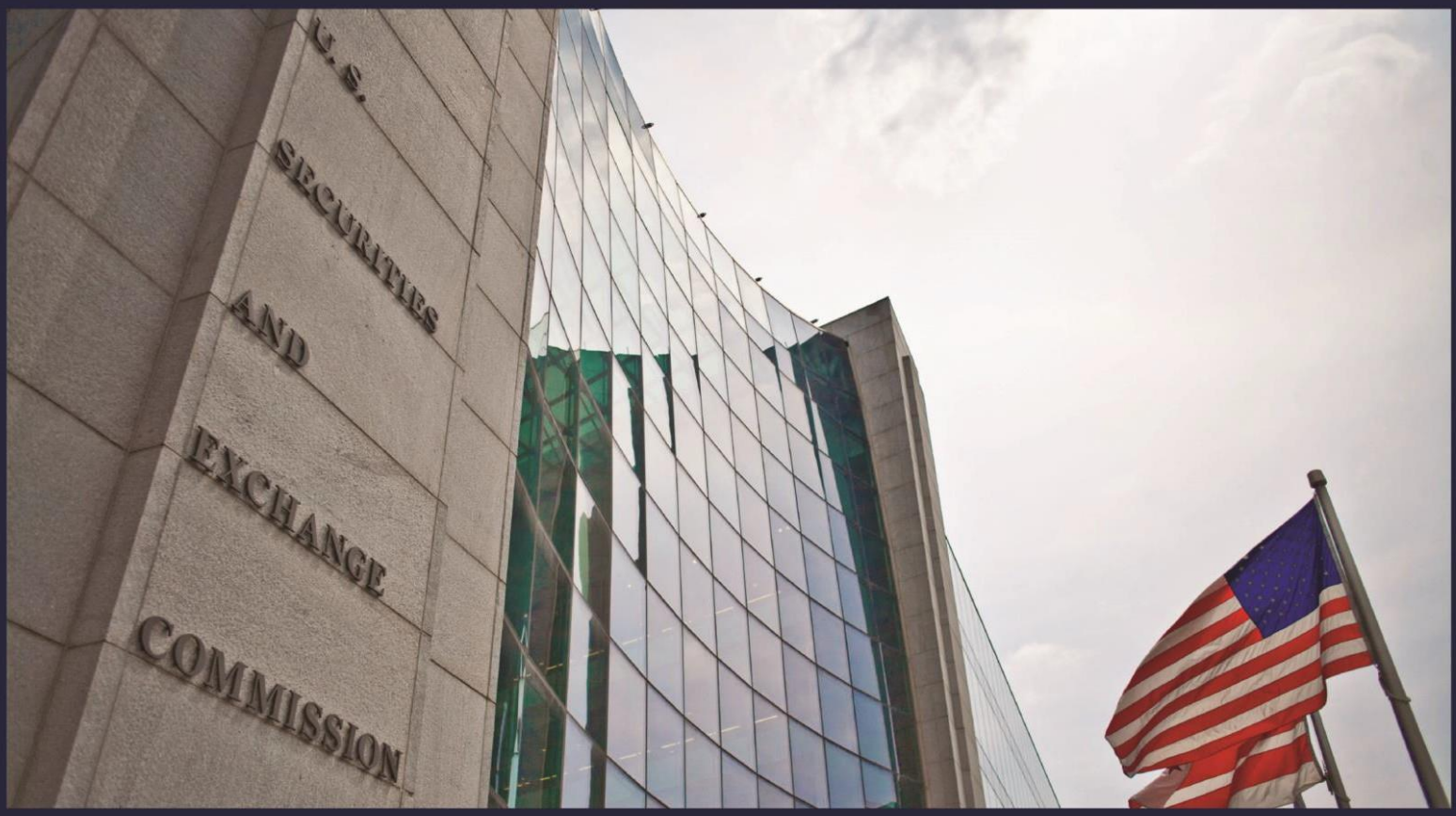
U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

# Audit of the SEC's Management of Its Data Centers




September 29, 2017

Report No. 543

**REDACTED FOR PUBLIC RELEASE**

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

OFFICE OF
INSPECTOR GENERAL

# M E M O R A N D U M

September 29, 2017

**TO:** Kenneth Johnson, Acting Chief Operating Officer

**FROM:** Carl W. Hoecker, Inspector General

**SUBJECT:** *Audit of the SEC's Management of Its Data Centers*, Report No. 543

Attached is the Office of Inspector General (OIG) final report detailing the results of our audit of the U.S. Securities and Exchange Commission's (SEC or agency) management of its data centers. The report contains ten recommendations that should help the agency develop a plan for future data center relocations and improve the SEC's data center contract management.

On September 13, 2017, we provided management with a draft of our report for review and comment. In its September 25, 2017, 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 SEC 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
Lucas Moskowitz, Chief of Staff, Office of Chairman Clayton
Sean Memon, Deputy Chief of Staff, Office of Chairman Clayton
Peter Uhlmann, Managing Executive, Office of Chairman Clayton
Michael S. Piwowar, Commissioner
Richard Grant, Counsel, Office of Commissioner Piwowar
Kara M. Stein, Commissioner
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein
Robert B. Stebbins, General Counsel
Rick A. Fleming, Investor Advocate
John J. Nester, Director, Office of Public Affairs
Bryan Wood, Director, Office of Legislative and Intergovernmental Affairs

Vance Cathell, Director, Office of Acquisitions
Pamela C. Dyson, Director/Chief Information Officer, Office of Information Technology
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

REDACTED FOR PUBLIC RELEASE

# Executive Summary

## Audit of the SEC's Management of Its Data Centers
## Report No. 543
## September 29, 2017

### Why We Did This Audit

The U.S. Securities and Exchange Commission's (SEC or agency) data centers house critical telecommunications, data, and computing resources, including the agency's (b)(7)(E) and EDGAR—the Electronic Data Gathering, Analysis, and Retrieval system—which supports the financial reporting of public companies in the United States. Between 2012 and 2013, the SEC completed actions to relocate its data centers to their present locations. The agency awarded new data center contracts to (b)(7)(E) (hereinafter D1) and (b)(7)(E) (hereinafter D2) to provide data center services. The SEC's contracts with D1 and D2 total about $16 million and $18 million, respectively, if all contract options are exercised. We conducted this audit to assess the SEC's management of its data centers, ensure the data centers have adequate physical and environmental controls, and determine whether SEC personnel properly monitored the contractors' performance.

### What We Recommended

We made ten recommendations for corrective action, including that the SEC conduct comprehensive reviews of the 2012-2013 data center relocations to identify lessons learned. We have previously reported that agency staff did not always perform contract management duties consistently and as required. Therefore, in addition to our recommendations regarding data center-related contract management, we strongly encourage the Director of the Office of Acquisitions to conduct a comprehensive review of the SEC's COR program and ensure controls are developed or strengthened to improve the SEC's contract management activities. 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 security program. We redacted (deleted) the non-public information to create this public version.

### What We Found

In 2008, the SEC paid $162,000 for a contractor-developed plan to relocate the agency's data centers. However, the SEC did not follow the plan's recommended steps or timeline to ensure the 2012-2013 data center relocations were properly executed and that the SEC's data center providers, D1 and D2, could meet the agency's needs before awarding contracts and migrating data, thereby exposing SEC data to vulnerabilities. We were unable to determine why the SEC did not follow the recommended data center relocation steps or timeline because the current officials responsible for the SEC's data centers were not aware of the relocation plan, many key officials responsible for the data center relocations no longer work at the SEC, and, as discussed further below, contract files were incomplete. However, because the agency derived little, if any, benefit from the 2008 data center relocation plan, we believe the $162,000 paid for the plan represents funds that the SEC may have wasted. Furthermore, we determined that SEC data and equipment at the D1 data center have been exposed to certain physical and environmental control vulnerabilities since the inception of the contract. These vulnerabilities have disrupted SEC operations and resulted in increased costs to the agency. Specifically, we estimate that since 2014 the SEC spent about $370,000 in questioned costs to mitigate the physical and environmental vulnerabilities at the D1 data center. Finally, based on our observations, we question whether the D1 data center meets a key contract requirement—to be a Tier III data center or greater—as defined in Telecommunications Industry Association standards.

Additionally, we determined that the SEC did not adequately manage or monitor its data center contracts. We found that Contracting Officer's Representatives (CORs) did not always validate invoices or maintain complete files. COR contract files were missing required deliverables, justifications and support for critical decisions related to the data centers, and monthly reports. Further, D1's monthly power consumption reports were unusable and the SEC did not timely or adequately address known vulnerabilities at the D1 data center, or effectively assess physical and environmental controls at either data center. For example, the agency's 2016 and 2017 data center assessments identified no findings at either location, despite (b)(7)(E) vulnerabilities at the D1 data center and a report from a contractor we hired that identified 14 physical and environmental control deficiencies at the D2 data center.

Because of inadequate contract management, the SEC paid D2 invoices containing formula errors resulting in $217,159 in overpayments (which has been refunded). We also identified about $2.8 million in unsupported costs paid to D1. If the SEC does not take corrective action to validate certain costs and if all contract options are exercised, the agency will incur additional costs of about $2.7 million in funds that could put to better use over the remaining life of D1's contract.

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

# TABLE OF CONTENTS

# ABBREVIATIONS

| | |
|---|---|
| CO | Contracting Officer |
| COR | Contracting Officer's Representative |
| EDGAR | Electronic Data Gathering, Analysis, and Retrieval System |
| (b)(7)(E) | [redacted] |
| FAR | Federal Acquisition Regulation |
| GAO | U.S. Government Accountability Office |
| (b)(7)(E) | [redacted] |
| Milligan | Milligan and Company, LLC/Samlin Consulting |
| NIST | National Institute of Standards and Technology |
| OA | Office of Acquisitions |
| OIG | Office of Inspector General |
| OIT | Office of Information Technology |
| P&E | physical and environmental |
| PDU | power distribution unit |
| POA&M | plan of action and milestones |
| SEC or agency | U.S. Securities and Exchange Commission |
| SECR | SEC Administrative Regulation |
| SP | Special Publication |
| TIA | Telecommunications Industry Association |
| UPS | uninterruptable power supply |

# Background and Objectives

## Background

A data center houses and protects computers and communications equipment that store and process data necessary to support business operations. To carry out its mission, the U.S. Securities and Exchange Commission (SEC or agency) has two data centers located in commercial facilities. The data centers house the SEC's critical telecommunications, data, and computing resources, including EDGAR—the agency's Electronic Data Gathering, Analysis, and Retrieval system—which supports the financial reporting of public companies in the United States. The SEC relies on two data center contractors: (1) (b)(7)(E) (hereinafter D1) and (2) (b)(7)(E) (hereinafter D2).[1]

Inside the D1 center data, the SEC maintains a secure cage (that is, a fenced-in area separated from other data center customers within a shared space) that houses racks of SEC equipment. The D1 data center (b)(7)(E) Inside the D2 data center, the SEC maintains modules (that is, secure pods with their own walls, physical security protocols, cooling, and power infrastructure) that house racks of SEC equipment.

The SEC's contracts with D1 and D2 total about $16 million and $18 million, respectively, if all contract options are exercised. The agency's Office of Information Technology (OIT) and its Office of Acquisitions (OA) are responsible for overseeing the SEC's data center operations and monitoring the agency's data center contracts.

According to the National Institute of Standards and Technology (NIST)[2] Special Publication (SP) 800-12, *An Introduction to Information Security,* (NIST SP 800-12)[3] physical and environmental (P&E) controls protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.

[1] The SEC awarded the D1 data center contract (contract number (b)(7)(E) ) on (b)(7)(E) . It is a firm-fixed price 1-year contract with nine option years and was last renewed on (b)(7)(E) . The SEC awarded the D2 data center contract (contract number (b)(7)(E) ) on (b)(7)(E) . It is also a firm-fixed price 1-year contract with nine option years and was last renewed on (b)(7)(E) . Neither contract includes a lease. Rather, D1 and D2 provide services only.

[2] NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems.

[3] NIST SP 800-12, Rev. 1, *An Introduction to Information Security*, June 2017. This publication introduces the information security principles that organizations may leverage to understand the information security needed for their respective systems.

NIST SP 800-12 also provides an overview of information security principles by introducing related concepts and security control families defined in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53).[4] The SEC's data center contracts state that D1 and D2 are responsible for providing all moderate controls identified in the NIST SP 800-53 P&E control family. Those controls include protection from physical threats such as fire, roof leaks, and unauthorized access, and controls over facility services such as electricity, heating, and air conditioning. Furthermore, the data center contracts provide the SEC the right to perform periodic security tests and evaluations of the P&E controls implemented by its data center contractors to ensure the controls meet applicable standards, including NIST SP 800-53.

The SEC's data center contracts also require D1 and D2 to comply with "Tier III or greater standards as defined by the Telecommunications Industry Association (TIA) Standards for Data Centers."[5] TIA specifies the minimum requirements for telecommunications infrastructure of data centers and computer rooms, and covers all aspects of a physical data center including site location, architecture, security, fire suppression, electrical, and mechanical. Moreover, TIA includes information for four tiers or ratings relating to various levels of a data center's availability and security.[6] A Tier IV data center, for example, has higher availability and security than a Tier I data center. (b)(7)(E) [redacted] Table 1 on the following page provides a high-level description of some of the elements from each tier level.

[4] NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013. This publication provides a catalog of security and privacy controls for Federal information systems and organizations and a process for selecting controls to protect organizational operations, organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors.

[5] In August 2012, TIA-942-A, *Telecommunications Infrastructure Standard for Data Centers,* superseded TIA-942-2. The contents of TIA-942-2 were incorporated into TIA-942-A.

[6] The term "tier" was used in the TIA-942 standard until March 2014, at which time the term "tier" was replaced by either "rated" or "rating". Also, a data center can have a different tier rating for different portions of its infrastructure (architectural, security, mechanical, electrical, telecommunications). However, the overall rating for the data center is equal to the lowest tier rating of the components of its infrastructure.

**Table 1. Data Center Tier Levels**

| Tier Level | Description |
|---|---|
| Tier I | A data center that (1) has cabling, racks, cabinets, and pathways compliant with relevant TIA specifications; (2) has no requirements for protection against physical events, intentional or accidental, natural or man-made, which could cause the data center to fail; (3) has a single feed from a utility substation; and (4) has no redundant air conditioning units. |
| Tier II | A data center that (1) has diversely routed access provider entrances and maintenance holes with minimum 20 meter separation; (2) is not within the 50-year flood hazard area; (3) has a single feed from a utility substation; and (4) has one redundant air conditioning unit per critical area. |
| Tier III | A data center that (1) has redundant access provider services – multiple access providers, central offices, access provider right-of-ways; (2) is not within the 100-year flood hazard area and is greater than 300 feet from 50-year flood hazard area; (3) has an N+1 redundant feed; and (4) has a quantity of air conditioning units sufficient to maintain critical areas during loss of one source of electrical power. |
| Tier IV | A data center that (1) has a redundant main distribution area, a redundant intermediate distribution area (if present), and redundant horizontal cabling and pathways; (2) is greater than 300 feet from the 100-year flood hazard area; (3) has a 2N redundant feed from different utility substations or generator plant; and (4) has a quantity of air conditioning units sufficient to maintain critical areas during loss of one source of electrical power. |

Source: Office of Inspector General (OIG)-generated based on information related to TIA data center standards.

# Objectives

Our objective was to assess the SEC's management of its data centers. Specifically, we sought to determine whether:

1. SEC personnel properly monitored the contractors' performance at the agency's D1 and D2 data centers;
2. the SEC's D2 data center includes P&E controls that are commensurate with Federal guidance, industry standards, SEC policies and procedures, and the contract terms; and
3. SEC personnel timely and adequately addressed vulnerabilities previously identified at the D1 data center.

Appendices I and II include additional information about our objective, scope, and methodology, and the results of our contractor's assessment of the D2 data center P&E controls. Appendix III includes calculations of monetary impacts (that is, funds that may have been wasted, questioned costs, unsupported costs, and funds that could be put to better use) we identified during our audit.[7]

[7]As stated in Appendix III, we relied, in part, on the Inspector General Act of 1978, as amended (Public Law 95–452; 5 U.S.C. App.), to define monetary impact terms.

# Results

## Finding 1: The SEC Did Not Adequately Assess Contractors' Capabilities or Allocate Sufficient Time to Relocate Its Data Centers, Exposing SEC Data to Vulnerabilities

The SEC did not adequately assess its data center contractors' capabilities to meet the agency's needs, or allocate sufficient time to relocate its data centers, thereby exposing SEC data to certain vulnerabilities. Specifically, we determined that in 2008 the SEC paid an information technology provider—SMS—$162,000 to develop a data center relocation plan. According to the plan, a properly planned and executed data center relocation includes multiple comprehensive assessments and should take between 67 and 68 weeks to complete. However, the SEC did not follow SMS' recommendations for assessing D1's and D2's (b)(7)(E) capabilities and ensuring those capabilities met agency needs before awarding contracts and migrating agency data. In addition, the SEC selected and moved into the D1 location in about 25 weeks and, shortly thereafter, selected and moved into the D2 location in about 37 weeks. Finally, based on our observations, we question whether the D1 data center meets the contract requirement for compliance with TIA Tier III or greater standards.

SEC personnel currently responsible for the SEC's data centers were unaware of the 2008 data center relocation plan, and many of the key personnel responsible for the data center relocations no longer work at the SEC, including the individuals who served as the Chief Operating Officer, the Chief Information Officer, and the Contracting Officer (CO) at the time. In addition, as discussed in Finding 2, the SEC's data center contract files were incomplete. Therefore, we were unable to determine the rationale for not following SMS' data center relocation plan, or identify who was responsible for the decision to relocate both data centers within a compressed period.

Because the agency did not adequately assess its contractors' capabilities or allocate sufficient time to relocate its data centers before awarding contracts and migrating data, the SEC's D1 data center in particular has been exposed to (b)(7)(E) vulnerabilities since the inception of the contract. These vulnerabilities have disrupted the SEC's D1 data center operations, increased the risk to SEC equipment and data, and resulted in increased costs to the agency. We used an OIT estimate to determine that the SEC spent at least $300,000 to address (b)(7)(E) at the D1 data center between April 2014 and April 2015

and as a result of incidents that occurred on (b)(7)(E), (b)(7)(E), and (b)(7)(E). In addition, since contract award, the has SEC spent about $69,805 on (b)(7)(E) to mitigate P&E vulnerabilities identified through audits, reviews, and inspections, for a total of about $369,805 in questioned costs. Finally, because the SEC derived little, if any, benefit from SMS' data center relocation plan, the $162,000 paid to SMS represents funds that the SEC may have wasted.[8]

**The SEC Did Not Perform Adequate Assessments to Ensure Data Center Contractors Could Meet Agency Needs.** In 2008, the SEC paid SMS to develop a comprehensive plan for relocating the agency's data center operations that, at that time, were located in Ashburn and Alexandria, Virginia.[9] SMS completed a data center relocation plan that cost the SEC $162,000. According to SMS' plan, data center relocations include three phases: (1) Discovery, Planning, and Design; (2) Migration Preparation; and (3) Migration. SMS' plan identified best practices within each phase and indicated that a properly planned and executed data center relocation should take between 67 and 68 weeks to complete. SMS' plan also stated that a key part of the Migration Preparation phase is to perform an assessment to ensure all services are in place before the migration of any live data. Furthermore, the plan indicated that the migration preparation assessment should cover 12 items, including determining whether the proposed facility has in place sufficient power, cooling for planned equipment (current and future), and physical security controls which prevent unauthorized access.

We determined that the SEC did not follow SMS' recommendations for assessing D1's and D2's (b)(7)(E) capabilities and ensuring those capabilities met agency needs before awarding contracts and migrating agency data in 2012 and 2013. OIT provided us draft versions of its assessments of the D1 and D2 data centers. The draft versions, which cross-walked the SEC's data center requirements to the contractors' technical proposals, indicated that more comprehensive and detailed reports would be completed at a later date. However, OIT was unable to provide us with final versions of its data center assessments, or with evidence that OIT performed additional detailed assessments. In addition to OIT's draft data center assessments, OIT relied on (1) a questionnaire to identify areas to evaluate, validate, or clarify; and (2) interviews rather than independent verification of the contractors' ability to meet the SEC's data center requirements. For example, the SEC

[8] Appendix III includes calculations of monetary impacts.

[9] According to SMS' website, accessed on September 8, 2017, "SMS has extensive and demonstrated experience consolidating, building and operating data centers with over 2 million square feet completed to date . . . [SMS supports] government and military customers with their transformation and consolidation of data centers to reduce cost, improve operational efficiency, increase security, maximize performance levels, consolidate applications, and decrease energy costs."

stated that it required a data center that could provide (b)(7)(E) [redacted] However, the SEC did not determine or verify how much (b)(7)(E) [redacted] the D1 or D2 data centers could provide.

Moreover, we visited the D1 data center in June 2017 and noted the following conditions that appear to be noncompliant with TIA Tier III standards: (b)(7)(E) [redacted] As previously stated, the SEC's contracts with D1 and D2 require the data centers to meet TIA Tier III or greater standards. Based on our observations, we believe D1 may not be in compliance with the terms of its contract with the SEC. Therefore, SEC systems and data may be exposed to greater risks.[11]

**The SEC Did Not Allocate Sufficient Time To Relocate Its Data Centers.** The SEC did not follow SMS' recommendations and allocate sufficient time to properly complete the task of relocating its critical data center operations. For example, we compared best practices identified by SMS to the actions OIT took before selecting and moving into the D1 data center. Figures 1 and 2 show the differences in the activities and amount of time SMS recommended for each data center relocation phase and OIT's actions to complete each phase of the SEC's relocation to the D1 data center.

As shown in Figure 2, OIT selected and moved into the D1 data center in about 25 weeks instead of 67 to 68 weeks, as recommended by SMS. Of particular concern is the amount of time allocated to the Migration Preparation phase. As shown in Figure 1, SMS recommended a series of steps in this phase to be completed over 35 weeks. In comparison, as shown in Figure 2, OIT completed the D1 data center Migration Preparation phase in about 4 weeks. The SEC selected and moved into the D2 data center on a less aggressive schedule (in about 37 weeks), however, some of the activities to relocate both data centers overlapped.

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

[11] We visited the D2 data center in January and May 2017 and did not identify similar concerns.

**Figure 1. Recommended Data Center Relocation Best Practices and Timeframes**

| Discovery, Planning, & Design (20 weeks) | Migration Preparation (35 weeks) | Migration (12-13 weeks) |
|---|---|---|
| **Discovery** – Gather full information on the existing data center.<br>**Planning** – Develop project schedule and identify dependencies to aid in the migration.<br>**Design** – Develop a New Facilities and System Design Plan, and an Implementation Plan. | **Migration Preparation** – Perform assessment to ensure all services are in place prior to the migration of any live data.<br>Optimize and align source environment prior to the move to the new data center. | **Migration Phase** – Once target facility is operational, data and servers can be migrated. |
| **Total Time Recommended by SMS:** Between 67 and 68 weeks | | |

Source: OIG-generated based on the 2008 SMS data center relocation plan.

**Figure 2. Actual D1 Data Center Relocation Activities and Timeframes**

| Discovery, Planning, & Design (about 13 weeks) | Migration Preparation (about 4 weeks) | Migration (about 8 weeks) |
|---|---|---|
| **Discovery** – We did not identify any evidence to demonstrate that OIT gathered full information on the SEC data centers that existed at the time.<br>**Planning** – We did not identify a finalized project schedule.<br>**Design** – We did not identify a New Facilities and System Design Plan, or an Implementation Plan. | **Migration Preparation** – We were only able to obtain a draft assessment, which was not adequate in scope.<br>We did not identify any evidence to demonstrate that OIT optimized and aligned the source environment prior to the move to the new data center. | **Migration Phase** – We did not identify any evidence to demonstrate that the target facility was operational prior to the migration. |
| **Total Time OIT Took to Complete the SEC's D1 Data Center Relocation:** About 25 weeks | | |

Source: OIG-generated based on our review and analysis of contract documentation.

Current SEC personnel in both OIT and OA were unaware of the 2008 SMS data center relocation plan. Moreover, many of the key personnel responsible for the 2012-2013 data center relocations no longer work at the SEC, including the individuals who served as the Chief Operating Officer, the Chief Information Officer, and the CO at the time. In addition, as discussed in Finding 2, the SEC's data center contract files were incomplete. Therefore, we are unable to determine the rationale for not following SMS' data center relocation plan, or identify who was responsible for the decision to relocate both data centers within a compressed period.

**Vulnerabilities Posed Additional Risks and Costs for the SEC's D1 Data Center.** Because the agency did not adequately assess its contractors' capabilities or allow sufficient time to relocate its data centers before awarding contracts and migrating data,

the SEC's D1 data center in particular has been exposed to certain P&E vulnerabilities since the inception of the contract.[12] As discussed below, these vulnerabilities disrupted the SEC's D1 data center operations, increased the risk to SEC equipment and data, and resulted in about $369,805 in increased, questioned costs to the agency. In addition, because the SEC derived little, if any, benefit from SMS' data center relocation plan, the $162,000 paid to SMS represents funds that the SEC may have wasted.

(b)(7)(E) *Vulnerability.* Based on our discussions with SEC OIT and OA personnel, there appeared to be a misunderstanding between the agency and D1 regarding aspects of the power requirements stated in the contract, (b)(7)(E) shortly after the SEC moved in. Specifically, SEC personnel told us that, in early 2013, (b)(7)(E) As a result, in July 2013, the SEC modified its contract with D1 to ensure the agency's power needs were met. As further discussed in Finding 2, because of poor contract documentation, we could not determine whether the contract modification resulted from an error in the SEC's stated power requirements, the contractor's inability to meet the SEC's power requirements, or other factors. However, these issues may not have occurred had the SEC properly planned the data center move and adequately assessed D1's capabilities before awarding the contract. The corresponding contract modification is discussed in greater detail on page 15.

(b)(7)(E) *Vulnerability*. (b)(7)(E) has been an issue since the inception of the SEC's D1 data center contract. For example, in March 2013 (a month after the SEC moved into the D1 data center) OIT staff determined that (b)(7)(E) Even after (b)(7)(E) at the data center continued. The SEC contends that on 27 separate days between April 2014 and April 2015, (b)(7)(E) A similar incident occurred on (b)(7)(E), (b)(7)(E)

[12] We did not identify similar vulnerabilities at the SEC's D2 data center attributable to the agency's 2012–2013 data center relocations.

[13] (b)(7)(E)

(b)(7)(E) These incidents resulted in the SEC (b)(7)(E)

According to (b)(7)(E), D1 did not (b)(7)(E) at the D1 data center in accordance with the contract. Moreover, the (b)(7)(E) states D1's actions have caused (b)(7)(E) which have damaged SEC equipment, required vital systems to be shut down, and required significant SEC time and effort to resolve. (b)(7)(E) Nevertheless, on (b)(7)(E), and on (b)(7)(E), the D1 data center again (b)(7)(E) and the SEC had to shut down vital systems, (b)(7)(E). As of the date of this report, (b)(7)(E)

OIT personnel estimated that the SEC spent at least $10,000 on labor and equipment costs every time the agency experienced (b)(7)(E) at the D1 data center. Based on this estimate, we determined that the SEC spent at least $300,000 to address (b)(7)(E) at the data center on the 27 days cited in (b)(7)(E) and as a result of the (b)(7)(E), (b)(7)(E), and (b)(7)(E), incidents.[15] Furthermore, the SEC spent about $64,000 for (b)(7)(E) to mitigate the D1 data center's (b)(7)(E) vulnerability.

(b)(7)(E) *Vulnerability.* As further discussed in Finding 2, reviews conducted by (b)(7)(E) since 2014 identified vulnerabilities with the D1 data center's (b)(7)(E) According to SEC staff, the SEC has spent about $5,492 on (b)(7)(E)

[14] (b)(7)(E)

[15] We were unable to determine the total number of incidents involving (b)(7)(E) that have occurred at the D1 data center over the life of the contract because the SEC has not tracked the number of incidents. Therefore, we based our calculation on the incidents outlined in (b)(7)(E) and other incidents we became aware of during our audit.

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

[17] (b)(7)(E)

(b)(7)(E)

[redacted]

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

As of August 2017, there were five option years left on the SEC's data center contracts. On August 21, 2017, the SEC issued a request for information to help define its understanding of the availability of other potential data center facilities prior to release of a request for proposal. We encourage SEC leadership to begin identifying necessary resources and developing data center relocation plans. In preparation for future data center relocations, we recommend that the Office of the Chief Operating Officer:

**Recommendation 1:** Conduct comprehensive reviews of the D1 and D2 data center moves, requirements gathering efforts, and operations to identify lessons learned.

> **Management's Response.** The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Information Technology will conduct comprehensive reviews of past data center relocations, requirements gathering efforts, and operations to identify lessons learned. 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:** Obtain an assessment of the D1 data center, performed by qualified internal or external personnel, to determine whether the data center meets current agency requirements, including requirements specified in the contract. If the data center does not meet requirements, take action(s) deemed necessary and appropriate.

> **Management's Response.** The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Information Technology has undertaken an assessment of the D1 data center to determine if it meets SEC requirements. The Acting Chief Operating Officer further stated that the Office of Information Technology will review the results of its assessment and, if the data center does not meet contractual requirements, take appropriate action. 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: The SEC Did Not Adequately Manage or Monitor Its Data Center Contracts

The SEC did not adequately manage or monitor its data center contracts. Specifically, we found that:

- Contracting Officer's Representatives (CORs) did not always validate contractor invoices;
- the agency's data center contract files were incomplete and did not contain adequate support for critical decisions, including cost increases, related to the data centers;
- the data center contractors did not provide (and the SEC did not request) all required contract deliverables, such as annual security assessments and monthly reports, and the power consumption reports provided by D1 were unusable;
- the SEC did not effectively assess P&E controls at the data centers; and
- the SEC did not timely or adequately address a number of known vulnerabilities at the D1 data center.

The inadequate management and monitoring of the data center contracts was caused by (1) a lack of understanding and communication among key stakeholders in OA and OIT, including the CO and CORs; (2) insufficient oversight; and (3) OIT's lack of coordination with other stakeholders to identify vulnerabilities for which a plan of action and milestones (POA&M) should be created. In addition, OIT set unreasonable remediation deadlines.

As a result, the SEC paid D2 invoices containing formula errors resulting in $217,159 in overpayments (which has since been refunded). We also determined that the agency paid D1 about $2.8 million in unsupported costs. Specifically, through contract Task Order 1, the SEC paid D1 $947,075 for data center build-out costs although the COR contract file did not contain evidence of an acceptance certificate or an inspection or receiving report form for the work. In addition, the SEC approved an increase in the kilowatt-per-hour rate charged by D1—which cost the agency about $1.7 million between January 2013 and July 2017—that was not adequately supported. The SEC also paid D1 $125,443 in unsupported costs to rent power distribution units (PDUs) between January 2013 and July 2017 instead of purchasing the PDUs. Moreover, the SEC paid for deliverables that the contractors did not provide or provided in unusable formats. If the SEC does not take corrective action to validate certain costs associated with contract Modification 3 and if all

contract options are exercised, the agency will incur additional costs of about $2.7 million in funds that the SEC could put to better use over the remaining life of D1's contract.[18] Finally, because the SEC did not effectively assess P&E controls at the data centers and timely or adequately address a number of known vulnerabilities at the D1 data center, SEC equipment and data has been vulnerable to (b)(7)(E) [redacted]

**CORs Did Not Always Validate Contractor Invoices.** We reviewed all 59 invoices paid under D1's contract between January 2013 and July 2017, and all 48 invoices paid under D2's contract between December 2013 and July 2017. Although the CORs have maintained a spreadsheet to track and validate total invoiced amounts for both contracts, the CORs did not always verify the accuracy of underlying rates or quantity calculations in the invoices, as required by SEC Administrative Regulation (SECR) 10-15, *Contracting Officer's Representative* (Rev. 3; January 14, 2016) (SECR 10-15).[19] For example, we could not trace 21 of the 48 D2 invoices to supporting documentation and, therefore, questioned monthly recurring charges for module space at the D2 data center. The COR could not provide an explanation and had to ask D2 personnel for the underlying formula and information the contractor used to charge the SEC.

We determined that the CORs did not always validate invoices from the SEC's data center contractors because the CORs did not fully understand their duties and responsibilities. Furthermore, the CO did not provide effective oversight of the CORs' invoice validation process and never reviewed COR contract files. We have previously reported that SEC CORs have not always performed their duties consistently and as required, CORs did not fully understand their roles and responsibilities, and COs did not adequately oversee CORs.[20]

As a result, the SEC paid D1 and D2 but did not ensure that it paid correct amounts or that the contractors provided required services in accordance with the terms of their

[18] Appendix III includes calculations of monetary impacts.

[19] SECR 10-15 states that the COR's approval of an invoice indicates acceptance and that the invoice conforms to the terms of the contract. CORs must keep an invoice tracking sheet and ensure that (1) the products or services being invoiced have been received by the SEC and meet contract requirements or standards; (2) invoices are approved only after the delivery or performance is satisfactorily completed; (3) invoices indicate the contract line item number and the amount the contractor is billing against each line item; and (4) information such as unit prices, billing rates, and periods of performance are correct and conform to the contract. Otherwise, CORs must reject invoices. Although the SEC released the current version of SECR 10-15 after the agency awarded data center contracts to D1 and D2, these COR responsibilities have remained largely unchanged.

[20] U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Contracting Officers' Representative Program* (Report No. 530; September 18, 2015), and *Management of the SEC's Protective Security Force Contract Needs Improvement* (Report No. 536; June 22, 2016).

contracts. In response to our questions about 21 of D2's 48 invoices, D2 personnel performed an internal review and concluded that they inadvertently failed to adjust D2's billing to reflect variations in the number of housing racks provided under the SEC's contract between August 2015 and February 2017. Consequently, the SEC overpaid D2 $217,159. On May 1, 2017, D2 refunded the full amount to the SEC.

**Data Center Contract Files Were Incomplete.** Federal Acquisition Regulation (FAR) Subpart 4.8, *Government Contract Files*, section 4.801(b), states:

> The documentation in the [contract] files (see 4.803) shall be sufficient to constitute a complete history of the transaction for the purpose of— (1) providing a complete background as a basis for informed decisions at each step in the acquisition process; (2) supporting actions taken; (3) providing information for reviews and investigations; and (4) furnishing essential facts in the event of litigation or congressional inquiries.

Furthermore, section 4.803 of FAR Subpart 4.8 states that contracting office files normally contain, among other things, justifications and approvals, determinations and findings, and associated documents; the original signed contract or award; all contract modifications; and documents supporting modifications. Additionally, according to SECR 10-15, the COR must maintain a "COR contract file" that, at a minimum, contains the following: (1) COR appointment letter signed by all parties; (2) contract and contract modifications, orders, and order modifications (if applicable); (3) all contract correspondence; (4) records of COR inspections; (5) documentation of any and all contract decisions or actions and the rationale for them; (6) records of conversations with the contractor; and (7) invoices and vouchers.

We determined that the CO's and CORs' contract files for the SEC's data center contracts were incomplete and did not contain adequate support for critical decisions (including cost increases) related to the data centers, or information necessary to properly monitor the contracts, perform day-to-day contract administration, and manage the contracts' complex technical requirements. For example, the official contract files maintained by the CO did not include final preliminary and post-award on-site assessments of either data centers, or the SEC-approved floor plan for the D1 data center. The CO was able to provide contract modifications upon request, although he did not always maintain the modifications in the contract files. In addition, as further described below, the COR contract files were incomplete. The files did not contain—and the SEC did not maintain elsewhere—some meeting minutes and invoices, including sufficient support for expenses paid by the SEC for a significant build-out at the D1 data center. Additionally, the COR contract files did not include rationale and sufficient support for a significant modification to D1's contract that increased agency costs and located the (b)(7)(E) [redacted]

*Missing Meeting Minutes, Invoices, and Related Documents*. We determined that the D1 and D2 data center COR contract files each contained meeting minutes for about a 1-year period even though the contracts have been ongoing for over 4 years. Additionally, the D1 COR contract file was missing 10 of 59 invoices paid under D1's contract between January 2013 and July 2017, and the D2 COR contract file was missing 9 of 48 invoices paid under D2's contract between December 2013 and July 2017. Finally, in January and February 2013, D1 invoiced the SEC for a total of $947,075 for a significant build-out at the D1 data center to install physical infrastructure including cages, racks, power strips, and other power infrastructure covered under contract Task Order 1. The SEC paid the full invoiced amount. However, the D1 COR contract file did not contain an itemized list of what the SEC purchased or evidence of acceptance[21] of Task Order 1 work, as required by the contract and the task order.[22] Additionally, Modification 3 to the D1 contract (signed after Task Order 1) indicated that the modification was for infrastructure, namely:

> . . . the cost of the utility energy generation, utility energy transmission, facility [uninterruptable power supply] UPS and battery capacity, generator fuel, lighting fixtures and all related system components from the facility/utility demarcation through the (b)(7)(E) [redacted], all operation and maintenance of this equipment and the capital required to supplement it as SEC capacity increases.

As discussed below, Modification 3 was made retroactive to all base and option periods. Therefore, it appears that the facilities, equipment, and communication circuits paid for as part of the build-out under Task Order 1 may not have met the SEC's requirements.

*Missing Rationale and Support for a Significant Modification to the D1 Contract (Modification 3)*. The COR contract file for the SEC's D1 data center contract did not include a clear rationale for a significant contract modification. Modification 3, signed on July 1, 2013, and made retroactive to all base and option periods, allowed D1 to more than double the rate it charged the SEC per kilowatt hour for power used, and bill the SEC for additional recurring monthly charges. The kilowatt-per-hour rate increased from (b)(4) [redacted] However, neither the modification nor the corresponding memorandum to the record clearly justified the significant rate increase or explained why the SEC agreed to the increased costs. According to the documents we reviewed,

[21] According to sections 46.501 and 46.502 of FAR Subpart 46.5, *Acceptance*, acceptance constitutes acknowledgment that the supplies or services conform with applicable contract quality and quantity requirements, and shall ordinarily be evidenced by execution of an acceptance certificate on an inspection or receiving report form or commercial shipping document or packing list.

[22] The SEC's contract with D1 states that the SEC will conduct tests to ensure that the contractor's facilities, equipment, and communication circuits meet SEC requirements. The contract further states that the SEC will formally accept the contractor's data center, equipment, and communications circuits after completing testing and, for final acceptance, the SEC will review and approve its own testing results.

the change in the SEC's kilowatt-per-hour rate was expected to increase the SEC's cost by about $1.3 million over the life of the contract, which the SEC believed represented cost savings when compared to a previous data center contractor. When asked, SEC personnel could not provide documentation supporting their calculation or explain how this figure was calculated.

We determined that the cost increase incurred as a result of the increase in the agency's kilowatt-per-hour rate between January 2013 and July 2017 has already exceeded the SEC's projected cost increase for the life of the contract. Specifically, between January 2013 and July 2017, the SEC paid about $1.7 million in additional unsupported costs as a result of the kilowatt-per-hour rate increase (or about $400,000 over the SEC's projected amount for the life of the contract). We estimate that the cost of the rate increase for the remaining life of the contract, if all options are exercised, will be about $2.5 million, for total increased costs of about $4.2 million.[23]

In response, OA personnel told us that the total prices paid for both the D1 and D2 data centers are similar for like services, and that, according to section 15.404-1(b)(2) of FAR Subpart 15.4, *Contract Pricing*, price analysis can be used to determine reasonableness without evaluation of separate costs. OA contends that revised prices paid in Modification 3 were within the original government estimate and within competitively proposed prices.

However, FAR 15.404-1(b)(2) also specifies that, if using price analysis, the prior price must be valid for comparison and must be adjusted for materially differing terms and conditions. For example, if the reasonableness of the prior price is uncertain, it may not be a valid basis for comparison. As OA could not provide us the source of the comparison of the prior data center costs, or how personnel calculated Modification 3 pricing used in the comparison, we could not assess the reasonableness of the comparison. Furthermore, correspondence between D1 and SEC personnel indicated that D1 proposed infrastructure costs as a lump sum. At the SEC's request, D1 personnel proposed an alternative solution: an increase in the agency's kilowatt-per-hour rate. However, the COR contract file did not include documentation on the lump sum cost or a comparison of the lump sum cost versus the rate increase.

Additionally, Modification 3 allowed D1 to charge the SEC rent (as a monthly reoccurring cost) for 62 PDUs—items that distribute power to computers and equipment in a data center—in the SEC's cage area at the D1 data center. The contract file did not contain any documentation explaining why the SEC agreed to pay monthly rent for the PDUs instead of purchasing them. The cost of renting the PDUs between January 2013

[23] We based our calculation on actual power consumption from January 2013 through July 2017 (about $1.7 million) plus projected power consumption for the remaining contract option years (about $2.5 million, based on a 1 percent increase per year, as estimated by the SEC) multiplied by the rates included in Modification 3.

through the remaining life of the contract is about $306,162, which greatly exceeds what it would have cost the SEC to purchase the PDUs (about $16,715 in total). As of July 2017, the SEC had already paid $125,443 in unsupported PDU rental costs. Unless the SEC takes corrective action, the agency will effectively pay for the PDUs almost 18 times over. However, purchasing the PDUs would result in about $164,004 in funds that could be put to better use.[24]

(b)(7)(E)

The SEC's data center contract files were incomplete and did not contain adequate support for critical decisions, including cost increases, because the CORs did not fully understand their duties and responsibilities or the limits of their authority, and the CO did not provide sufficient oversight of the CORs' activities. Specifically, the CO did not meet with each new COR during transitions to establish expectations or provide background on the contracts.[25] Furthermore, the CO did not ensure CORs were monitoring the contractors' compliance with the terms and conditions of the contracts. Finally, according to OA policy personnel, although the CORs were required to maintain contract files, the CORs did not have a designated system to maintain their documents. In the future, the CORs will use the SEC's newly implemented electronic filing system.

Incomplete CO and COR contract files have several implications. Chief among them was our inability to obtain adequate documentation supporting important contract-related decisions, including significant cost increases. As a result, we identified the cost of (1) the D1 data center build-out, (2) the increase in the D1 data center kilowatt-per-hour rate between January 2013 and July 2017, and (3) PDU rental at the D1 data center between January 2013 and July 2017 as unsupported costs. These unsupported costs total about $2.8 million.

**Data Center Contractors Did Not Provide, and the SEC Did Not Request, All Required Contract Deliverables, and Some Deliverables Were Unusable.** The SEC's data center contracts require the contractors to provide the agency 31 deliverables on a recurring basis, including annual information security assessments

[24] We based our calculation on the cost of renting the current number of PDUs over the remaining life of the contract at the monthly rates specified in the contract (about $180,719) minus the cost of purchasing the PDUs at their current approximate cost ($16,715).

[25] As of August 2017, the SEC's data center contracts had each had at least four different CORs.

and results of physical security reviews.[26] The contractors must also provide the SEC with monthly reports to verify the contractors' performance.[27] We reviewed the contractors' submissions of required contract deliverables since contract award and determined that the contractors did not provide, and the SEC did not request, all required deliverables. Specifically, as of April 2017, D1 had provided only 1 required contract deliverable, and D2 had not provided any of the 31 required contract deliverables. Additionally, D2 did not provide the SEC with monthly reports until March 2015, or 2 years after the contract was awarded. D1 consistently provided monthly reports; however, the reports stated only that D1 was in compliance with the service level agreement between the contractor and the SEC.[28] Lastly, an SEC official noted that D1's required monthly power consumption reports were not in a format useful for monitoring the SEC's operations at the D1 data center.

We determined that the CORs did not fully understand their duties and responsibilities or the limits of their authority, and did not perform their duties as required. For example, the CORs thought they had the authority to waive deliverables required by the contracts. According to the FAR and SEC policy, CORs do not have such authority.[29] Additionally, the CORs believed that if they did not specify deliverable formats at the beginning of the contracts they could not later define deliverable formats or content. According to OA policy personnel, this is also inaccurate.

Without the deliverables the SEC required under the contracts, we question how the agency could adequately monitor the contractors' performance to ensure SEC equipment and data was not vulnerable to damage, loss, or system disruptions. Specifically, it is unclear how SEC personnel maintained an up-to-date understanding of

[26] The SEC is considering a modification to both data center contracts that would remove some or all of the deliverables outlined in Attachment 3 to the data center contracts—*SEC [Information Technology] Security Requirements for [Information Technology] Acquisitions.*

[27] The exact content and format of monthly reports was to be defined by the contractor and the SEC, however, the reports were to include, at a minimum, information on any unplanned or emergency outages, exceptions for any contract service terms not met, the contractors' annual testing schedule, access logs, and monthly power consumption information. Furthermore, according to SECR 10-15, the COR must ensure that all required items, work products, documentation, data and/or reports are submitted as required by the contract. Also, the COR must perform a final inspection and acceptance of all deliverables required under the contract.

[28] A service level agreement is a formal, negotiated document that defines in quantitative and perhaps qualitative terms the service being offered to a customer. The SEC's data center service level agreements cover power availability, recovery time, power incident management communications and escalations, electrical infrastructure, cross connect availability, and security breach notifications.

[29] Section 1.602-2(d)(5) of FAR Subpart 1.6, *Career Development, Contracting Authority, and Responsibilities*, states that a COR "Has no authority to make any commitments or changes that affect price, quality, quantity, delivery, or other terms and conditions of the contract nor in any way direct the contractor or its subcontractors to operate in conflict with the contract terms and conditions."

the security state and risk posture of information systems and data stored and processed at the agency's data centers. As a result, we question whether agency personnel could make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses, including contract actions, as needed.

In addition, because the deliverables specified in the contracts were included in the price of the contracts, the SEC paid for items it never received.[30] Furthermore, because D1's monthly power consumption reports were not in a format useful for monitoring SEC equipment, OIT has, at least on one occasion, paid for additional analysis to ensure SEC equipment was not at risk. This additional ad-hoc analysis, performed by the SEC's Information System Support contractor, cost the SEC about $5,400.

**The SEC Did Not Effectively Assess P&E Controls at Its Data Centers.** OIT conducts assessments of P&E controls at the SEC's data centers as part of its General Support System Security Assessment and Authorization process. Furthermore, the E-Government Act of 2002 requires agencies to comply with the NIST P&E standards.[31] However, we determined that OIT's assessments of the data centers' P&E controls were not comprehensive or risk-based and did not effectively assess the controls at either data center. For example, the OIT staff member who conducted the reviews (the assessor) did not consider known vulnerabilities or contract requirements when selecting the methodology for the assessments. Also, at times, the assessor relied primarily on interviews for items that were easily testable. For instance, to review temperature controls, the assessor interviewed contractor personnel rather than independently test data center temperatures. The assessor's November 2016 assessment of the D1 data center identified no findings (b)(7)(E) [redacted] at that location. Similarly, the January 2017 assessment of the D2 data center identified no findings even though an assessment conducted about 5 months later by a contractor we hired identified 14 deficiecies related to (b)(7)(E) [redacted].[32] Appendix II provides a summary of the deficiencies noted in our contractor's report and each deficiency's severity.

[30] We were unable to determine the cost of contract deliverables never received as such costs were not separately identified in the contracts.

[31] These standards describe the controls that should be in place to ensure P&E safeguards are sufficient for Federal information systems. The effectiveness of the P&E controls can be assessed by examination, testing, interviewing, or a combination of all three. Regarding P&E controls, the SEC's data center contracts stipulate specific temperature, humidity, and access control requirements.

[32] During our audit, we contracted the services of Milligan and Company, LLC/Samlin Consulting (Milligan) to perform an assessment of the P&E controls at the D2 data center. Milligan performed the assessment on May 31, 2017.

According to OIT personnel, the selection of methods used to assess P&E controls at the SEC's data centers was at the discretion of the assessor. The OIT staff member who assessed P&E controls at both the D1 and D2 data centers indicated that she was unaware of (b)(7)(E) at D1. She further stated that, even if she had known about the results of prior audits and reviews, she would not have altered her assessment methodology.

Because OIT's assessments of the data centers' P&E controls were not risk-based and did not effectively assess the controls at either data center, (b)(7)(E)

Additionally, (b)(7)(E) vulnerabilities at the D1 data center and the 14 deficiencies identified by the contractor we hired to assess the D2 data center stand in stark contrast to the lack of findings from OIT's most recent assessments of both data centers. As a result, we believe the assessments conducted by OIT were ineffective and not useful.

**The SEC Did Not Timely or Adequately Address Known Vulnerabilities at the D1 Data Center.** OIT did not create a POA&M for 9 of the 29 vulnerabilities identified (b)(7)(E) Furthermore, OIT did not timely address 16 of the remaining 20 vulnerabilities with a POA&M. On average, it took OIT about 800 days to implement corrective actions for these 16 POA&M items.

According to the Office of Management and Budget, a POA&M is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones.[34] In addition, according to SECR 24-04 (Rev 2), *Information Technology Security Program*, vulnerabilities that require the deployment of additional resources are developed into POA&Ms. Each POA&M shall describe the risk, suggested mitigation activities, resources required for mitigation, responsibility for mitigation, and estimated completion date. OIT's Information Security Office is responsible for monitoring the progress of mitigation activities described in each POA&M and for periodic security compliance reviews of all information systems.

[33] (b)(7)(E)

[34] Office of Management and Budget, M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.

OIT staff told us that untimely and inadequate responses to known vulnerabilities at the D1 data center occurred because of the lack of review meetings to track progress or closure of POA&Ms, and because OIT set unreasonable remediation deadlines. Furthermore, we found that OIT's Information Security Office was not coordinating with other stakeholders to identify vulnerabilities for which a POA&M should be created. OIT officials stated that they have updated the SEC's POA&M process to ensure reasonable deadlines are set and regular review meetings occur.

Because vulnerabilities at the SEC's D1 data center were not timely or adequately addressed, SEC data, equipment, and systems were unnecessarily exposed to threats, (b)(7)(E) [redacted]

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

We have previously reported that SEC CORs did not always perform their duties consistently and as required; CORs did not fully understand their roles and responsibilities; and COs did not adequately oversee CORs. In response to our previous reports, the SEC took corrective action; however, those actions did not prevent the contract management deficiencies we observed during this audit. We strongly encourage the Director of the Office of Acquisitions to conduct a comprehensive review of the SEC's COR Program and ensure controls are developed or strengthened to improve the agency's contract management specific to activities performed by CORs and COs to oversee and document contractor performance and deliverables and contract actions.

In the agency's response to a draft of this report, the Acting Chief Operating Officer stated that the Director of OA will undertake a review of contractor performance oversight and documentation, including the Contractor Performance Assessment Reporting System, deliverables, and COR file documentation in order to improve the management of agency contracts. Additionally, OA will review COR and CO training for areas of improvement specific to understanding roles and responsibilities, including improvements in CO oversight of COR actions and documentation. Management's complete response is reprinted in Appendix IV.

To improve the U.S. Securities and Exchange Commission's management of its data center contracts, we recommend that:

**Recommendation 3:** The Contracting Officer address (b)(7)(E) issued to D1 data center provider on May 6, 2015.

**Management's Response.** The Acting Chief Operating Officer concurred with the recommendation and stated that the Contracting Officer will continue to work with the Office of General Counsel, Office of Information Technology, and contractor to address the (b)(7)(E). In particular, management will continue to work with the contractor to address the underlying issue of (b)(7)(E). 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 4:** Under the Contracting Officer's oversight, the Contracting Officer's Representatives for the agency's data center contracts validate underlying calculations and quantities for all invoices paid under both contracts as of the date of this report, and resolve any discrepancies identified.

**Management's Response.** The Acting Chief Operating Officer concurred with the recommendation and stated that the Contracting Officer and Contracting Officer's Representatives will work together to validate all invoices paid to include underlying calculations and quantities under both contracts and resolve identified discrepancies. 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 5:** The Contracting Officer and Contracting Officer's Representatives for the agency's data center contracts (a) review their records, including emails and other hardcopy and soft copy files, to identify any documents that should have been included in the official data center contract files, and properly file any documents found; (b) establish a process for ensuring the contract files will be properly maintained for the remainder of the contracts, including through the use of the agency's electronic filing system; and (c) develop steps the Contracting Officer will undertake to closely monitor the activities of the Contracting Officer's Representatives for the remainder of the contracts, including regular meetings and file reviews, and establish a schedule for accomplishing each step.

**Management's Response.** The Acting Chief Operating Officer concurred with the recommendation and stated that the Contracting Officer and Contracting Officer's Representatives will work together to review the data center(s) contract file records, including emails and other hard copy and soft copy files, to identify any documents that should be included in the contract files. According to the Acting Chief Operating Officer, the Contracting Officer and Contracting Officer's Representatives will also follow established procedures to ensure the contract files are properly maintained for the remainder of the contracts, including the use of the electronic filing system. The Office of Acquisitions will review existing procedures and develop steps for the Contracting Officer to take to closely monitor the activities of the Contracting Officer's Representatives for the remainder of the contracts, including regularly scheduled meetings and file reviews. 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 6:** The Contracting Officer and Contracting Officer's Representative for the agency's D1 data center contract (a) validate the need to rent from the contractor power distribution units, and consider purchasing the units instead; and (b) validate all other monthly recurring costs in the contract to determine whether those costs are reasonable, necessary, and in the best interests of the government, including the cost of the kilowatt-per-hour rate increase.

**Management's Response.** The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Acquisitions and Office of Information Technology will review and validate the rental of power distribution units and determine if purchasing the units outright is in the best interest of the government, taking liability risk into account. The Contracting Officer and Contracting Officer's Representative will also review other recurring costs and reconfirm the previous determination of those prices paid, including prices paid for power as reasonable, necessary, and in the best interests of the government in accordance with FAR 15.4. 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 7:** The Contracting Officer and Contracting Officer's Representatives for the agency's data center contracts assess all required contract deliverables and, where needed, work with the contractors to establish or clarify expectations for each deliverable's format, content, and timeframe for submission to the agency.

**Management's Response.** The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Acquisitions and Office of Information Technology have already initiated the process of assessing all required contract deliverables. It is anticipated that the Contracting Officer and Contracting Officer's Representative will clarify with the contractor the requirements for each needed deliverable's format, content, and timeframe for submission to the agency. 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 8:** The Office of Information Technology ensure assessors use a risk-based or comprehensive approach to data center physical and environmental control assessments that considers prior audits, assessments, and known vulnerabilities.

**Management's Response.** The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Information Technology will ensure assessors use a risk-based approach to data center physical and environmental control assessments that considers prior audits, assessment, and known vulnerabilities. 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 9:** The Office of Information Technology develop a plan to timely address the physical and environmental vulnerabilities at the D2 data center identified by our contractor.

**Management's Response.** The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Information Technology has begun developing a plan to address the vulnerabilities identified. 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 10:** The Office of Information Technology ensure responsible personnel coordinate with other stakeholders to identify data center vulnerabilities for which a plan of action and milestones should be created, and address existing plan of action and milestones items related to vulnerabilities at the D1 data center.

**Management's Response.** The Acting Chief Operating Officer concurred with the recommendation and stated that the Office of Information Technology has identified responsible personnel to coordinate with other stakeholders to identify data center vulnerabilities. Creation of a plan of action and milestones is underway to address existing vulnerabilities at the D1 data center. 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, an other matter of interest that did not warrant recommendations came to our attention. We discussed the matter, described below, with agency management for their consideration.

As previously stated, the SEC awarded the D1 and D2 data center contracts on (b)(7)(E), and (b)(7)(E), respectively. Since that time, the SEC has modified the D1 data center contract more than 20 times, and has modified the D2 data center contract more than 15 times. However, the SEC did not update either contract's requirements to reflect current versions of industry standards and guidance cited in the contracts. Specifically, both data center contracts require the contractors to:

- comply with Tier III or greater standards as defined in *Telecommunications Infrastructure Standard for Data Centers*, TIA-942-2; and

- implement security controls commensurate with NIST SP 800-53, Revision 3 for systems with the security categorization of "Moderate," as defined in NIST Federal Information Processing Standards 199 and 200.

At the time of both awards, however, TIA-942-2 had been superseded by TIA-942-A, which was published in August 2012. In addition, in April 2013, NIST released Revision 4 of NIST SP 800-53.

The SEC required its data center contractors to comply with applicable telecommunications industry standards and NIST guidance to ensure, among other things, agency equipment and data were not vulnerable to damage, loss, and system disruptions. To ensure this objective is achieved, we encourage agency management to consider modifying both contracts to reference current versions of the industry standards and guidance cited in the contracts.

# Appendix I. Scope and Methodology

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

**Scope.** The audit covered SEC activities between 2008 and 2013 to prepare for relocation of the agency's data centers, including awarding the existing contracts with D1 and D2. The audit also covered SEC activities to manage and monitor the D1 and D2 data centers and corresponding contracts after contract award through September 29, 2017.

Our objective was to assess the SEC's management of its data centers. Specifically, we sought to determine whether:

1. SEC personnel properly monitored the contractors' performance at the agency's D1 and D2 data centers;

2. the SEC's D2 data center includes P&E controls that are commensurate with Federal guidance, industry standards, SEC policies and procedures, and the contract terms; and

3. SEC personnel timely and adequately addressed vulnerabilities previously identified at the D1 data center.

We performed fieldwork at the SEC's Headquarters in Washington, DC, and the SEC's data centers located in (b)(7)(E) [redacted].

**Methodology.** We interviewed SEC personnel from OIT and OA to understand the SEC's management of its data centers and data center contractors, P&E controls at the SEC's data centers, and processes for addressing vulnerabilities previously identified at the D1 data center. We also interviewed the CO and CORs to understand their roles and responsibilities for overseeing the data center contractors. In addition, we reviewed contract files, correspondence, task orders, invoices, and prior audits and assessments of the data centers, and performed site visits at both data center locations.

We hired a contractor (Milligan) to assess the SEC's D2 data center P&E controls and to determine whether the controls were commensurate with Federal guidance, industry standards, SEC policies and procedures, and the terms of the SEC's contract with D2. Milligan reviewed applicable policies and procedures, identified relevant controls, performed an onsite assessment on May 31, 2017, and discussed with D2 and SEC

personnel the results of the assessment. On June 30, 2017, we provided the SEC with Milligan's report, which summarized the deficiencies Milligan identified and recommended corrective actions. Appendix II includes additional details on the results of Milligan's D2 data center P&E control assessment.

Finally, we reviewed the SEC's corrective actions to address known vulnerabilities at the D1 data center. We interviewed officials responsible for addressing these vulnerabilities and determined whether corrective actions taken effectively addressed prior findings and recommendations.

**Internal Controls.** To assess internal controls relative to our objectives, we reviewed the SEC's management assurance statements and risk assessments covering OA and OIT for fiscal year 2016. In the management assurance statements, management reported that it tested control activities to evaluate the design and effectiveness of internal controls. SEC management identified areas requiring improvement but reported that the areas did not create the risk of material weakness. As a result, SEC management concluded that the controls and processes in place were effective.

We also tested key internal controls related to the SEC's management of its data center contracts. Specifically, we assessed (1) OIT's process for reviewing P&E controls at the SEC's data centers, (2) the CO's process for monitoring the contractors' performance, (3) the CORs' process for reviewing deliverables and approving invoices, and (4) OIT's process for addressing vulnerabilities at the D1 data center. As discussed in this report, we noted internal control weaknesses that impact the SEC's ability to ensure (1) agency equipment and data are not vulnerable to damage, loss, and system disruptions; (2) unsupported and/or questioned costs are not incurred related to the data center contracts and operations; (3) agency funds are used as efficiently and effectively as possible; and (4) the agency's data center contracts are properly managed. Our recommendations, if implemented, should correct the weaknesses we identified.

**Computer-processed Data.** We did not rely significantly on computer-processed data to address our audit objective. Therefore, we did not assess any system controls or the reliability of any computer-processed data.

**Prior Coverage.** Between 2014 and 2016, the SEC OIG and GAO issued the following four reports of particular relevance to this audit:

SEC OIG:

- *Audit of the SEC's Physical Security Program* (Report No. 523, August 1, 2014).
- *Audit of the SEC's Contracting Officers' Representative Program* (Report No. 530, September 18, 2015).

GAO:

- *Information Security, SEC Needs to Improve Controls over Financial Systems* (GAO-14-419, April 2014).
- *Information Security, Opportunities Exist for SEC to Improve Its Controls over Financial Systems and Data* (GAO-16-493, April 2016).

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

# Appendix II. Results of D2 Data Center P&E Control Assessment

As stated in Appendix I, we hired Milligan to assess the SEC's D2 data center P&E controls and to determine whether controls were commensurate with Federal guidance, industry standards, SEC policies and procedures, and the terms of the agency's contract with D2. On May 31, 2017, Milligan performed an onsite assessment and identified 14 control deficiencies categorized as either weaknesses in (b)(7)(E) [redacted] Table 2 summarizes the 14 control deficiencies and recommended corrective actions.

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

**Table 2. Summary of Milligan's D2 Data Center P&E Control Assessment**

| Deficiency Number | (b)(7)(E) [redacted] | [redacted] | [redacted] |
|---|---|---|---|
| 1 | (b)(7)(E) [redacted] | | |

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

| Deficiency Number | (b)(7)(E) | [redacted] | [redacted] |
|---|---|---|---|
| 2 | (b)(7)(E) | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |

| Deficiency Number | (b)(7)(E) | [redacted] | [redacted] |
|---|---|---|---|
| 9 | (b)(7)(E) [redacted] | | |
| 10 | | | |
| 11 | | | |
| 12 | | | |
| 13 | | | |

| Deficiency Number | (b)(7)(E) [redacted] | [redacted] | [redacted] |
|---|---|---|---|
| 14 | (b)(7)(E) [redacted] | | |

Source: Milligan and Company/Samlin Consulting, U.S. Securities and Exchange Commission, Office of Inspector General, *Data Center Physical and Environment Controls Assessment*, July 14, 2017.

# Appendix III. Calculations of Monetary Impacts

### Table 3. Funds That May Have Been Wasted[36]

| Item | Actual Cost |
|---|---|
| SMS Data Center Relocation Plan | $162,000 |

### Table 4. Questioned Costs[37]

| Item | Estimated Cost |
|---|---|
| Personnel and Equipment Costs Resulting from D1 Data Center (b)(7)(E) Between April 2014 and April 2015, and Incidents on (b)(7)(E) *(about $10,000 x 30 incidents)* | $300,000 |
| Cost of (b)(7)(E) Purchased to Improve D1 Data Center P&E Controls *(about $50,000 for (b)(7)(E), $14,313 for (b)(7)(E), and $5,492 for (b)(7)(E))* | $69,805 |
| Cost of Information System Support Contractor's Ad Hoc Analysis of D1's October 2016 Power Consumption Report | $5,400 |
| **Total Questioned Costs** | **$375,205** |

### Table 5. Unsupported Costs[38]

| Item | Actual Cost |
|---|---|
| Cost of D1 Data Center Build-out *(invoices dated January 14 and February 8, 2013)* | $947,075 |
| Cost of Kilowatt-per-hour Rate Increase at D1 Data Center, Resulting from Modification 3 *(January 1, 2013, through July 31, 2017)* | $1,706,364 |
| Monthly Cost to Rent PDUs at D1 Data Center, Resulting from Modification 3 *(January 1, 2013, through July 31, 2017)* | $125,443 |
| **Total Unsupported Costs** | **$2,778,882** |

[36] We defined "waste" as use or expense of resources carelessly, extravagantly, or to no purpose. Waste can include activities that do not involve abuse or a violation of law. Rather, waste relates primarily to mismanagement, inappropriate actions, and inadequate oversight.

[37] As defined by the Inspector General Act of 1978, as amended (Public Law 95–452; 5 U.S.C. App.), questioned costs include those costs questioned because of an alleged violation of a provision of a contract, and expenditures of funds that are unnecessary or unreasonable.

[38] As defined by the Inspector General Act of 1978, as amended (Public Law 95–452; 5 U.S.C. App.), unsupported costs are those costs questioned because, at the time of the audit, the costs were not supported by adequate documentation.

We recommend that the CO and COR for the agency's D1 data center contract (a) validate the need to rent from D1 PDUs, and consider purchasing the units instead; and (b) validate all other monthly recurring costs in the contract to determine whether those costs are reasonable, necessary, and in the best interests of the government, including the cost of the kilowatt-per-hour rate increase resulting from contract Modification 3 (see Recommendation 6). If the SEC does not take corrective action to validate these costs and if all contract options are exercised, as shown in Table 6 below, the agency will incur costs of about $2.7 million in funds that the SEC could put to better use over the remaining life of D1's contract.

**Table 6. Funds That Could Be Put to Better Use**[39]

| Item | Estimated Cost |
|---|---|
| Cost of Kilowatt-per-hour Rate Increase at D1 Data Center, Resulting from Modification 3 *(projected power consumption, based on 1 percent increase per year, for the remaining contract option years [August 2017 – October 2022])* | $2,534,580 |
| Cost of Monthly Rental of PDUs at D1 Data Center Less Estimated PDU Purchase Cost *($180,719 rent over contract option years [August 2017 – October 2022] minus $16,715 estimated purchase cost)* | $164,004 |
| **Total Funds That Could Be Put to Better Use** | **$2,698,584** |

[39] As defined by the Inspector General Act of 1978, as amended (Public Law 95–452; 5 U.S.C. App.), funds that could be put to better use are those funds that could be used more efficiently if management takes action to implement recommendations. This includes costs not incurred and other costs savings achieved through corrective action.

# Appendix IV. Management Comments*

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

FROM: /s/ Kenneth A. Johnson, Acting Chief Operating Officer

DATE: September 25, 2017

SUBJECT: Response to Draft Report on SEC's Management of Its Data Center

Thank you for the opportunity to review and comment on the draft report on the SEC's management of its data centers. We take very seriously our obligation to protect the agency's critical telecommunications, data, and computing resources and our obligation to be good stewards of agency resources.

We appreciate your acknowledgment of the corrective actions we have already taken to strengthen contract management and welcome your recommendation on how we can further improve. As we note below, we concur with all the recommendations in your draft report, and believe they correctly identify a number of lessons to be learned from the process by which the SEC procured, migrated to, and managed its data centers. We believe it is important context to note that despite the particular cost increases discussed in the report pertaining to our Data Center 1 in (b)(7)(E), the costs for that data center are still below those for our previous data center and still remain comparable to our second data center, which is a near mirror image of Data Center 1. Nevertheless, SEC management concurs with the deficiencies noted in the draft report and intends to work swiftly and diligently to address them.

A response to each of the recommendations is provided below.

**Recommendation 1**: Conduct comprehensive reviews of the (b)(7)(E) data center moves, requirements gathering efforts, and operations to identify lessons learned.

**Management Response:** Management concurs. OIT will conduct comprehensive reviews of past data center relocations, requirements gathering efforts, and operations to identify lessons learned.

**Recommendation 2**: Obtain an assessment of the (b)(7)(E) data center, performed by qualified internal or external personnel, to determine whether the data center meets current agency requirements, including requirements specified in the contract. If the data center does not meet requirements, take action(s) deemed necessary and appropriate.

**Management Response:** Management concurs. OIT has undertaken an assessment of the (b)(7)(E) data center to determine if it meets SEC requirements. OIT will review the results and if the data center does not meet contractual requirements, take appropriate action.

*We removed all non-public information contained in our recommendations to management and redacted any non-public information management included in its response.

**Recommendation 3:** The Contracting Officer address the (b)(7)(E) issued to (b)(7)(E) on May 6, 2015.

**Management Response:** Management concurs. The Contracting Officer will continue to work with the Office of General Counsel, Office of Information Technology, and contractor to address (b)(7)(E) In particular, management will continue to work with the contractor to address the underlying issue of (b)(7)(E)

**Recommendation 4**: Under the Contracting Officer's oversight, the Contracting Officer's Representatives for the agency's data center contracts validate underlying calculations and quantities for all invoices paid under both contracts as of the date of this report, and resolve any discrepancies identified.

**Management Response:** Management concurs. The CO and CORs will work together to validate all invoices paid to include underlying calculations and quantities under both contracts and resolve identified discrepancies.

**Recommendation 5:** The Contracting Officer and Contracting Officer's Representatives for the agency's data center contracts (a) review their records, including emails and other hard copy and soft copy files, to identify any documents that should have been included in the official data center contract files, and properly file any documents found; (b) establish a process for ensuring the contract files will be properly maintained for the remainder of the contracts, including through the use of the agency's Electronic Filing System; and (c) develop steps the Contracting Officer will undertake to closely monitor the activities of the Contracting Officer's Representatives for the remainder of the contracts, including regular meetings and file reviews, and establish a schedule for accomplishing each step.

**Management Response:** Management concurs. The CO and COR(s) will work together to review the data center(s) contract file records, including emails and other hard copy and soft copy files, to identify any documents that should be included in the contract files. Additionally, the CO and COR will follow established procedures to ensure the contract files are properly maintained for the remainder of the contracts, including the use of the electronic filing system. OA will review existing procedures and develop steps for the Contracting Officer to take to closely monitor the activities of the COR for the remainder of the contracts, including regularly scheduled meetings and file reviews.

**Recommendation 6:** The Contracting Officer and Contracting Officer's Representative for the agency's (b)(7)(E) data center contract (a) validate the need to rent from the contractor power distribution units, and consider purchasing the units instead; and (b) validate all other monthly recurring costs in the contract to determine whether those costs are reasonable, necessary, and in the best interests of the government, including the cost of the kilowatt-per-hour rate increase.

**Management Response**: Management concurs. OA and OIT will review and validate the rental of power distribution units and determine if purchasing the units outright is in the best interest of the government, taking liability risk into account. The CO and COR will also review other recurring costs and reconfirm the previous determination of those prices paid, including prices

paid for power as reasonable, necessary, and in the best interests of the government in accordance with FAR 15.4.

Recommendation 7: The Contracting Officer and Contracting Officer's Representatives for the agency's data center contracts assess all required contract deliverables and, where needed, work with the contractors to establish or clarify expectations for each deliverable's format, content, and timeframe for submission to the agency.

Management Response: Management concurs. OA and OIT have already initiated the process of assessing all required contract deliverables. It is anticipated that the CO and COR will clarify with the contractor the requirements for each needed deliverable's format, content, and timeframe for submission to the agency.

Recommendation 8: The Office of Information Technology ensure assessors use a risk-based or comprehensive approach to data center physical and environmental control assessments that considers prior audits, assessments, and known vulnerabilities.

Management Response: Management concurs. OIT will ensure assessors use a risk-based approach to data center physical and environmental control assessments that considers prior audits, assessment, and known vulnerabilities.

Recommendation 9: The Office of Information Technology develop a plan to timely address the physical and environmental vulnerabilities at the (b)(7)(E) data center identified by our contractor.

Management Response: Management concurs. OIT has begun developing a plan to address the vulnerabilities identified.

Recommendation 10: The Office of Information Technology ensure responsible personnel coordinate with other stakeholders to identify data center vulnerabilities for which a plan of action and milestones should be created, and address existing plan of action and milestones items related to vulnerabilities at the (b)(7)(E) data center.

Management Response: Management concurs. OIT has identified responsible personnel to coordinate with other stakeholders to identify data center vulnerabilities. Creation of a plan of action and milestones is underway to address existing vulnerabilities at the (b)(7)(E) data center.

***

In addition, while not a formal recommendation, the OIG encouraged the Director of OA to conduct a comprehensive review of the SEC's COR Program. OA will undertake a review of contractor performance oversight and documentation, including the Contractor Performance Assessment Reporting System, deliverables, and COR file documentation in order to improve the management of agency contracts. OA will review COR and CO training for areas of improvement specific to understanding roles and responsibilities, including improvements in CO oversight of COR actions and documentation.

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

cc: Vance Cathell, Director, Office of Acquisitions
Pam Dyson, Chief Information Officer, Office of Information Technology

## Major Contributors to the Report

Carrie Fleming, Audit Manager

Kelli Brown-Barnes, Audit Manager

John Dettinger, Lead Auditor

Sumeer Ahluwalia, Auditor

Matthew Fryer, Auditor

Leann Harrier, Assistant Counsel

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

Web: www.reportlineweb.com/sec_oig

Telephone: (877) 442-0854

Fax: (202) 772-9265

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

## Comments and Suggestions

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