diagram
Data Reference Model (DRM)	High-Level Logical Data Model
Application Reference Model (ARM)	Application Interface Diagram
Infrastructure Reference Model (IRM)	High-Level Network Diagram
Security Reference Model (SRM)	Security Control List/Catalog

Source: OIG-generated based on OMB's FEAF and Common Approach to Federal EA.

In addition to the one required core artifact for each reference model, OMB's FEAF and Common Approach to Federal EA establish dozens of elective EA artifacts to support additional analysis if needed. These elective artifacts include, but are not limited to:

- a strategic plan and performance measures scorecards for the PRM;
- a business operating plan and use case narratives for the BRM;
- a data dictionary and data flow diagram for the DRM;
- an application inventory and application maintenance procedure for the ARM;
- a technical standards profile and asset inventories (including hardware and software inventories) for the IRM; and
- a disaster recovery plan and continuity of operations plan for the SRM.

According to the agency's Chief Enterprise Architect, the SEC is developing EA artifacts as outlined in OMB guidance. However, as we further describe below, in FYs 2020 and 2021 the agency did not (1) develop a set of core and elective artifacts for each of the six reference models, or (2) ensure that existing artifacts were complete and current.

Required Core Artifacts. The SEC developed the required core artifacts for four of the six reference models (the BRM, IRM, ARM, and SRM), but did not develop the required core artifacts for the remaining two reference models (the PRM and DRM). In addition, at the time of our audit, only one of these four artifacts was current (the security control list/catalog for the SRM). The remaining required core artifacts were either not up-to-date and/or were incomplete. For example, the high-level business process diagram for the BRM and the high-level network diagram for the IRM were last updated in April 2016 and February 2020, respectively; and the application interface diagram for the ARM was not complete.

Elective Artifacts. The SEC developed a complete set of elective artifacts for one of the six reference models (the SRM), but either did not develop, complete, or keep current elective artifacts for the remaining five reference models. For example, although OIT staff stated that the agency's EA team informally has efforts to address EA outcomes, there was no artifact or formal process to define and measure EA outcomes such as performance measures scorecards used to track performance metrics

and identify performance gaps. In addition, the SEC has efforts underway to develop an operating plan, use case narratives, an authoritative application list, and guidelines and policies for classifying data as High, Medium, or Low sensitivity. However, at the time of our audit fieldwork, the agency's data catalog did not consistently include a data classification or a data dictionary describing each dataset. Furthermore, [redacted], technical standards profile, and assets inventory listings were not comprehensive or up-to-date. In March 2018, SEC OIG Report No. 546 recommended that OIT define and implement a process to develop and maintain up-to-date inventories, including inventories of SEC hardware, [redacted].[17] Although in FY 2021 OIT established processes to address this prior OIG recommendation, the SEC's [redacted] was not comprehensive or up-to-date as of the time of our fieldwork.

The SEC did not fully develop or maintain EA artifacts in accordance with OMB guidance, in part, because OIT had not defined the agency's expectations including the core artifact and relevant elective artifacts needed to support each of the six reference models. Additionally, the SEC had not defined processes, including roles and responsibilities, to develop and periodically update core and elective EA artifacts. As a result, the SEC may be hindered in its ability to (1) promote consistent views and interoperability within the agency, and (2) identify duplicate investments, gaps, and opportunities for collaboration within the agency and across agencies. In Finding 3, we further discuss concerns with tasking a contractor to review artifacts, policies, procedures, and guidance it helped create.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

To improve the SEC's implementation of a well-defined enterprise architecture, we recommend that the Office of Information Technology:

Recommendation 1:

Define and/or establish processes, including roles and responsibilities, to prepare and timely update the SEC enterprise roadmap at regular intervals and to submit the roadmap to the Office of Management and Budget in accordance with federal guidance.

Management's Response. Management concurred with the recommendation. The SEC will work with the Office of Management and Budget to determine and submit appropriate roadmap materials. Management's complete response is reprinted in Appendix V.

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.

[17] U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017* (Report No. 546, March 2018); Recommendation 3.

Recommendation 2:

Define the SEC's expectations including the core artifact and relevant elective artifacts needed to support each of the six enterprise architecture reference models, and processes, including roles and responsibilities, to develop and periodically update these artifacts.

Management's Response. Management concurred with the recommendation. The Office of Information Technology will define which artifacts are required or elective to support each of the six enterprise architecture reference models and develop processes, including roles and responsibilities, to develop and periodically update these artifacts. Management's complete response is reprinted in Appendix V.

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

FINDING 2. GOVERNANCE PROCESSES DID NOT ALWAYS DEMONSTRATE THAT OIT CONSISTENTLY INTEGRATED EA INTO THE SEC'S CPIC PROCESS

According to OMB's Common Approach to Federal EA, the first "basic element" to ensure that agency EA programs are complete and can be effective in developing solutions that support planning and decision-making is governance, which addresses the processes, approval mechanisms, policies, roles, and responsibilities needed to establish and operate the EA program. Moreover, federal guidance establishes the need to directly align EA with capital planning efforts to meet agency strategic objectives and performance goals. The SEC has established governance boards with various degrees of involvement in the agency's EA, and an EA policy addressing the roles and responsibilities for the agency's EA program. However, the agency's governance processes did not always demonstrate that OIT consistently integrated EA into the SEC's CPIC process in accordance with the SEC EA policy. Specifically, we found that OIT did not always document IT investments' alignment with the SEC's EA before approving investments' funding; and governance boards did not always periodically review IT investments for EA alignment. This occurred, in part, because SEC IT governance is complex and there is not a designated entity within the agency that is ultimately accountable for EA development and maintenance and for aligning EA with capital planning efforts. The SEC has efforts underway to improve IT governance; however, without clearly defined EA governance, the agency risks (1) unwarranted overlap across IT investments, and (2) hindering its ability to ensure maximum systems interoperability and the selection and funding of IT investments with manageable risks and returns.

Federal and SEC Capital Planning and EA Governance Requirements, Roles, and Responsibilities

The Clinger-Cohen Act requires that each agency establish a CPIC process "for maximizing the value and assessing and managing the risks of information technology acquisitions of the executive agency" throughout the investment life cycle. In addition, OMB's Common Approach to Federal EA states that the first basic element to ensure that agency EA programs are complete and can be effective in developing solutions that support planning and decision-making is governance. According to OMB, governance identifies the planning, decision-making, and oversight processes and groups that will determine how the EA is developed, verified, versioned, used, and sustained over time. OMB's FEAF also makes clear that governance provides "a definition of roles and responsibilities to ensure performance metrics are met." Moreover, in reports issued in 2006 and 2010,[18] GAO has stated:

- An executive committee should be ultimately accountable for EA development and maintenance, and "an organization should have a chief architect who leads the corporate EA program office and who is responsible for EA development and maintenance and accountable to the executive committee."

[18] U.S. Government Accountability Office, Report to the Chairman, Committee on Government Reform, House of Representatives, *Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation* (GAO-06-831; August 2006); and U.S. Government Accountability Office, Executive Guide, *A Framework for Assessing and Improving Enterprise Architecture Management* (Version 2.0) (GAO-10-846G; August 2010).

- A written EA policy should provide for developing a performance and accountability framework that identifies each player's roles, responsibilities, and relationships and describes the results and outcomes for which each player is responsible and accountable.
- A well-defined EA is an essential tool for leveraging IT to transform business and mission operations, and using EA to identify and address ongoing and proposed IT investments that are conflicting, overlapping, not strategically linked, or redundant avoids unwarranted overlap across investments and ensures maximum systems interoperability, as well as the selection and funding of IT investments with manageable risks and returns.

According to the SEC's EA portal, EA governance addresses the processes, approval mechanisms, policies, roles, and responsibilities needed to establish and operate the SEC's EA program. The SEC established a CPIC process and governance boards to approve for funding (that is, select), manage, and evaluate IT investments. Specifically, the CPIC policy and SECR 24-02 establish and define the SEC's CPIC policy and processes. SECR 24-02 refers to the following three governance boards (or authorities) with various degrees of involvement in the agency's EA:

1. Information Technology Capital Planning Committee (ITCPC)
2. Project Review Board (PRB)
3. Information Officers' Council (IOC)

These governance boards have the authority to select, manage, and evaluate IT investments within their purview. SECR 24-02 also states "the CPIC process shall be structured so that the SEC can establish a process, based on IT investment selection criteria for preparing, submitting, and evaluating IT business cases," and such criteria should establish whether and how the proposed investments meet compliance requirements including federal and SEC EA requirements. To ensure compliance with EA, the SEC EA policy states the ITCPC, assisted by the IOC and the Technical Review Board (TRB), serves as the EA review board. The SEC EA policy also states "EA shall be fully integrated with the SEC's IT capital planning process," and the TRB "evaluates current and proposed IT projects for compliance with EA." In addition, the SEC established an Enterprise Architecture Council (EAC) to provide input to the EA alignment of programs, projects, or other IT investments. According to the TRB charter, the TRB provides a process for reviewing technology solutions and technical architecture designs that align with the SEC's EA. Appendix IV includes a high-level description of governance authorities with a role in EA based on their respective charters and/or OIT policies.

OIT uses spreadsheets to capture its review of IT investments' EA alignment before ITCPC funding approval. These spreadsheets capture and specify whether OIT has fully documented each proposed investment's alignment with the agency's EA, and whether OIT consulted with the EA team regarding each request.

Although the SEC has established governance boards with various degrees of involvement in the agency's EA and an EA policy, for IT investments funded in FY 2020, governance processes did not always demonstrate that OIT consistently integrated EA into the SEC's capital planning process in accordance with agency policy. As we further describe in the sections that follow, OIT did not always

document IT investments' alignment with EA before approving investments' funding; and governance boards did not always review the SEC's IT investments for EA alignment.

OIT Did Not Always Document IT Investments' Alignment With EA Before Funding Approval

In FY 2020, the SEC spent about $357 million on IT investments for the development, modernization, and enhancement (DME) of SEC systems and for steady state (that is operations and maintenance) investments.[19] OIT provided FY 2020 OIT EA review spreadsheets listing 123 DME investments and 415 steady state investments and stated, "These indicate that there was EA review of FY 20 investments." However, the spreadsheets did not indicate that OIT fully documented any of the 123 DME investments' alignment with EA. In addition, for 68 of the 123 DME investments (or about 55 percent), FY 2020 OIT EA review spreadsheets did not indicate that OIT consulted with the EA team regarding the investments' funding requests before ITCPC funding decision/approval. Likewise, the spreadsheets did not indicate that OIT consulted with the EA team regarding any of the 415 steady state investments' funding requests before ITCPC funding approval. OIT management and staff provided documentation to demonstrate there were subgroup meetings (before ITCPC funding approval meetings) to walk through the investments in more detail. However, OIT did not provide documentation to demonstrate that these subgroup meetings discussed IT investments' alignment with EA. OIT management and staff also stated that, in their view, because steady state investments provide continued operations support for systems in production and do not introduce new technology, OIT management and staff are not required to consult the EA team before ITCPC meetings.

Governance Boards Did Not Always Review the SEC's IT Investments for EA Alignment

To determine whether the SEC governance boards previously mentioned reviewed IT investments in accordance with the SEC EA policy and the boards' respective charters, we requested and reviewed the governance boards meeting minutes for FY 2020, as well as project status reports and presentations. We found that either the governance boards' meeting minutes did not demonstrate that these boards reviewed IT investments for alignment with EA, or the governance boards did not meet in FY 2020. Specifically:

- The FY 2020 ITCPC and PRB meeting minutes and investment documents (such as monthly or quarterly status report and issues/risks log) did not demonstrate that the ITCPC or the PRB reviewed IT investments for alignment with EA.
- In FY 2020, neither the EAC nor the IOC met or reviewed IT investments for alignment with EA as required by their respective charters and/or by the SEC EA policy.

[19] 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. DME investments lead to new IT assets or systems, or change or modify existing IT assets to substantively improve capability or performance.

In addition, we judgmentally selected 4 of the 10 [redacted]-related investments funded in FY 2020,[20] including 3 DME investments and 1 steady state investment, and requested documentation to demonstrate TRB review of these investments for alignment with EA in accordance with the TRB charter. We found that the TRB did not review two of the four IT investments included in our sample [redacted] for alignment (or compliance) with the SEC's EA. OIT provided documentation to demonstrate that the TRB reviewed the remaining two investments in our sample [redacted] for alignment with EA. OIT management and staff explained that the TRB did not discuss the [redacted] steady state investments' alignment with EA because TRB reviews are not required for steady state investments. OIT added that the requirement for steady state investments to go through the CPIC process became effective in FY 2021. In addition, OIT provided documentation showing that the EA team reviewed the FY 2021 DME investments proposed for funding. OIT personnel also stated that TRB meetings are not required for the [redacted] Strategic Planning investment and provided documentation to demonstrate that OIT discussed high-level strategic plans for the next generation [redacted] solution with the Enterprise Architect and the EA team to ensure alignment with EA. However, according to the SEC EA policy, the TRB (not the Chief Enterprise Architect) evaluates current and proposed IT investments for compliance with EA. Furthermore, SECR 24-02 states that the CPIC process (which applies to all IT investments) should establish criteria addressing whether and how the proposed investments (1) have been evaluated to determine their benefits and risks from both business and technical perspectives, and (2) comply with federal and SEC requirements.

These conditions occurred because SEC IT governance is complex and not clearly defined, as there is not a designated entity ultimately accountable for aligning EA with the agency's capital planning efforts. In addition, OIT did not clearly define the roles and responsibilities of key stakeholders involved in EA. For example, the SEC EA policy does not clearly define or address the roles, responsibilities, and accountability to: develop and maintain EA artifacts/components, develop EA standard operating procedures to support the implementation of the EA policy, or define and monitor EA performance metrics. The SEC has efforts underway to improve IT governance. According to OIT staff, during the ITCPC meeting held on January 26, 2021, it was determined that the EAC would be disbanded and several of the EAC functions were expected to move to a new board (the Technology Management Board, or TMB). In addition, the Chief Information Officer (CIO) stated that the TMB would consolidate the functions of the IOC and EAC. The TMB members began meeting regularly on February 23, 2021, and OIT implemented a TMB charter in April 2021. The TMB reviews have included a review of investments included in the FY 2022 and FY 2023 budget requests to identify investments that are not needed, among other things. However, the TMB charter did not establish a designated entity ultimately accountable for aligning EA with the agency's

SEC IT governance is complex and roles and responsibilities of key stakeholders involved in EA are not clearly defined

[20] Appendix I of this report provides more information on our sampling methodology, and Appendix III presents the four investments selected for review.

capital planning efforts, and OIT did not update its policies and procedures to reflect the TMB as a governance authority, and to remove the IOC and EAC.

Without clearly defined EA governance, the SEC may not avoid unwarranted overlap across IT investments and ensure maximum systems interoperability and the selection and funding of IT investments with manageable risks and returns.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

To improve the SEC's implementation of a well-defined enterprise architecture, we recommend that the Office of Information Technology:

Recommendation 3:

Update existing policies and/or procedures to (a) specify a designated entity ultimately accountable for enterprise architecture development and maintenance, and for aligning enterprise architecture with the SEC's capital planning efforts; and (b) reflect the Technology Management Board as a governance authority, and remove the Information Officer's Council and the Enterprise Architecture Council.

Management's Response. Management concurred with the recommendation. The Office of Information Technology will update existing governance charters to specify a designated entity ultimately accountable for enterprise architecture development and maintenance; and will review and update as necessary, policies for aligning enterprise architecture with the SEC's capital planning efforts. Management's complete response is reprinted in Appendix V.

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 4:

Update existing policies and/or procedures to define the roles and responsibilities of key stakeholders involved in enterprise architecture, including the roles, responsibilities, and accountability to develop standard operating procedures to support the implementation of the SEC's enterprise architecture policy**.**

Management's Response. Management concurred with the recommendation. The Office of Information Technology will update existing policies and/or procedures to define the roles and responsibilities of key stakeholders, including over standard operating procedures. Management's complete response is reprinted in Appendix V.

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. SEC OVERSIGHT OF EA SUPPORT SERVICES CONTRACTS CAN BE IMPROVED

The SEC relies on contractors for EA support services, including developing EA artifacts, standards, processes, and guidelines and performing the SEC's annual EA self-assessment. GAO and the Federal Acquisition Regulation (FAR) have established standards and requirements addressing contract duplication and oversight. Nonetheless, we determined that the SEC's oversight of EA support services contracts can be improved. Specifically, we found that:

- two EA support services contracts potentially overlapped as the SEC awarded a new contract for EA support services already covered under an existing contract; and
- OIT did not adequately oversee contracts for EA support services to mitigate the risk of bias that might arise from contractors' conflicting roles, and to ensure the SEC's annual EA self-assessment results were adequately supported.

These conditions occurred, in part, because different OIT branches initiated and oversaw the SEC's EA support services contracts, and OIT did not define or establish robust processes for monitoring contractors' activities. In addition, the SEC's Office of Acquisitions did not clarify relevant contractual language to prevent the appearance of a potential organizational conflict of interest. As a result, between June and August 2020, the SEC spent more than $1 million on two contracts for potentially duplicative application and data rationalization tasks. Also, another contractor's objectivity might have been impaired with respect to performing the SEC's annual EA self-assessments, which may have misled agency officials about the state of the SEC's EA program. Without an accurate understanding of the design and operating effectiveness of EA core elements, responsible agency officials may invest or continue to invest in organizational operations and supporting technology infrastructures and systems that are duplicative, poorly integrated, unnecessarily costly to maintain and interface, and unable to respond quickly to shifting environmental factors.

Two EA Support Services Contracts Potentially Overlapped

According to GAO, contract duplication can occur when an agency awards two or more contracts to different vendors for similar products or services.[21] In addition, SECR 24-02 states that the contracting officer's representative is responsible for overseeing the day-to-day contract administration aspects of a specified contract including surveillance of the contractor's performance.

We found that, in May 2020, the SEC awarded a new contract to the MITRE Corporation (MITRE)[22] for strategic planning and EA support services already covered under an existing contract with Chevo Consulting LLC (Chevo).[23] Specifically, both contracts included application and data rationalization efforts to enable the SEC's strategic plan. According to OIT management, application and data rationalization

[21] U.S. Government Accountability Office, *Information Technology — Selected Federal Agencies Need to Take Additional Actions to Reduce Contract Duplication* (GAO-20-567; September 2020).

[22] The MITRE contract period of performance was June 2020 to May 2021.

[23] The Chevo contract period of performance was September 2018 to September 2020.

efforts aim to identify the dispositioning (including retirement, consolidation, and maintenance) of existing applications. The MITRE contract also stated that MITRE tasks supported the validation of Chevo application and data rationalization deliverables. Although both contracts included application and data rationalization efforts, the contractors provided different deliverables aimed at identifying and documenting the SEC's investment needs. For example, Chevo provided an *Enterprise-wide Implementation Plan* (August 2020), which included a list of investment initiatives proposed for prioritization and a high-level phased roadmap for the prioritized initiatives for FY 2021 to FY 2023. However, the MITRE application and data rationalization deliverables also included an investment roadmap (embedded in the pre-decisional *FY 2021-2023 SEC Information Technology Operating Plan*, dated May 2021), which depicts "a sequenced portfolio of application and architecture investment choices that will inform decision-making for capital planning activities" through FY 2023. According to the MITRE investment roadmap, previous SEC attempts to identify and document the SEC's investment needs included the FY 2020 Chevo efforts. The MITRE investment roadmap also states that MITRE's investment roadmap was based on lessons learned from these previous attempts, and that these previous attempts "met only with limited success in identifying a viable means for effectively managing technology investments."

The potential contract overlap occurred, in part, because the contracting officer's representatives who oversaw the two contracts were located in two different branches within OIT. According to OIT officials, the OIT Strategy and Innovation Directorate initiated the Chevo contract, and the OIT EA Branch initiated the MITRE contract.

When asked about these two contracts, OIT management and staff stated that the contracts addressed different purposes or levels of application and data rationalization. They also explained that, although the MITRE contract states MITRE tasks supported the validation of Chevo application rationalization deliverables, MITRE personnel simply viewed the research performed by Chevo personnel and held a few knowledge transfer meetings. Nonetheless, based on our review of the contracts and invoices, it appears that there was a potential for duplication of effort between June and August 2020. During these months, the SEC spent a combined total of more than $1 million on these contracts for application and data rationalization efforts ($891,217.80 spent on Chevo, and $136,690.60 spent on MITRE).

OIT Did Not Adequately Oversee Contracts for EA Support Services

GAO and the FAR address requirements to provide greater objectivity and reduce the potential for organizational conflicts of interest. Specifically, GAO's *Standards for Internal Control in the Federal Government* (September 2014) states the following:

- management uses ongoing monitoring and separate evaluations to evaluate the design and operating effectiveness of the internal control system;
- documentation is a necessary part of an effective internal control system; and

- separate evaluations "provide greater objectivity when performed by reviewers who do not have responsibility for the activities being evaluated."[24]

Additionally, FAR 2.101, *Definitions*, describes the impacts of organizational conflicts of interest, stating "that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage." FAR Subpart 9.5, *Organizational and Consultant Conflicts of Interest*, prescribes responsibilities, general rules, and procedures for identifying, evaluating, and resolving organizational conflicts of interest. According to FAR 9.505, one of the underlying principles for evaluating organizational conflicts of interest is "preventing the existence of conflicting roles that might bias a contractor's judgment." FAR 9.504 also advises that significant potential conflicts of interest shall be avoided, neutralized, or mitigated before contract award.

OIT Did Not Establish Processes To Mitigate the Risk of Bias That Might Arise From Contractors' Conflicting Roles. Before January 2021, the SEC contracted with SRA International Inc. (SRA)[25] to, among other activities, lead and assist the agency in developing EA artifacts, standards, processes, and guidelines. Another activity performed by SRA was conducting the SEC's FY 2020 EA self-assessment, which included assessing the EA artifacts, policies, procedures, and guidance SRA had developed.

Contractor objectivity in performing the SEC's FY 2020 EA self-assessment was potentially impaired

Tasking SRA to review artifacts, policies, procedures, and guidance it helped create appears to raise the potential of conflicting roles that might bias a contractor's judgment and impair its ability to be objective. We note that on January 31, 2021, the SEC ended EA support services under the SRA contract and transferred the responsibilities to Procentrix Inc. (Procentrix), creating the same potential of conflicting roles within that contract. During our audit, SEC personnel from the Office of Acquisitions agreed to review and update as necessary relevant contractual documents to clarify the type of support required and to resolve the appearance of a potential conflict.

When asked about these circumstances, OIT management stated that a former OIT staff member reviewed SRA's FY 2020 EA self-assessment results as part of staff's monitoring processes. OIT management also provided documentation to demonstrate that OIT personnel discussed the FY 2020 EA self-assessment results with SRA. Although SRA made editorial updates to the self-assessment report after this discussion, OIT personnel did not take steps to demonstrate or document the actions OIT performed to validate the results of SRA's assessment or to prevent or mitigate the bias that might arise from the contractor's conflicting roles. Specifically, OIT did not demonstrate or document that agency

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

[25] The SRA contract period of performance (base period to option year 3) was May 2020 to April 2021.

personnel verified the SEC's FY 2020 EA self-assessment or otherwise ensured that the results presented by SRA accurately represented the SEC's EA program.

The SEC's FY 2020 EA Self-Assessment Results Were Not Adequately Supported. As stated above, OIT contracted with SRA (and later, Procentrix) to perform an annual assessment of the SEC's EA program. As previously stated in the Background of this report, GAO's EAMMF consists of 59 core elements, or building blocks of EA management that are central to an effective EA program. These 59 core elements are collectively the EA practices, structures, activities, and conditions that can permit organizations to progress to increasingly higher states of EA management maturity and thereby maximize the chances of realizing an EA institutional value.

We assessed OIT's implementation of 19 of the 59 EA core elements (or about 32 percent) to (1) determine the status of each of these core elements in FY 2020, and (2) validate the SEC's FY 2020 EA self-assessment results provided by SRA. This included 10 EA core elements that were assessed as fully or partially met in the SEC's FY 2020 EA self-assessment; all 5 EA core elements that were assessed as not met in the SEC's FY 2020 EA self-assessment; and 4 EA core elements that improved status from FY 2019 to FY 2020. We determined that self-assessment results for 8 of the 19 EA core elements we reviewed were adequately supported. For the remaining 11 EA core elements, the results provided by SRA were not adequately supported.

For example, for EA core element 1 ("Written and approved organization policy exists for EA development, maintenance, and use"), GAO's EAMMF states an organization should have a documented policy to institutionalize the architecture's importance, role, and relationship to other corporate management disciplines. Among other things, the policy should define the EA as consisting of the current ("as-is") and target ("to-be") architecture, as well as the transition plan for migrating from the current to the target architecture. GAO adds that the policy "should provide for developing a performance and accountability framework that identifies each player's roles, responsibilities, and relationships and describes the results and outcomes for which each player is responsible and accountable." Although the SEC has documented a policy that defines the EA as consisting of the current and target architecture, as well as the transition plan, the SEC's EA policy does not provide for developing a performance and accountability framework and OIT did not provide any documentation addressing the EA performance and accountability framework. Nonetheless, the SEC's FY 2020 EA self-assessment results indicated that this EA core element was fully met. As another example, the SEC's FY 2020 EA self-assessment indicated that EA core element 2 ("Executive committee representing the enterprise exists and is responsible and accountable for EA") was fully met. However, in FY 2020, OIT did not assign responsibility and accountability for directing, overseeing, and approving the architecture to a formally chartered committee. Also, the FY 2020 EA self-assessment indicated that EA core element 41 ("EA results and outcomes are measured and reported") was fully met, although OIT had not formally established or defined EA outcomes and results or a method to measure EA outcomes and results. Table 3 in Appendix II provides additional details about the EA core elements we reviewed, including each EA core element title, the SEC's FY 2020 EA self-assessment result, and the OIG's assessment result.

The conditions we observed occurred, in part, because the SEC's Office of Acquisitions did not clarify the relevant contractual language to prevent the appearance of a potential organizational conflict of interest.

In addition, OIT did not define robust processes to adequately oversee the SEC's contracts for EA support services to mitigate the risk of bias that might arise from contractors' conflicting roles, and to ensure EA self-assessment results provided by contractors were adequately supported. As a result, SRA's objectivity in performing the annual assessment of the SEC's EA program might have been impaired, which may have misled agency officials about the state of the SEC's EA program. In addition, without adequate documentation to support the SEC's EA self-assessment results, OIT may not be able to demonstrate the design and operating effectiveness of EA core elements. This may cause the agency's EA program to be ineffective and can result in organizational operations and supporting technology infrastructures and systems that are duplicative, poorly integrated, unnecessarily costly to maintain and interface, and unable to respond quickly to shifting environmental factors.

RECOMMENDATIONS, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

To improve the SEC's implementation of a well-defined enterprise architecture, we recommend that the Office of Information Technology:

Recommendation 5:

Implement processes and controls to mitigate the risk of bias that might arise from contractors' conflicting roles, and to ensure that annual enterprise architecture self-assessment results are adequately supported.

Management's Response. Management concurred with the recommendation. The SEC will evaluate whether future voluntary self-assessments require assessor independence and determine whether to utilize federal staff for such work, or if using contractors, fully document controls to avoid an actual or perceived conflict of interest. Management's complete response is reprinted in Appendix V.

OIG's Evaluation of Management's Response. We are pleased that management concurred with the recommendation. However, as stated in the recommendation, management should also ensure that annual enterprise architecture self-assessment results are adequately supported. We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is fully responsive to the recommendation.

To improve the SEC's oversight of enterprise architecture support services contracts, we recommend that the Office of Information Technology and Office of Acquisitions work together to:

Recommendation 6:

Review and, as necessary, update the SEC's existing enterprise architecture support services contracts to prevent contract duplication and eliminate potential organizational conflicts of interest, even in appearance.

Management's Response. Management concurred with the recommendation. The Office of Information Technology and the Office of Acquisitions have begun efforts to update the two existing enterprise architecture support services contracts to eliminate the appearance of possible contract overlap and potential organizational conflict of interest. Management's complete response is reprinted in Appendix V.

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

FINDING 4. OIT DID NOT PERIODICALLY ASSESS IT INVESTMENTS IN ACCORDANCE WITH FEDERAL AND SEC GUIDANCE, AND DID NOT DETERMINE WHETHER TO CONTINUE OR DISCONTINUE USING THE [redacted] PLATFORM

As previously discussed, the SEC has established processes to select, monitor, and evaluate IT investments. However, OIT did not assess one of the four IT investments included in our sample in accordance with the Clinger-Cohen Act; OMB guidance; and SEC CPIC policy, governance board charters, and related guidance. In addition, OIT did not determine whether to continue or discontinue using the [redacted] platform even though records indicate that the platform no longer met SEC business needs and strategic goals. This occurred in part, because, before June 2020, the SEC CPIC policy did not address a periodic review of steady state investments. In addition, the SEC did not document a formal strategy for the continued use and/or retirement of the [redacted] platform. Without periodic assessment of the cost, performance, and risk associated with IT investments, and a formal strategy for the continued use and/or retirement of the [redacted] platform, the SEC may not be able to minimize costs related to the operational life of agency assets, and minimize unnecessary and poorly planned investments.

Federal and SEC Requirements Addressing IT Investments Performance

The Clinger-Cohen Act states executive agencies shall ensure that performance measurements are prescribed for IT used by or to be acquired by each agency, and that the performance measurements measure how well the IT system supports agency programs. The Clinger-Cohen Act also requires agencies to monitor and evaluate the performance of IT programs to determine whether to continue, modify, or terminate a program or project. In line with the Clinger-Cohen Act, OMB Circular No. A-130 directs agencies to define processes and policies requiring that appropriate measurements are used to evaluate the cost, schedule, and overall performance variances of IT projects across the portfolio. According to FITARA, benefits of reviewing IT investments include identifying potential duplication, waste, and cost savings; and to develop plans for actions to optimize the information technology portfolio, programs, and resources.

For steady state investments, OMB's Circular No. A-11, *Capital Programming Guide,* states a formal operational analysis is warranted,[26] and "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." OMB further states that the investment selection process should eliminate unnecessary and poorly planned projects (or investments). In addition, the Clinger-Cohen Act states that the CIO of an executive agency "shall be responsible for...developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency." Furthermore, "the term 'information technology architecture', with respect to an executive agency, means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals." Similarly, according to OMB Circular No. A-130, EA should "align business and technology resources to achieve strategic

[26] According to OMB, a formal operational analysis includes examining the ongoing performance of an operating asset investment and measuring that performance against an established set of cost, schedule, and performance goals.

outcomes" and "incorporate agency plans for significant upgrades, replacements, and disposition of information systems when the systems can no longer effectively support missions or business functions."

During a prior OIG review, the OIG recommended that the SEC update its CPIC policies and procedures and implement processes for selecting, managing, and evaluating steady state investments in accordance with the Clinger-Cohen Act and with applicable OMB circulars and other guidance.[27] In response, OIT developed and issued the CPIC policy, which established specific processes, roles, and responsibilities for the CPIC process within OIT. These new CPIC processes went into effect as of October 1, 2020, and on November 12, 2020, the SEC began holding PRB meetings to consider and review FY 2021 steady state requests.

According to the SEC's new CPIC policy, all DME investments requiring the expenditure of funds over the government charge card threshold of $10,000, and all steady state investments, must go through the CPIC process.[28] Furthermore, SECR 24-02 states "IT investments over $2 million that are scheduled to take 6 months or longer to complete from time of contract award shall be subject to greater scrutiny and oversight. At a minimum, the responsible project team shall brief the designated governance authority every 6 months concerning resource issues and current progress made against cost, schedule and scope baselines." The PRB charter states that the PRB may require periodic project or program status reviews during an investment's life cycle. In addition, for each investment presented, the PRB will recommend either continuing the investment as proposed by the investment team, or terminating all activities immediately. According to the PRB charter, "if the performance, cost, or schedule is not expected to meet its goals" the PRB can recommend modification, termination, or pursuit of alternatives. Finally, in response to federal requirements to perform an annual operational analysis of steady state investments, OIT developed an online survey to assess whether each steady state investment continues to meet business needs and SEC strategic goals.

OIT Did Not Periodically Assess One IT Investment, As Required, or Determine Whether To Continue or Discontinue Using the [redacted] Platform, Despite Known Concerns

As previously stated, we reviewed one steady state investment and three DME investments funded in FY 2020 [redacted]. We found that OIT did not periodically assess one of these IT investments as required, to identify potential waste or cost savings. In addition, OIT did not determine whether to continue or discontinue using the [redacted] platform even though records indicate that the platform no longer met the SEC's business needs and strategic goals. Specifically:

- For one of the three DME investments in our sample [redacted], OIT did not provide documentation to demonstrate that the PRB reviewed the investment every 6 months in accordance with the SEC's CPIC policy and as required by SECR 24-02. OIT personnel stated

[27] U.S. Securities and Exchange Commission, Office of Inspector General, *The SEC Has Processes To Manage Information Technology Investments But Improvements Are Needed* (Report No. 555; September 2019); Recommendation 1.

[28] 24-01-CPIC, *Capital Planning and Investment Control* (June 25, 2020).

that the designated governance authority mentioned in SECR 24-02 is the Program Management Office, not the PRB, and provided documentation to demonstrate that the Program Management Office reviewed the [redacted] investment every 6 months. However, SECR 24-02 does not specify that the Program Management Office is the designated governance authority.

- To address OMB requirements for a formal operational analysis, OIT performed a survey of steady state investments in FY 2020, which determined that the [redacted] operations and maintenance investment did not meet business needs and SEC strategic goals. However, the PRB did not make a determination to continue or discontinue using the [redacted] platform, and the agency did not use the survey results as a trigger mechanism to take corrective action. As previously stated, "if the performance, cost, or schedule is not expected to meet its goals," the PRB can recommend modification, termination, or pursuit of alternatives.[29] Based on our review of PRB meeting minutes from October 2019 through September 2020, the PRB did not review the steady state investment included in our sample ([redacted] Operations and Maintenance Support). This occurred because this investment was approved for funding in January 2020, before the implementation of the CPIC policy requirement that all steady state investments go through the CPIC process.

[redacted] is an enterprise platform that currently hosts seven applications, which are mission critical to the SEC's business users. These seven applications are [redacted].

Prior OIG reviews have identified challenges related to the agency's implementation of the [redacted] platform.[30] Moreover, OIT's [redacted]

OIT determined that the [redacted] platform is not a viable long-term solution for hosting applications

[redacted] According to discussions held in January 2021, OIT's proposed plan is to move [redacted] from the [redacted] platform to [redacted] or [redacted] within [redacted]. OIT also plans to move [redacted]. OIT provided documentation for a [redacted], which aims to move the system off the [redacted] platform. Similarly, OIT provided an investment proposal for [redacted]. In addition, the agency hired a contractor [redacted]

[29] In FY 2020, the SEC spent about $12.7 million for [redacted] steady state operations and maintenance support.

[30] [redacted]

[redacted] Nonetheless, the SEC has not documented a formal strategy for the continued use and/or retirement of the [redacted] platform.

Without periodic assessments of the cost, performance, and risk associated with these IT investments, or a formal strategy for the continued use or retirement of the [redacted] platform, the SEC may not be able to minimize costs related to the operational life of certain SEC assets, and minimize unnecessary and poorly planned investments.

RECOMMENDATION, MANAGEMENT'S RESPONSE, AND EVALUATION OF MANAGEMENT'S RESPONSE

To improve the SEC's implementation of a well-defined enterprise architecture, we recommend that the Office of Information Technology:

Recommendation 7:

Document a formal strategy for the continued use and/or retirement of the [redacted] platform.

Management's Response. Management concurred with the recommendation. According to the Chief Information Officer, migrations off of the platform [redacted] are underway and funding has been requested to move the remaining applications. In addition, the Office of Information Technology will develop a consolidated strategy, including plans for the applications remaining hosted on the platform. Management's complete response is reprinted in Appendix V.

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

Appendix I. Scope and Methodology

We conducted this performance audit from December 2020 through September 2021 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.

Objective and Scope

Our overall objective was to determine the extent to which the SEC has implemented an effective EA program to guide and facilitate the modernization of the agency's IT environment. Our audit covered the SEC's EA program and performance processes in place as of FY 2021, including those relevant to the [redacted] platform and the critical systems it hosts.

Methodology

To address our objective, among other work performed, we:

- interviewed SEC management and staff assigned to OIT, the Office of Acquisitions, and the Office of the Chief Data Officer at the SEC's Headquarters in Washington, DC;
- reviewed applicable federal law, regulation, and guidance, and relevant SEC policies and procedures; and
- reviewed the SEC's EA self-assessment results from FYs 2016 to 2020, as well as documentation describing management actions to address risks related to EA core elements that were assessed as not met in the FY 2020 self-assessment.

We also selected and reviewed a nonstatistical, judgmental sample of 10 of the 54 EA core elements that were assessed as fully or partially met in the SEC's FY 2020 EA self-assessment, all 5 EA core elements that were assessed as not met in the SEC's FY 2020 EA self-assessment, and 4 of the 6 EA core elements that improved status from FY 2019 to FY 2020. For each of the 19 EA core elements in our sample, we reviewed artifacts to determine their status in FY 2020, and to validate the FY 2020 EA self-assessment results provided by SRA. Because our selection and review of these core elements was nonstatistical, our results cannot be projected. Appendix II includes details about the EA core elements we reviewed.

In addition, we reviewed reports showing the SEC's FY 2020 IT investments including [redacted]-related investments. In FY 2020, the SEC spent about $25 million on 10 DME and steady state investments associated with the [redacted] platform and its hosted applications. This included three DME and two steady state investments for the [redacted] platform totaling about $21 million, and five DME investments to enhance [redacted] applications totaling about $4 million. We selected a nonstatistical, judgmental sample of 4 of these 10 investments. Our sample represented more than 50 percent of the total amount spent on [redacted] and its hosted applications in FY 2020. For each of the IT investments included in our sample, we reviewed investment and contractual documents and focused our review on those controls

intended to ensure that OIT (1) integrated EA in the SEC's CPIC process; and (2) tracked/monitored the cost, performance, and risks associated with these investments and associated systems. Because our selection and review of these four IT investments was nonstatistical, our results cannot be projected. Appendix III includes details about the IT investments we reviewed.

Internal Controls

We identified and assessed internal controls, applicable internal control components, and underlying principles significant to our objectives, as we describe below.

Control Environment. We assessed the control environment established by OIT by reviewing OIT's organizational structure and by interviewing OIT management and staff from various branches including the Enterprise Architecture Branch and the Platform Management Branch. We also reviewed relevant SEC policies and procedures and identified multiple governance boards involved in EA. Based on the work performed, we identified a deficiency in EA governance processes as Finding 2 discusses.

Risk Assessment. We obtained and reviewed OIT's FY 2020 management self-assessment statement and risk controls matrices to identify risks and controls related to the SEC's EA. We also reviewed the SEC's Risk Portfolio and Profile report. One of the outstanding management actions as of September 2020 (included in OIT's FY 2020 management self-assessment statement) pertained to the early architecture review of all technology items. In addition, the SEC's Risk Portfolio and Profile report identified risks related to the SEC's EA and to the [redacted] platform. We considered this information as we planned and performed our work.

Control Activities. We reviewed federal law, regulation, guidance, and SEC policies, procedures, and administrative regulations related to the SEC's EA program. We also sent written inquiries to OIT to obtain descriptions of the control activities applicable to the SEC's EA program. Control activities identified included the governance boards' review of IT investments, and contract monitoring activities. Based on the work performed, we identified a deficiency in EA governance processes as Finding 2 discusses. In addition, as Findings 3 and 4 discuss, OIT did not define robust processes to adequately oversee the SEC's contracts for EA support services, and a formal [redacted] strategy.

Information and Communication. We determined that OIT communicates policies and procedures related to the SEC's EA through the SEC Insider internal site and the EA SharePoint site. However, as Finding 1 discusses, many of the SEC's EA artifacts did not exist or were outdated or incomplete.

Monitoring. We discussed with OIT management and staff their roles and responsibilities for ensuring EA is integrated in the SEC's CPIC process, and in monitoring the performance of the [redacted] platform and the applications it hosts. We also reviewed SEC policies and procedures addressing the controls in place to ensure EA is integrated in the SEC's CPIC process, and to periodically monitor/track the cost, performance, and risks associated with [redacted]-related investments and the corresponding systems. As Finding 2 discusses, we identified deficiencies in integrating EA in the CPIC process (before approving investments' funding, and throughout the investment lifecycle).

Based on the work performed, as noted in this report, we identified areas of potential improvement related to internal control deficiencies that were significant within the context of our audit objective. Our recommendations, if implemented, should correct the weaknesses we identified.

Data Reliability

GAO's *Assessing Data Reliability* (GAO-20-283G, December 2019) states reliability of data means that data are applicable for audit purpose and are sufficiently complete and accurate. Data primarily pertains to information that is entered, processed, or maintained in a data system and is generally organized in, or derived from, structured computer files. Furthermore, GAO-20-283G defines "applicability for audit purpose," "completeness," and "accuracy" as follows:

> "Applicability for audit purpose" refers to whether the data, as collected, are valid measures of the underlying concepts being addressed in the audit's research objectives.
>
> "Completeness" refers to the extent that relevant data records and fields are present and sufficiently populated.
>
> "Accuracy" refers to the extent that recorded data reflect the actual underlying information.

To address our objective, we relied on computer-processed data such as SEC approved hardware, software, and application lists from the agency's EA portal; the SEC Data Catalog; and reports showing FY 2020 IT investments. To assess the reliability of the data from the EA portal and from the SEC Data Catalog, we interviewed SEC management and staff from OIT and from the Office of the Chief Data Officer. We also reviewed the SEC OIG report *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017* (Report No. 546, March 2018), which addressed the need for the SEC to define and implement a process to develop and maintain up-to-date inventories (including hardware, [redacted]). In addition, to assess the reliability of FY 2020 IT investment reports, we corroborated information from OIT's system for tracking IT spending with the investments and contractual records for a sample of four IT investments.

Based on our assessment, the computer-processed data we reviewed was sufficiently reliable in the context of our objective.

Prior Coverage

Between 2006 and 2020, the SEC OIG and GAO issued the following reports of particular relevance to this audit:

SEC OIG:

- *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017* (Report No. 546, March 2018).
- *The SEC Has Processes to Manage Information Technology Investments But Improvements Are Needed* (Report No. 555, September 2019).

GAO:

- *Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation* (GAO-06-831; August 2006).
- *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0)* (GAO-10-846G; August 2010).
- *Organizational Transformation: Enterprise Architecture Value Needs to Be Measured and Reported* (GAO-12-791; September 2012).
- *Information Technology: Selected Federal Agencies Need to Take Additional Actions to Reduce Contract Duplication* (GAO-20-567; September 2020).

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

Appendix II. EA Core Elements Reviewed

The following table provides details about the 19 EA core elements we judgmentally selected and reviewed, including each element's title, the SEC's FY 2020 EA self-assessment results (provided by SRA), and our asessment results based on our review. As shown below and as previously discussed on page 18 of this report, our assessment results for 8 of the 19 EA core elements we reviewed agreed with the SEC's FY 2020 self-assessment results. For the remaining 11 EA core elements we reveiewed, our assessment results differed from the SEC's FY 2020 self-assessment results. As a result, we determined that the SEC's FY 2020 EA self-assessment was not adequately supported.

TABLE 3. Comparison of SEC and OIG Assessment Results for Select EA Core Elements (FY 2020)

	#	EA Core Element Title and Number	SEC	OIG
SEC and OIG Assessment Results Agreed	1	EA performance and accountability framework is established. (Core element 8)	Partially Met	Partially Met
	2	Initial versions of corporate "as-is" and "to-be" EA and sequencing plan exist. (Core element 37)	Partially Met	Partially Met
	3	Subordinate architecture alignment with the corporate EA is measured and reported. (Core element 43)	Partially Met	Partially Met
	4	Corporate EA and sequencing plan are enterprise wide in scope. (Core element 48)	Not Met	Not Met
	5	All segment and/or federated architectures exist and are horizontally and vertically integrated. (Core element 50)	Not Met	Not Met
	6	Corporate and subordinate architectures are extended to align with external partner architectures. (Core element 51)	Not Met	Not Met
	7	EA products and management processes are subject to independent assessment. (Core element 52)	Not Met	Not Met
	8	EA continuous improvement efforts reflect the results of external assessments. (Core element 59)	Not Met	Not Met
SEC and OIG Assessment Results Did Not Agree	9	Written and approved organization policy exists for EA development, maintenance, and use. (Core element 1)	Fully Met	Partially Met
	10	Executive committee representing the enterprise exists and is responsible and accountable for EA. (Core element 2).	Fully Met	Partially Met
	11	EA framework(s) is adopted. (Core element 7)	Fully Met	Partially Met
	12	EA program management plan exists and reflects relationships with other management disciplines. (Core element 15)	Fully Met	Partially Met
	13	EA-related risks are proactively identified, reported, and mitigated. (Core element 25)	Fully Met	Partially Met
	14	Architecture products are being developed according to the EA content framework. (Core element 29)	Fully Met	Partially Met
	15	Program office human capital needs are met. (Core element 36)	Fully Met	Partially Met
	16	One or more segment and/or federation member architectures exists and is being implemented. (Core element 39)	Fully Met	Partially Met
	17	EA results and outcomes are measured and reported. (Core element 41)	Fully Met	Partially Met
	18	Corporate EA and sequencing plan are aligned with subordinate architectures. (Core element 49)	Partially Met	Not Met
	19	EA quality and results measurement methods are continuously improved. (Core element 58)	Partially Met	Not Met

Source: OIG-generated based on OIG review of EA documents provided by OIT.

Appendix III. IT Investments Reviewed

The following table provides details about the three DME and one steady state investment we reviewed, including each IT investment's name and purpose, and the amount spent on each in FY 2020.

TABLE 4. Summary of IT Investments Reviewed

#	Investment Name	Investment Description	Expense Type	Amount Spent in FY 2020
1	[redacted] Application Operations and Maintenance Support	To provide funding for [redacted] application operations and maintenance support, including funding for the applications that are hosted on the [redacted] platform.	Steady State	$12,773,111
2	[redacted]	To provide funding for [redacted]	DME	$2,005,098
3	[redacted] Platform DME Initiatives	To implement (1) [redacted] for the more than [redacted] of content stored on the [redacted] platform, and (2) [redacted] and enhanced report capabilities for the platform and the numerous components.	DME	$1,701,680
4	[redacted]	[redacted]	DME	$493,253
Total FY 2020 Spending for All IT Investments Reviewed				**$16,973,142**

Source: OIG-generated based on FY 2020 IT investment information provided by OIT.

Appendix IV. Governance Authorities Involved in EA

The following table provides a high-level description of the roles and responsibilities of governance authorities with a role in EA based on their respective charters and/or OIT policies.

TABLE 5. Governance Authorities Involved in EA

Governance Authorities	Roles and Responsibilities
EAC	Supports and guides the activities of the SEC's EA. The EAC provides advice to the Chief Enterprise Architect in the conduct of the agency's EA. The EAC also reviews the alignment of IT investments, projects, or programs with the EA. Membership: Members include managing executives and assistant directors from various SEC divisions and offices such as OIT, the Division of Enforcement, and the Division of Corporation Finance. Chaired by the Chief Enterprise Architect.
IOC	Reviews the official version of the current and target architectures prior to the annual review of the IT portfolio, and ensures that the agency's EA practices comply with OMB published guidelines. Membership: Members are senior officers (associate directors or higher) from various SEC divisions and offices including OIT, the Office of Acquisitions, the Office of General Counsel, the Division of Enforcement, and the Division of Corporation Finance. Chaired by the CIO.
ITCPC	Provides strategic direction inputs for the development of EA, evaluates major technology investments, makes final funding decisions by using EA inputs, and uses feedback from EA in monitoring progress toward stated IT goals and in evaluating project results to support future funding decisions. Membership: Members are senior executives from various SEC divisions and offices including OIT, the Office of General Counsel, the Division of Enforcement, and the Division of Corporation Finance. Chaired by the Chief Operating Officer.
PRB	Provides recommendations to the CIO and IOC based on the agency's progress toward implementing projects and programs that align with the SEC's EA. The PRB also reviews IT investments against decision milestones and cost, schedule, or performance goals; and risk mitigation efforts. On an annual basis or as required, the PRB assists the IOC in its preparation and delivery of an EA status update to the ITCPC. Membership: Members are assistant directors from OIT, the Office of Acquisitions, and the Office of Financial Management. Chaired by the associate director/OIT managing executive.
TMB[31]	Established in April 2021, the TMB has the authority to approve all IT investments that fall within the budgetary guidelines set by the ITCPC for the fiscal year. The TMB approves the high-level statement of SEC IT strategic objectives for future fiscal year, oversees the collection of IT investment data from the divisions and offices, and endorses for ITCPC approval the resource requirements and investment roadmap associated with implementing SEC IT strategic objectives. The TMB serves as a forum for discussing ways that future projects could meet the needs of multiple divisions and offices. Membership: Members are senior officials from various SEC divisions and offices including OIT, the Division of Enforcement, the Division of Corporation Finance, and the Office of Acquisitions. Chaired by the CIO.
TRB	Evaluates current and proposed IT projects for compliance with EA, reviews and approves statements of work and ensures compliance with EA, provides strategic direction to the development of EA, and performs a technical review of all EA components. Membership: Members are all from OIT. No designated chair.

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

[31] As previously stated, according to the CIO, the TMB consolidates the functions of the IOC and EAC.

Appendix V. Management Comments

MEMORANDUM

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

From: David Bottom, Chief Information Officer

Bottom, David

Digitally signed by Bottom, David
Date: 2021.09.22 11:58:26 -04'00'

Date: September 21, 2021

Subject: Management Response to Draft OIG Management Report, "Additional Steps are Needed for the SEC to Implement a Well-Defined Enterprise Architecture"

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) Management report, "Additional Steps are Needed for the SEC to Implement a Well-Defined Enterprise Architecture." I appreciate OIG's thorough work analyzing the SEC's Enterprise Architecture (EA) program at the SEC, and concur with the report's seven recommendations for improvement as detailed in Appendix A.

We further appreciate that the OIG recognized the efforts already taken to improve the EA program. These steps include developing an EA portal on the SEC intranet, developing an EA Management Maturity Framework (EAMMF), updating SEC Capital Planning and Investment Control (CPIC) policies, and establishing the new Technology Management Board (TMB) to replace the Enterprise Architecture Council (EAC). Notably, in February of 2021 the Office of Information Technology (OIT) completed a reorganization to join the EA branch with the IT Capital Planning and IT Governance branches, to promote integration and collaboration among these interrelated disciplines.

OIT's EA Branch has also 1) recently completed the Security Reference Model (SRM) to close prior year OIG recommendation 565-05, 2) made significant progress in updating the SEC's [redacted] in advance of upcoming cybersecurity and supply chain vendor management requirements, and 3) initiated a hiring action for a permanent full-time manager for the branch.

I would like to provide some additional context regarding certain sections of the OIG report. The OIG identified two contract-related issues that could have resulted in unnecessary costs, inaccurate programmatic design, and duplicative work. While we understand the OIG's views, we believe that despite the potential for these consequences to occur, due to our strong collaboration between the Office of Acquisitions (OA) Contracting Officers (COs) and OIT Contracting Officer's Representatives (CORs), these detrimental outcomes did not occur.

Two EA Services Contracts Potentially Overlapped

The report describes two contracts where there was potential overlap, specifically in application and data rationalization efforts. OA coordinates closely with divisions and offices to develop contracts that allow the agency flexibility in obtaining services from contractors. This flexibility

1

is balanced by the oversight of the CORs and COs to ensure that work is not duplicated. While the scope of the two contracts identified by OIG provided the SEC with the ability to potentially meet similar service areas, the contracts were used to address different agency requirements, which is reflected in the differing activities, business participants, and deliverables produced by the two vendors.

Mitigation of Bias that Might Arise from Contractors Roles

The report describes an instance where the contractor team that provided program support for the SEC's EA team also completed an EA self-assessment of the SEC's program against the Enterprise Architecture Maturity Model Framework[1]. The self-assessment was intended to provide the EA program an understanding of their current compliance with the EAMMF and identify areas for improvement and was not a required activity of any Federal statute or mandate. While OIT understands OIG's perspective that this approach may be a potential conflict of interest, this was a voluntary assessment and Federal staff provided robust oversight and performed a review of results to ensure the findings were appropriate and accurate, including one review by an EA federal staff member and a second by the Chief Enterprise Architect. Ultimately, the assessment was finalized based on the input of the Federal staff and not the contractor team.

Thank you once again for the professionalism and courtesies you and the OIG audit team demonstrated throughout this audit. We intend to pursue corrective actions as described in Appendix A as a priority, and look forward to working with your office to confirm our actions fully address the issues identified in your report.

cc: Kenneth Johnson, Chief Operating Officer

Vance Cathell, Director, Office of Acquisitions

[1] Per GAO, the EAMMF framework has two primary uses. *First, it can provide a standard yet flexible benchmark against which to determine where the enterprise stands in its progress toward the ultimate goal: having a continuously improving EA program that can serve as a featured decision support tool when considering and planning large-scale organizational restructuring or transformation initiatives (maturity Stages 5 and 6). Second, it can provide a basis for developing architecture management improvement plans, as well as for measuring, reporting, and overseeing progress in implementing these plans.*

Appendix A: Management's Responses to OIG's Recommendations

The following are management's responses to each of the recommendations provided in the OIG report.

Recommendation 1: Define and/or establish processes, including roles and responsibilities, to prepare and timely update the SEC enterprise roadmap at regular intervals and to submit the roadmap to the Office of Management and Budget in accordance with Federal guidance.

> **Response:** We concur. The SEC will work with the Office of Management and Budget (OMB) to determine and submit appropriate roadmap materials. Pending confirmation of OMB requirements, OIT will incorporate this reporting requirement into the SEC's external reporting calendar and follow the appropriate processes for submission.

Recommendation 2: Define the SEC's expectations including the core artifact and relevant elective artifacts needed to support each of the six EA reference models, and processes, including roles and responsibilities, to develop and periodically update these artifacts.

> **Response:** We concur. OIT will define which artifacts are required or elective to support each of the six EA reference models and develop processes, including roles and responsibilities, to develop and periodically update these artifacts.

Recommendation 3: Update existing policies and/or procedures to (a) specify a designated entity ultimately accountable for EA development and maintenance and for aligning EA with the SEC's capital planning efforts; and (b) reflect the TMB as a governance authority and remove the Information Officer's Council [IOC], and the EAC.

> **Response:** We concur. OIT will update existing governance charters to specify a designated entity ultimately accountable for EA development and maintenance. In particular, the charters will be updated reflect the TMB as a governance authority and remove the now-defunct IOC and EAC. OIT will review, and update if necessary, policies for aligning EA with the SEC's capital planning efforts.

Recommendation 4: Update existing policies and/or procedures to define the roles and responsibilities of key stakeholders involved in EA, including the roles, responsibilities, and accountability to develop standard operating procedures to support the implementation of the SEC's EA policy.

> **Response:** We concur. OIT will update existing policies and/or procedures to define the roles and responsibilities of key stakeholders, including over standard operating procedures.

Recommendation 5: Implement processes and controls to mitigate the risk of bias that might arise from contractors' conflicting roles, and to ensure that annual EA self-assessment results are adequately supported.

Response: We concur. The SEC will evaluate whether future voluntary self-assessments require assessor independence and determine whether to utilize federal staff for such work, or if using contractors, fully document controls to avoid an actual or perceived conflict of interest.

Recommendation 6: To improve the SEC's oversight of EA support services contracts, we recommend that the Office of Information Technology and Office of Acquisitions work together to: Review and, as necessary, update the SEC's existing EA support services contracts to prevent contract duplication and eliminate potential organizational conflicts of interest, even in appearance.

Response: We concur. OIT and OA have already begun efforts to update the two existing EA Support Contracts to eliminate the appearance of possible contract overlap and potential organizational conflict of interest. As noted in the audit report, two prior EA support contracts that were cited have expired, so no additional action on these agreements is anticipated.

Recommendation 7: Document a formal strategy for the continued use and/or retirement of the [redacted] platform.

Response: We concur. Migrations off of the [redacted] platform are already underway for [redacted]. The divisions and offices sponsoring the [redacted] have requested FY22 funding to begin their moves. In addition, OIT will develop a consolidated [redacted] strategy that brings together the plans for the remaining applications hosted by the [redacted] platform.

Major Contributors to the Report

Kelli Brown-Barnes, Audit Manager
Sara Tete Nkongo, Lead Auditor
Douglas Carney, Auditor
Michael Burger, Auditor
Sean Morgan, Assistant Counsel

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 below.

TO REPORT

fraud, waste, and abuse

Involving SEC programs, operations, employees, or contractors

FILE A COMPLAINT ONLINE AT

www.sec.gov/oig

CALL THE 24/7 TOLL-FREE OIG HOTLINE

833-SEC-OIG1

CONTACT US BY MAIL AT

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