U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services

November 7, 2019
Report No. 556

REDACTED FOR PUBLIC RELEASE

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

November 7, 2019

TO: Kenneth Johnson, Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General

SUBJECT: *The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services*, Report No. 556

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) adoption of cloud computing services. The report contains three recommendations that should help improve the SEC's planning, management, and implementation of cloud strategies, and the security of its cloud-based systems.

On October 17, 2019, we provided management with a draft of our report for review and comment. In its October 31, 2019, response, management concurred with our recommendations. We have included management's response as Appendix IV in the final report.

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

We appreciate the courtesies and cooperation extended to us during the audit. If you have questions, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects.

Attachment

cc: Jay Clayton, Chairman
Sean Memon, Chief of Staff, Office of Chairman Clayton
Bryan Wood, Deputy Chief of Staff, Office of Chairman Clayton
Peter Uhlmann, Managing Executive, Office of Chairman Clayton
Kimberly Hamm, Chief Counsel/Senior Policy Advisor, Office of Chairman Clayton
Robert J. Jackson Jr., Commissioner
Prashant Yerramalli, Counsel, Office of Commissioner Jackson

REDACTED FOR PUBLIC RELEASE

Hester M. Peirce, Commissioner
Jonathan Carr, Counsel, Office of Commissioner Peirce
Elad L. Roisman, Commissioner
Matthew Estabrook, Counsel, Office of Commissioner Roisman
Allison Herren Lee, Commissioner
Andrew Feller, Counsel, Office of Commissioner Lee
Gabriel Benincasa, Chief Risk Officer
Holli Heiles Pandol, Director, Office of Legislative and Intergovernmental Affairs
John J. Nester, Director, Office of Public Affairs
Robert B. Stebbins, General Counsel
Vance Cathell, Director, Office of Acquisitions
Gregory Steigerwald, Competition Advocate/Small Business Specialist, Office of Acquisitions
Charles Riddle, Acting Chief Information Officer, Office of Information Technology
Laura Kurup, Associate Director/Chief Strategy and Innovation Officer, Office of Information Technology
Andrew Krug, Associate Director/Chief Information Security Officer, Office of Information Technology

Executive Summary

The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services

Report No. 556
November 7, 2019

Why We Did This Audit

Beginning in December 2010, the Office of Management and Budget—citing cloud computing benefits such as potential cost savings, ease in scalability, and procurement efficiencies—directed Federal agencies to default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. Since that time, the Government Accountability Office has issued multiple cloud computing reports, identifying issues such as the need for some Federal agencies to (1) pursue additional cloud opportunities and costs savings, (2) incorporate key performance practices, and (3) improve security.

We conducted this audit to assess the U.S. Securities and Exchange Commission's (SEC or agency) management of the planning, implementation, and security of its cloud computing services. Specifically, we sought to (1) assess the SEC's strategy for migrating information technology services and applications to the cloud, and (2) determine whether key security measures were in place to adequately protect SEC systems that use cloud computing services.

What We Recommended

We made three recommendations to improve the SEC's planning, management, and implementation of cloud strategies, and the security of its cloud-based systems. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action. This report contains non-public information about the SEC's information technology program. As a result, we redacted the non-public information to create this public version.

What We Found

Consistent with Federal guidance, in 2017, the SEC developed its (b) (7)(E) [redacted], which defined the goals and objectives of the agency's cloud program, and a (b) (7)(E) [redacted], which established cloud-related goals. However, we found that the SEC did not fully implement its cloud strategy; follow a clear, robust strategic plan to evaluate and prioritize information technology services and applications for migration to the cloud; or effectively track related goals. Instead, the agency used an "ad hoc" or "as-needed" approach to implementing cloud computing. This occurred because the SEC did not coordinate or collaborate on cloud strategies at an enterprise level. As a result, the SEC has not fully realized the potential performance and economic benefits attributed to cloud computing services.

In addition, we assessed the SEC's key security measures for protecting agency systems that use cloud computing services. Although the SEC's Office of Information Technology developed an information technology security program, an (b) (7)(E) [redacted], and other supporting security policies and procedures governing the agency's systems, processes for protecting the SEC's cloud-based systems need improvement. Specifically, we found that the SEC's:

- system security plans for its [redacted] cloud-based systems in operation as of March 20, 2019, were missing cloud-specific security controls and enhancements; and
- security assessment reports for the [redacted] systems were incomplete.

These conditions occurred because the Office of Information Technology had not developed policies and procedures specific to cloud system security, or adequate processes to ensure compliance with Federal Risk and Authorization Management Program baseline controls and enhancements for which the agency is responsible. As a result, the SEC's processes did not adequately ensure compliance, assess risk, identify issues, or mitigate vulnerabilities specific to the agency's cloud-based systems.

We also identified four other matters of interest that did not warrant recommendations; however, we discussed the matters with agency management for their consideration. These matters involved security categories, reporting of cloud services, incident response processes, and inclusion of security requirements in cloud service contracts. We noted that an open recommendation from prior Office of Inspector General work should address the matter regarding the SEC's cloud service contracts, and we encourage management to implement the previously agreed-to corrective action.

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

TABLE OF CONTENTS

ABBREVIATIONS

CIO	Chief Information Officer
eGRC	enterprise Governance, Risk, and Compliance
FedRAMP	Federal Risk and Authorization Management Program
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
IT	information technology
NIST	National Institute of Standards and Technology
OA	Office of Acquisitions
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
POA&M	plan of action and milestones
SAR	security assessment report
SEC or agency	U.S. Securities and Exchange Commission
(b) (7)(E)	(b) (7)(E)
SP	Special Publication
SSP	system security plan

Background and Objectives

Background

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1] Beginning in December 2010, the Office of Management and Budget (OMB)—citing benefits such as potential cost savings, ease in scalability, and procurement efficiencies—directed Federal agencies to shift to a "Cloud First" policy.[2] In part, this policy required that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. Nevertheless, between 2014 and 2018, the Government Accountability Office (GAO) reported that some Federal agencies needed to (1) pursue additional cloud opportunities and cost savings, (2) incorporate key performance practices, and (3) improve security.[3] In 2019, GAO also reported benefits other Federal agencies realized because of cloud computing services.[4] Such benefits included:

- improved delivery and reduced costs of information technology (IT) services,
- increased efficiency of agency operations and systems,
- enhanced customer service, and
- strengthened mission assurance.

In February 2011, OMB issued its *Federal Cloud Computing Strategy* to further support agencies in migrating toward cloud computing. The strategy highlights security requirements for cloud computing and requires each agency to re-evaluate its

[1] NIST Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*; September 2011.

[2] OMB's *25 Point Implementation Plan to Reform Federal Information Technology Management*; December 9, 2010.

[3] U.S. Government Accountability Office, *Cloud Computing: Additional Opportunities and Savings Need to Be Pursued* (GAO-14-753; September 25, 2014).

U.S. Government Accountability Office, *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance* (GAO-16-325; April 7, 2016).

U.S. Government Accountability Office, *Information Security: Agencies Need to Improve Implementation of Federal Approach to Security Systems and Protecting against Intrusions* (GAO-19-105; December 18, 2018).

[4] U.S. Government Accountability Office, *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked* (GAO-19-58; April 4, 2019).

technology sourcing strategy to include consideration and application of cloud computing solutions as part of the budget process.

Then, in December 2011, OMB issued to agency Chief Information Officers (CIOs) a memorandum titled, *Security Authorization of Information Systems in Cloud Computing Environments*. According to the memorandum, the Federal Government's adoption and use of information systems operated by cloud service providers depends on security, interoperability, portability, reliability, and resiliency. OMB also helped develop the Federal Risk and Authorization Management Program (FedRAMP) to support agencies in cloud computing adoption. FedRAMP is responsible for providing standardized security requirements for the authorization and ongoing cybersecurity of cloud services and a repository of authorization packages for cloud services that can be leveraged Government-wide. OMB's December 2011 guidance states that each agency shall use FedRAMP when conducting risk assessments and security authorizations, and when granting authorizations to operate for cloud services.

Over the years, OMB, NIST, and other Federal entities issued additional policies and guidance in support of cloud adoption and cloud security. Such policies and guidance generally state that agencies are accountable for the security and privacy of data held by a cloud provider on the agency's behalf.

SEC Roles and Responsibilities. Organizations within the U.S. Securities and Exchange Commission (SEC or agency) that play key roles in the agency's strategic and secure adoption of cloud computing include the Office of Information Technology's (OIT) Strategy and Innovation and Information Security organizations, as well as the agency's Office of Acquisitions (OA). Strategy and Innovation is responsible for ensuring that new IT services, including cloud services, adhere to the SEC's reference architecture and IT strategic plan, while Information Security provides engineering expertise to help identify strategies for developing and deploying technology in a secure manner. OA supports all aspects of procurement and contract administration at the SEC, including cloud computing contracts.

The SEC also established a Cloud Governance Committee in July 2016 to serve as an advisory body in response to proposed cloud strategies and policies, and to provide high-level strategic direction and governance for the SEC's cloud program. According to the committee's charter, specific duties include:

- providing input to and advising and consenting on OIT's development of the SEC's cloud strategy, cloud migration plan, cloud governance principles, and cloud-related policies and procedures; and

- prioritizing and deciding on the SEC's cloud pilot efforts.

However, after establishing its charter, the committee—composed of senior officers from the divisions of Corporation Finance, Economic and Risk Analysis, Enforcement, Investment Management, and Trading and Markets; and the offices of Compliance

Inspections and Examinations, General Counsel, Information Technology, and Information Security—almost immediately went on hiatus. This generally coincided with the Cloud Governance Committee Chair leaving the SEC.

During our review, OIT officials acknowledged a cloud coordination gap and, on June 9, 2019, appointed a Cloud Program Lead to take inventory of the program and to further develop the agency's cloud strategy. According to the Chief Strategy and Innovation Officer, one of the Cloud Program Lead's first tasks will be to reestablish the SEC's Cloud Governance Committee.

SEC Cloud Strategy and Goals. On September 26, 2016, the SEC awarded a contract for cloud strategy development, concept of operations development, cloud migration planning, and cloud data analytics and data processing support.[5] In March 2017, the agency extended the contract's period of performance from 6 months to 9 months, and changed the deliverables to cloud strategy development, concept of operations development, workload assessment framework, Joint Integrated Project Team support, and 8 weeks of Amazon Web Services support services. Two deliverables the SEC received in 2017 from the contract were (1) an (b) (7)(E) (b) (7)(E) (b) (7)(E), and (2) a (b) (7)(E) (b) (7)(E). According to the (b) (7)(E)

(b) (7)(E)

Later that same year, the SEC established the following cloud-related goals in its (b) (7)(E):

- Within 12 - 18 months: Launch (b) (7)(E) cloud pilots.
- Within 18 - 36 months: Migrate (b) (7)(E) to the cloud.[6]

[5] The SEC awarded contract number SECHQ116C0127 to Technical Services Corporation with an initial period of performance of 6 months and a total award amount of $1,051,586.00. A contract modification dated March 3, 2017, extended the period of performance by 3 months and revised the statement of work as described above but did not change the total award amount.

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

- Within 36 months - 5 years: Broad scaling of cloud capabilities.

According to the Chief Strategy and Innovation Officer, in 2018, the SEC launched two cloud pilots—the Data Science Workstation, and (b) (7)(E) —to inform the agency's cloud strategy and to provide high computing power on demand, and an enterprise (b) (7)(E) , respectively. The target date for these efforts to migrate from pilots to enterprise programs is November 2019.

SEC Cloud-Based Systems. According to OIT officials and the SEC's enterprise Governance, Risk, and Compliance (eGRC) system, as of March 20, 2019, the SEC had (b) (7)(E) cloud-based systems operated by 7 cloud service providers. As the following table shows, OIT categorized (b) (7)(E) of these (b) (7)(E) systems as (b) (7)(E) and the remaining (b) (7)(E) as (b) (7)(E) under Federal Information Processing Standards Publication (FIPS PUB) 199.[7] In addition, OIT classified (b) (7)(E) of the (b) (7)(E) systems as (b) (7)(E) applications and the remaining (b) (7)(E) as (b) (7)(E) applications.[8] OIT's inventory of systems also identified (b) (7)(E) (b) (7)(E) ; however, none of those systems were cloud-based.[9]

[7] FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004), establishes security categories for information systems (for example, high, moderate, or low) based on assessments of the potential impact that a loss of confidentiality, integrity, or availability of the information or system would have on organizational operations, organizational assets, or individuals.

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

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

Table 1. The SEC's Cloud-Based Systems (as of March 20, 2019)

(b) (7)(E)

Source: Office of Inspector General (OIG)-generated based on system documents and eGRC system reports as of March 20, 2019.

Objectives

Our overall objective was to determine whether the SEC effectively managed the planning, implementation, and security of its cloud computing services. Specifically, we (1) assessed the SEC's strategy for migrating IT services and applications to the cloud, and (2) determined whether key security measures were in place to adequately protect SEC systems that use cloud computing services.

To address our objectives, among other work performed, we interviewed OIT and OA officials and personnel. We also reviewed applicable Federal laws and guidance, relevant SEC policies and procedures, and OIT's and OA's fiscal year 2018 risk control matrices and management assurance statements. In addition, we clarified cloud program requirements with officials from OMB and FedRAMP, and assessed the SEC's strategic cloud implementation efforts since the time OMB launched the *Federal Cloud Computing Strategy* in February 2011. Specifically, we assessed the SEC's enterprise

cloud strategy and the security controls and processes associated with each of the agency's (b) (7)(E) cloud-based systems in operation as of March 20, 2019.

Appendix I includes additional information about our scope and methodology, including our review of relevant internal controls and prior coverage. Appendix II provides additional information on the cloud-based systems we reviewed, including the system names, cloud service providers, and system descriptions. Appendix III provides examples of cloud-specific controls and enhancements that we determined were missing from the system security plans (SSP) for most of the SEC's (b) (7)(E) cloud-based systems we assessed, as further discussed in Finding 2.

Results

Finding 1. The SEC Used an Ad Hoc Approach To Implementing Cloud Computing

> OMB directed Federal agencies to shift to a "Cloud First" policy, requiring that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. According to the SEC's fiscal year 2020 budget justification and performance plan, "Building foundational capabilities in the SEC's cloud environment will unlock future opportunities for cost savings, application consolidation, and security enhancements."[10] However, the SEC did not fully implement its cloud strategy; follow a clear, robust strategic plan to evaluate and prioritize IT services and applications for migration to the cloud; or effectively track related goals. Instead, the agency used an "ad hoc" or "as-needed" approach to implementing cloud computing. This occurred because the SEC did not coordinate or collaborate on cloud strategies at an enterprise level. As a result, the SEC has not yet fully realized the potential performance and economic benefits attributed to cloud computing services.

Federal Guidance and Best Practices for Implementing Cloud Computing. To accelerate the pace at which the Government will realize the value of cloud computing, Federal guidance emphasizes the need for agencies to evaluate safe, secure cloud computing options before making any new investments. For example, OMB's 2011 *Federal Cloud Computing Strategy* states:

> Successful organizations carefully consider their broad IT portfolios and create roadmaps for cloud deployment and migration. These roadmaps prioritize services that have high expected value and high readiness to maximize benefits received and minimize delivery risk. Defining exactly which cloud services an organization intends to provide or consume is a fundamental initiation phase activity in developing an agency roadmap.

Also, according to the CIO and Chief Acquisition Officers councils' joint publication, *Creating Effective Cloud Computing Contracts for the Federal Government* (February 24, 2012), proactive planning with all necessary agency stakeholders (for example, CIOs, general counsels, privacy officers, records managers, e-discovery counsel, Freedom of Information Act officers, and procurement staff) is essential when evaluating and procuring cloud computing services. In addition, the General Services

[10] U.S. Securities and Exchange Commission, *Fiscal Year 2020 Congressional Budget Justification and Annual Performance Plan; Fiscal Year 2018 Annual Performance Report*; March 18, 2019.

Administration's *Best Business Practices for [U.S. Government] Cloud Adoption* (September 2016) states:

> Considerations for planning a migration to the cloud include: (1) knowing your current architecture and developing a technology program/project schedule; (2) developing a plan to migrate products and/or services to the cloud to include capacity management, performance metrics, and historical contractual costs; and (3) service level agreements.[11]

During our audit, OMB finalized its "Cloud Smart" strategy to accelerate agency adoption of cloud-based solutions, which states:

> Additionally, all Federal agencies will rationalize their application portfolios to drive Federal cloud adoption. The rationalization process will involve reducing an application portfolio by (1) assessing the need for and usage of applications; and (2) discarding obsolete, redundant, or overly resource-intensive applications. Decreased application management responsibilities will free agencies to focus on improving service delivery by optimizing their remaining applications.[12]

The SEC Did Not Fully Implement Its Cloud Strategy or Effectively Track Related Goals. Consistent with Federal guidance, the SEC developed (1) an (b) (7)(E) (b) (7)(E), which defined the goals and objectives of the agency's cloud program, and (2) a (b) (7)(E), which established cloud-related goals. However, at the time of our audit, the SEC had not fully implemented its cloud strategy. According to the SEC's infrastructure support services contract, as well as the Chief Strategy and Innovation Officer, the SEC used an "ad hoc" or "as-needed" approach to its cloud adoption.[13] Specifically, the SEC migrated individual systems based on each system's business and technological needs or opportunities rather than a clear and robust strategic plan for IT services and applications enterprise-wide. Furthermore, the agency did not follow a clear, robust strategic plan to evaluate its inventory of systems to determine their respective cloud compatibility, and had not prioritized systems to be migrated.[14] Finally, the SEC did not track its progress toward implementing its cloud-related goals over the last 2 years.

---

[11] General Services Administration, *Best Business Practices for [U.S. Government] Cloud Adoption*; September 2016.

[12] Office of Management and Budget, *Federal Cloud Computing Strategy*; June 24, 2019.

[13] SEC contract number SECHQ116C0032 for infrastructure support services states, "The SEC has utilized an 'ad hoc,' 'as-needed' technique for its Cloud adoption that has delivered significant value and results by using both public and in-house infrastructures."

[14] "Cloud compatibility" refers to whether a system is cloud ready, cloud capable, could benefit from being a cloud system, or could never be moved to the cloud.

The SEC Lacked Coordination on the Strategic Direction and Governance for Its Cloud Program. The conditions we observed occurred because the SEC did not coordinate or collaborate on cloud strategies at an enterprise level. For example, key stakeholders; including the CIO, as well as OIT and OA officials, did not work together to review the SEC's IT portfolio and employ best practices for adopting cloud computing services. As noted in the Background section of this report, OIT officials acknowledged a cloud coordination gap and, on June 9, 2019, appointed a Cloud Program Lead to take inventory of the program and to further develop the agency's strategy. According to the Chief Strategy and Innovation Officer, one of the Cloud Program Lead's first tasks will be to reestablish the SEC's Cloud Governance Committee.

Implementing Cloud Computing Strategically Could Result in Cost Savings, Ease in Scalability, and Procurement Efficiencies. Because the SEC did not coordinate or collaborate on cloud strategies at an enterprise level, the agency has not fully realized the potential performance and economic benefits attributed to cloud-based services. For example, the SEC had early success leveraging cloud technologies for the *SEC.gov* website. According to the (b) (7)(E) , this migration resulted in:

(b) (7)(E)

However, the SEC has yet to realize benefits comparable to those touted by OMB in 2010[15] or observed by GAO in 2019.[16] Moreover, because the SEC did not coordinate or collaborate on cloud strategies at an enterprise level, the SEC has yet to migrate any (b) (7)(E) to the cloud (a goal established in its (b) (7)(E)), which may have yielded performance and economic benefits for the agency.

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

To improve the SEC's management, planning, and implementation of cloud strategies, we recommend that the Office of Information Technology:

[15] Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management*; December 9, 2010.

[16] U.S. Government Accountability Office, *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked* (GAO-19-58; April 4, 2019).

Recommendation 1: Reestablish a cloud computing governance committee composed of key stakeholders with authority to coordinate and oversee agency-wide acquisition of cloud computing services and migration of SEC systems to the cloud.

Management's Response. Management concurred with the recommendation. The agency is establishing a multi-tiered governance structure for the cloud program which will include a Cloud Steering Committee to ensure appropriate coordination with other SEC functions, offices, and divisions that have a role in cloud-related matters. Management's complete response is reprinted in Appendix IV.

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

Recommendation 2: Develop a roadmap and implementation plan for cloud migration that provides for evaluating the agency's information technology portfolio; prioritizing systems and services for migration to the cloud, as appropriate, based on potential benefits and risks; and tracking of cloud-related goals.

Management's Response. Management concurred with the recommendation. The Office of Information Technology will (a) review current policies, procedures, roadmaps, and practices and make modifications as appropriate; (b) determine how it can further implement the cloud strategy by prioritizing systems and services for cloud migration based on potential benefits and risks; and (c) track cloud-related goals. Management's complete response is reprinted in Appendix IV.

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

Finding 2. Processes for Protecting the SEC's Cloud-Based Systems Need Improvement

According to NIST, "Organizations need to review, revise, and develop policy in the context of the global business and technical model enabled by cloud computing and other enabling technologies."[17] Furthermore, the Federal Information Security Modernization Act of 2014[18] (FISMA) requires Federal agencies to protect their information and information systems, including cloud-based or other systems used or operated by a contractor or other organization on the agencies' behalf. Although OIT developed an IT security program, an (b) (7)(E) (b) (7)(E), and other supporting security policies and procedures governing the SEC's systems, processes for protecting the SEC's cloud-based systems need improvement. Specifically, we found that:

- the SEC's SSPs for its (b) (7)(E) cloud-based systems in operation as of March 20, 2019, were missing cloud-specific security controls and enhancements; and
- security assessment reports (SARs) for the (b) (7)(E) systems were incomplete.

These conditions occurred because OIT had not developed policies and procedures specific to cloud system security, or adequate processes to ensure compliance with FedRAMP baseline controls and enhancements for which the SEC is responsible. As a result, the SEC's processes did not adequately ensure compliance, assess risk, identify issues, or mitigate vulnerabilities specific to cloud-based systems.

The SEC's SSPs for Its Cloud-Based Systems Were Missing Cloud-Specific Security Controls and Enhancements. The SEC's SSPs—which establish controls planned, in place, or inherited to meet information system security requirements—for the (b) (7)(E) cloud-based systems we reviewed were missing up to (b) (7)(E) percent of FedRAMP baseline controls and enhancements across (b) (7)(E) of the 17 NIST system-level control families. FedRAMP developed baselines for cloud systems above the standard NIST guidelines and requirements for low, moderate, and high systems to address the unique risks of cloud computing environments, such as multi-tenancy, visibility, control/responsibility, shared resource pooling, and trust. For example, NIST identifies 261 controls and enhancements in its moderate baseline, to which FedRAMP adds an additional 65 controls and enhancements for cloud-based systems. According to FedRAMP's *Security Controls Baseline*, "Federal Agencies and [cloud service

[17] NIST SP 500-293, *U.S. Government Cloud Computing Technology Roadmap Volume I: High-Priority Requirements to Further [U.S. Government] Agency Cloud Computing Adoption;* October 2014.

[18] P.L. 113-283, 128 Stat 3073; December 18, 2014.

providers] must implement these security controls, enhancements, parameters, and requirements within a cloud computing environment to satisfy FedRAMP requirements." Similarly, (b) (7)(E) which OA required to be included in all new and existing solicitations, contracts, and agreements involving cloud-based services, states, (b) (7)(E) Although OIT is developing a revised cloud SSP template that will help ensure missing cloud-specific (or FedRAMP) controls are included in cloud-based system SSPs in the future, the SEC's cloud-based SSPs were missing such controls at the time of our audit. Examples of missing controls and enhancements are included in Appendix III.

SARs for the SEC's Cloud-Based Systems Were Incomplete. SARs—which officials use to make risk-based decisions in the security authorization process—for the (b) (7)(E) cloud-based systems we reviewed were incomplete. Specifically, most SARs (1) did not include cloud service provider vulnerability information, (2) did not include information about the scope of FedRAMP information reviewed, (3) did not match corresponding SSPs, and (4) referenced outdated Federal policies. We describe each of these issues further below.

- *SARs Did Not Include Cloud Service Provider Vulnerability Information*. According to SEC Information Security officials, when developing SARs for the agency's cloud-based systems, personnel reviewed the FedRAMP-certified authorization packages to determine the status of security controls inherited from cloud service providers. However, Information Security officials acknowledged that the SARs did not include cloud service provider vulnerability information related to controls inherited from the FedRAMP authorization packages. During our audit, OIT began reporting in SARs summary cloud service provider plans of action and milestones (POA&M).[19] For example, in the SAR of one cloud system recently reauthorized, OIT reported that the cloud service provider had (b) (7)(E) open POA&Ms, of which (b) (7)(E) were overdue for mitigation.[20]

- *SARs Did Not Include Information About the Scope of FedRAMP Information Reviewed*. Although SARs for the SEC's cloud-based systems typically included a list of the documents used to determine the scope and perform the assessment, the SARs did not consistently list the FedRAMP cloud service provider authorization package information reviewed or the date of the information reviewed. OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016) (OMB Circular No. A-130), states that, when

[19] POA&Ms detail the findings from SARs that require mitigation.

[20] (b) (7)(E)

an agency leverages the authorization package generated by another party, the leveraging agency reviews the authorization package as a basis for determining risk. In addition, NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations*, Revision 2 (December 2018), states, "When reviewing the [cloud service provider's authorization package], the customer organization considers various risk factors such as the time elapsed since the authorization results were produced…."

- *SARs Did Not Match Corresponding SSPs*. SARs for the SEC's cloud-based systems typically included an appendix listing the controls that the SEC's Security Assessment and Authorization Team did not test because the controls were inherited from another system or control set. However, the inherited control lists in the SARs did not always match the inherited control lists in the corresponding SSPs. For example, the SSP for one cloud system we reviewed listed a total of (b) (7) (E) fully inherited controls/enhancements, whereas the system's SAR listed more than (b) (7)(E). Furthermore, the SEC and cloud service providers share responsibility for at least (b) (7) (E) of the controls included in the standard SAR list of controls that were not tested. As a result, authorizing officials did not always have a complete assessment of the effectiveness of controls applicable to the SEC's cloud systems.

- *SARs Referenced Outdated Federal Policies*. (b) (7)(E) of the (b) (7)(E) SARs for the SEC's cloud-based systems referenced the November 2000 version of OMB Circular No. A-130 instead of the revised July 2016 version. These same (b) (7)(E) SARs also referenced the July 2002 version of NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, which NIST updated in September 2012. The remaining (b) (7)(E) cloud system SARs either did not reference these policies or referenced the latest versions.

The conditions we observed occurred because OIT had not developed policies and procedures specific to cloud system security, or adequate processes to ensure compliance with FedRAMP baseline controls and enhancements for which the agency is responsible. Without policies and procedures addressing the unique risks of cloud computing environments, the SEC's processes did not adequately ensure compliance, assess risk, identify issues, or mitigate vulnerabilities specific to cloud-based systems.

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

To improve the security of the SEC's cloud-based systems, we recommend that the Office of Information Technology:

Recommendation 3: Develop policies and procedures to ensure the following for all new and existing cloud computing services:

(a) Applicable cloud system security controls and enhancements are included in the respective SEC cloud-based system security plan.

(b) Applicable cloud system security controls and enhancements are assessed and supported by sufficient evidence in the respective SEC cloud-based system security assessment report.

(c) The SEC authorizing official is provided with complete and appropriate information necessary to make risk-based decisions on whether to authorize the agency's cloud systems to operate.

Management's Response. Management concurred with the recommendation. The Office of Information Technology will complete its initiatives to implement policies and procedures for all new and existing cloud computing services. The Office of Information Technology will also (a) update cloud-based system security plans, (b) update cloud-based system security assessment reports, and (c) ensure SEC authorizing officials are provided complete and appropriate information necessary to make risk-based decisions on whether to authorize the agency's cloud systems to operate. Management's complete response is reprinted in Appendix IV.

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

Other Matters of Interest

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

Conflicting Security Categories. According to NIST SP 800-53, organizations first determine the security category of their information systems in accordance with FIPS PUB 199 and then apply the appropriately tailored set of baseline controls.[21] OIT identifies each system's FIPS PUB 199 category in the agency's eGRC system and in various system security documents, including SSPs, SARs, and authorization to operate letters. We reviewed this information and determined that OIT reported conflicting FIPS PUB 199 categories for at least (b) (7) (E) of the SEC's (b) (7)(E) cloud-based systems, as shown in the following table.

Table 2. Inconsistent Reporting of FIPS PUB 199 Categories

(b) (7)(E)

Source: OIG-generated based on system documents and OIT's eGRC system.

The Branch Chief of OIT's Security Assessment and Compliance Branch stated this can occur if OIT used the moderate SSP template before the system was categorized and then subsequently OIT categorized the system as low impact. We encourage management to validate the security categories for the SEC's cloud-based systems, and, as necessary, update the eGRC system and system security documents.

Underreporting of Cloud Services. In the SEC's 2nd Quarter 2019 CIO FISMA Report transmitted to OMB and the Department of Homeland Security, the Acting CIO underreported the number of cloud service providers the SEC uses. The Acting CIO reported that the SEC uses six cloud service providers although, as of the date of that report, the agency used seven. The Chief Information Security Officer stated that OIT plans to review the applicable guidance from OMB and update the information in the

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

next reporting period. We reviewed a draft version of the SEC's 4th Quarter 2019 CIO FISMA Report, which lists eight cloud service providers.

Improvements Needed in Cloud System Incident Response Processes. (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

To help ensure the SEC is timely alerted to incidents involving the agency's cloud-based systems, we encourage management to (1) properly identify its cloud-based systems for (b) (7)(E); (2) validate that (b) (7)(E)

(b) (7)(E) is successful before closing related POA&Ms; and (3) update its cloud service contracts to include accurate incident reporting information.

SEC Cloud Service Contracts Did Not Consistently Include Security Requirements. Since at least July 2017, OA has required contracting personnel to insert (b) (7)(E) in all new and existing solicitations, contracts, and agreements involving cloud-based services. (b) (7)(E) establishes responsibilities for meeting FedRAMP IT systems security requirements, including contractor responsibilities for:

1. complying with privacy and security safeguards such as sensitive information storage, protection of information, and disclosure of information; and

2. supporting actions to assess and authorize systems and continuously monitor operational controls to determine if security controls remain effective over time.

However, as we have previously reported, OIT and OA have not consistently implemented a process to ensure that the SEC's IT contracts, including cloud service contracts, contain appropriate security clauses.[22] During this audit, we determined that OIT and OA did not include (b) (7)(E) in contracts for (b) (7)(E) of the (b) (7)(E) cloud-based systems we reviewed (or (b) (7)(E) percent). As a result, the SEC limits its ability to ensure the security of its cloud-based systems and may lack assurance that contractors are adequately protecting sensitive, non-public SEC information and complying with requirements applicable to Federal systems.

In addition, contracts for (b) (7)(E) of the (b) (7)(E) cloud-based systems we reviewed generally required that SEC data remain locally within the United States and not be off-shored to a foreign nation state. At the time of our review, contracts for the remaining (b) (7)(E) cloud-based systems—including (b) (7)(E) cloud-based systems the SEC classified as (b) (7)(E)—did not address data jurisdiction. During our audit, on June 18, 2019, OA (in consultation with OIT and the SEC's Office of General Counsel) revised (b) (7)(E) (b) (7)(E) to establish data jurisdiction requirements, among other things. The June 2019 version of the (b) (7)(E) states, (b) (7)(E) This and other revisions to (b) (7)(E) further exemplify the need to ensure that contracting personnel insert the (b) (7)(E) in all new and existing solicitations, contracts, and agreements involving cloud-based services.

[22] 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 30, 2018), and *Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 552; December 17, 2018).

In OIG Report No. 546 (Recommendation 7), we recommended that OIT:

> Improve the agency's acquisition of information systems, system components, and information system services by coordinating with OA to (a) identify, review, and modify as necessary the agency's existing information technology contracts to ensure the contracts include specific contracting language, such as information security and privacy requirements, material disclosures, Federal Acquisition Regulation clauses, and clauses on protection, detection, and reporting of information; and (b) define and implement a process to ensure that future acquisitions of information technology services and products include such provisions.

As of the date of this report, the recommendation remains open. Implementing Recommendation 7 from OIG Report No. 546 should address the matter regarding the SEC's cloud service contracts; therefore, we are not making an additional recommendation at this time and we encourage management to fully implement the previously agreed-to corrective action.

Appendix I. Scope and Methodology

We conducted this performance audit from February through November 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope and Objective. Our overall objective was to determine whether the SEC effectively managed the planning, implementation, and security of its cloud computing services. Specifically, we (1) assessed the SEC's strategy for migrating IT services and applications to the cloud, and (2) determined whether key security measures were in place to adequately protect SEC systems that use cloud computing services.

The audit covered the SEC's strategic cloud implementation efforts since the time OMB launched the *Federal Cloud Computing Strategy* in February 2011. In addition, we assessed the security controls and processes associated with each of the SEC's (b) (7)(E) cloud-based systems in operation as of March 20, 2019. We performed fieldwork at the SEC's Headquarters in Washington, DC.

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

- reviewed applicable Federal laws and guidance and relevant SEC policies and procedures;
- clarified cloud program critical requirements with officials from OMB and FedRAMP; and
- interviewed key OIT and OA officials and personnel.

We also obtained and reviewed information about the SEC's enterprise cloud strategy, including documents accessed from the SEC's (b) (7)(E) (b) (7)(E) sites and received from OIT officials. In addition, we assessed the security controls and processes associated with the (b) (7)(E) cloud-based systems we reviewed, including the systems' security packages and authorization to operate letters. Finally, we assessed (b) (7)(E) contracts and (b) (7)(E) contract modifications covering the cloud-based systems we reviewed, as well as the SEC's cloud strategy contract files.

Internal Controls. To assess internal controls relative to our objectives, we reviewed OIT's and OA's management assurance statements and risk and control matrixes for fiscal year 2018. However, consistent with our audit objectives, we did not assess OIT's and OA's overall management control structure. Instead, we reviewed the SEC's controls specific to cloud-based system security. To understand OIT's management

controls pertaining to its policies, procedures, and methods of operation, we relied on information requested from and supplied by OIT staff and information from interviews with OIT personnel. We found that the SEC generally complied with applicable Federal and agency policies and procedures, except as identified in this report. Our recommendations, if implemented, should correct the weaknesses we identified.

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

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

We used OIT's eGRC system to obtain documents and reports about the SEC's cloud-based systems and inventory. We also used OA's electronic filing system to obtain contract documents. We did not perform extensive testing on the tool or the system because such testing was not part of our objectives. However, to assess the reliability of the computer-processed data used to support our conclusions, we compared and validated the data with testimonial evidence from OIT and OA personnel. Based on our assessments, we determined that the computer-processed data we reviewed was sufficiently reliable in the context of our objectives.

Prior Coverage. Between 2014 and 2019, the SEC OIG and GAO issued the following reports of particular relevance to this audit.

SEC OIG:

- *Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014* (Report No. 552, December 17, 2018).
- *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2017* (Report No. 546, March 30, 2018).

GAO:

- *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked* (GAO-19-58; April 4, 2019).

- *Information Security: Agencies Need to Improve Implementation of Federal Approach to Security Systems and Protecting against Intrusions* (GAO-19-105; December 18, 2018).

- *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance* (GAO-16-325; April 7, 2016).

- *Cloud Computing: Additional Opportunities and Savings Need to Be Pursued* (GAO-14-753; September 25, 2014).

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

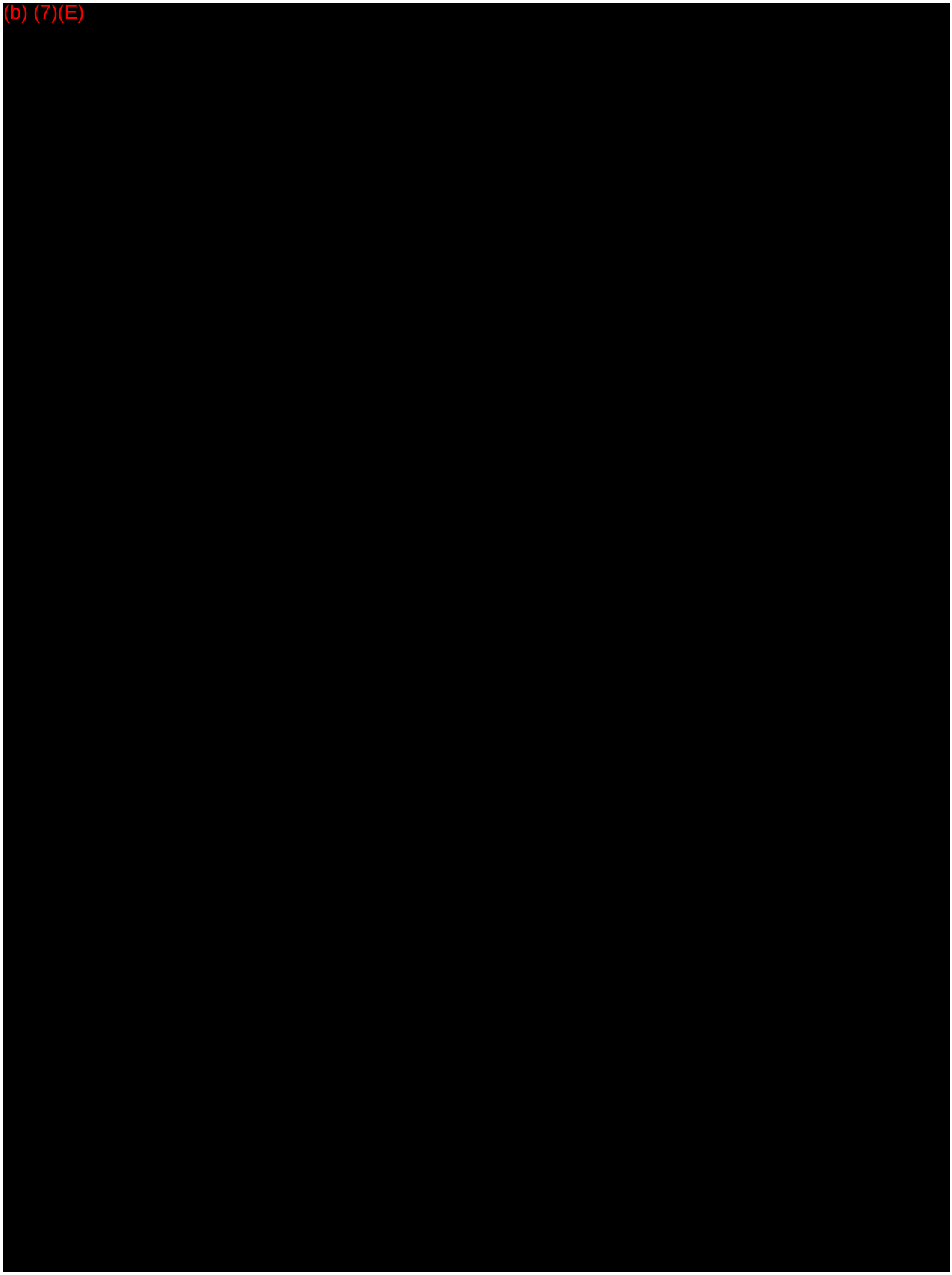
Appendix II. List of Cloud-Based Systems, Cloud Service Providers, and System Descriptions

The table below provides additional information on the cloud-based systems we reviewed, including the system names, cloud service providers, and system descriptions.

Table 3. Additional Information on the SEC's Cloud-Based Systems (as of March 20, 2019)

(b) (7)(E)

(b) (7)(E)



(b) (7)(E)

Source: OIG-generated based on system documents and eGRC system reports.

Appendix III. Examples of Missing Cloud-Specific Controls and Enhancements

The following tables provide examples of the cloud-specific (or FedRAMP) baseline controls and enhancements that were missing from SSPs for most of the SEC's (b) (7)(E) cloud-based systems we reviewed.

Table 4. Examples of Missing Controls and Enhancements: (b) (7)(E)

(b) (7)(E)

Source: OIG-generated based on FedRAMP baseline controls and NIST SP 800-53.

Table 5. Examples of Missing Controls and Enhancements: (b) (7)(E)

Source: OIG-generated based on FedRAMP baseline controls and NIST SP 800-53.

Appendix IV. Management Comments

MEMORANDUM

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

From: Kenneth Johnson, Chief Operating Officer

KENNETH JOHNSON Digitally signed by KENNETH JOHNSON Date: 2019.10.31 17:47:16 -04'00'

Date: October 31, 2019

Subject: Management Response to Draft Report No. 556, "The SEC Can More Strategically and Securely Plan, Manage, and Implement Cloud Computing Services"

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) recommendations related to its evaluation of the Securities and Exchange Commission's (SEC) management, implementation, and security of its cloud computing services (Report No. 556). The report evaluates the SEC's strategic cloud implementation efforts in accordance with the Office of Management and Budget (OMB) *Cloud First* policy,[1] *Federal Cloud Computing Strategy*,[2] and *Security Authorization of Information Systems in Cloud Computing Environments*.[3]

In its report, the OIG issued three recommendations relating to the SEC's adoption of cloud services, with which we concur. During the audit, OMB issued its 2019 Federal Cloud Computing Strategy revision.[4] This Cloud Smart policy outlines a strategy for agencies to adopt cloud solutions that streamline transformation and embrace modern capabilities. Consistent with OMB guidance, the SEC views the potential adoption of cloud services as key to accelerating the modernization of certain technologies and practices while facilitating new capabilities (and expansion of existing capabilities) in support of the agency's mission. Further, the SEC will continue to leverage the Federal Risk and Authorization Management Program (FedRAMP) to provide a cost-effective, risk-based approach for the adoption and use of cloud services, and to avoid duplicative efforts, inconsistencies, and cost inefficiencies associated with security authorization processes.

Indeed, we believe the OIG's recommendations illustrate the challenges that many other agencies are facing as they leverage new cloud capabilities. Notably, the recommendations provided in Report No. 556 are consistent with those from other Inspectors General and the

[1] OMB, *25 Point Implementation Plan to Reform Federal Information Technology Management (Cloud First)*, December 9, 2010, https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf.
[2] OMB, *Federal Cloud Computing Strategy (Cloud Smart)*, June 24, 2019, https://cloud.cio.gov/strategy.
[3] OMB Memorandum, *Security Authorization of Information Systems in Cloud Computing Environments*, December 8, 2011, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf.
[4] OMB, 2019 Federal Cloud Computing Strategy, June 24, 2018, https://cloud.cio.gov.

1

Government Accountability Office (GAO). In 2019, GAO reviewed 16 agencies' IT budgets and analyzed their use of cloud services, associated spending and savings data, and guidance for assessing investments for these services.[5] GAO made one recommendation to OMB on cloud savings reporting and 34 recommendations to the 16 agencies on cloud assessments and savings.[6] GAO determined the agencies lacked guidance for assessing IT investments and had insufficient mechanisms to track and report the savings associated with cloud initiatives. Additionally, in Fiscal Year (FY) 2019, the Department of the Treasury and Consumer Financial Protection Bureau Inspectors General[7][8] identified opportunities to improve the security assessment process around cloud systems. Further, in FY 2019, the U.S. General Services Administration (GSA) OIG performed an audit of FedRAMP's goals and objectives and found that the FedRAMP has not established an adequate structure comprising its mission, goals, and objectives for assisting the federal government with the adoption of secure cloud services.[9]

While more remains to be done to refine the SEC's cloud strategy, stakeholders across the SEC, led by the Office of Information Technology (OIT), have worked to coordinate efforts across business and technical areas. Additionally, our security assessment and authorization (SA&A) processes continue to mature. Consistent with the report's recommendations, OIT has improved how it incorporates the results of FedRAMP security reviews into agency security documentation and how it informs Authorizing Officials (AO) of residual risks.

Thank you for the professionalism and courtesies that you and all of the OIG personnel demonstrated throughout this audit. We look forward to working with your office to address the areas noted in your report.

A response to each of the recommendations is provided below.

Recommendation 1: Reestablish a cloud computing governance committee composed of key stakeholders with authority to coordinate and oversee agency-wide acquisition of cloud computing services and migration of SEC systems to the cloud.

Response: We concur. SEC is establishing a multi-tiered governance structure for the cloud program which will include a Cloud Steering Committee (CSC) to ensure appropriate coordination with other SEC functions, offices and divisions that have a role in cloud-related matters. The CSC will be responsible for the SEC Cloud Strategy and will work in coordination

[5] GAO, *Cloud Computing- Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked*, April 2019, https://www.gao.gov/assets/700/698236.pdf.
[6] *Id.*
[7] OIG, *Information Technology: Department of Treasury Federal Information Security Modernization Act FY 2018 Performance Audit*, October 31, 2018, https://www.oversight.gov/sites/default/files/oig-reports/OIG-19-007.pdf.
[8] OIG, *The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP*, July 17, 2019, https://www.oversight.gov/sites/default/files/oig-reports/bureau-fedramp-life-cycle-processes-jul2019_0.pdf.
[9] OIG, *Audit of the Federal Risk and Authorization Management Program*, PMO's Goals and Objectives, March 21, 2019, https://www.oversight.gov/sites/default/files/oig-reports/A170023_1.pdf.

with the Office of Acquisitions to ensure acquisitions adhere to the Service Delivery Framework (SDF) and governance processes.

Recommendation 2: Develop a roadmap and implementation plan for cloud migration that provides for evaluating the agency's information technology portfolio; prioritizing systems and services for migration to the cloud, as appropriate, based on potential benefits and risks; and tracking of cloud-related goals.

Response: We concur, and agree it is important to develop a roadmap and implement a plan for cloud migration. While the SEC already possesses an (b) (7)(E) and a (b) (7)(E) OIT will review current policies, procedures, roadmaps and practices and make modifications as appropriate. OIT will determine how it can further implement the cloud strategy by prioritizing systems and services for cloud migration based on potential benefits and risks, and will track cloud-related goals.

Recommendation 3: Develop policies and procedures to ensure the following for all new and existing cloud computing services: (a) Applicable cloud system security controls and enhancements are included in the respective SEC cloud-based system security plan. (b) Applicable cloud system security controls and enhancements are assessed and supported by sufficient evidence in the respective SEC cloud-based system security assessment report. (c) The SEC authorizing official is provided with complete and appropriate information necessary to make risk-based decisions on whether to authorize the agency's cloud systems to operate.

Response: We concur. Pursuant to this recommendation, OIT will complete its initiatives to implement policies and procedures for all new and existing cloud computing services. While the SEC already possesses policies and procedures for cloud computing services, OIT will (a) update cloud-based system security plans (SSP), (b) update cloud-based system security assessment reports (SARs), and (c) ensure SEC authorizing officials are provided complete and appropriate information necessary to make risk-based decisions on whether to authorize the agency's cloud systems to operate. The (b) (7)(E) and System Security Plan templates have been updated to include cloud-based security controls and are currently under management's review. For existing cloud systems, the SA&A Team has updated all SARs to include a summary of cloud risks associated with using a Cloud Service Provider (CSP). Additionally, the AO will sign new Authority to Operate (ATO) letters acknowledging the cloud risks.

cc: Charles Riddle, Acting Chief Information Officer, Office of Information Technology

Vance Cathell, Director, Office of Acquisitions

Major Contributors to the Report

Kelli Brown-Barnes, Audit Manager

Michael Burger, Lead Auditor

Douglas Carney, Auditor

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

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

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

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

Comments and Suggestions

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