U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015

June 2, 2016
Report No. 535

REDACTED FOR PUBLIC RELEASE

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

June 2, 2016

TO: Jeffrey Heslop, Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General

SUBJECT: *Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015,* Report No. 535

Attached is the Office of Inspector General's (OIG) final report detailing the results of our audit of the U.S. Securities and Exchange Commission's (SEC) compliance with the Federal Information Security Modernization Act for Fiscal Year 2015. To improve the SEC's information security program, we urge management to take action on all outstanding recommendations from prior year evaluations and areas of potential risk identified in this report. In addition, the report contains four new recommendations for corrective action that, if fully implemented, should strengthen the SEC's information security posture.

On May 19, 2016, we provided management with a draft of our report for review and comment. In its May 24, 2016, response, management concurred with our recommendations. We have included management's response as Appendix III 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 Office of Information Technology will address the recommendations.

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

Attachment

cc: Mary Jo White, Chair
Andrew Donohue, Chief of Staff, Office of the Chair
Michael Liftik, Deputy Chief of Staff, Office of the Chair
Nathaniel Stankard, Deputy Chief of Staff, Office of the Chair
Michael S. Piwowar, Commissioner
Jaime Klima, Counsel, Office of Commissioner Piwowar

Kara M. Stein, Commissioner
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein
Anne K. Small, General Counsel
Keith Cassidy, Director, Office of Legislative and Intergovernmental Affairs
John J. Nester, Director, Office of Public Affairs
Pamela C. Dyson, Director/Chief Information Officer, Office of Information Technology
Andrew Krug, Associate Director/Chief Information Security Officer, Office of Information Technology
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

Executive Summary

Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015
Report No. 535
June 2, 2016

Why We Did This Audit

The U.S. Securities and Exchange Commission's (SEC or agency) information systems process and store significant amounts of sensitive, nonpublic information including information that is personally identifiable, commercially valuable, and market-sensitive. The SEC's information security program protects the agency from the risk of unauthorized disclosure, modification, use, and disruption of this sensitive, nonpublic information. Without these controls, the agency's ability to accomplish its mission could be inhibited, and privacy laws and regulations that protect such information could be violated. To comply with the Federal Information Security Modernization Act of 2014 (FISMA), the SEC Office of Inspector General, with assistance from a contracting firm, Wingate, Carpenter, and Associates, P.C., assessed the SEC's implementation of FISMA information security requirements.

What We Recommended

To improve the SEC's information security program, we urge management to take action on all outstanding recommendations from prior year evaluations and areas of potential risk identified in this report. We also made four new recommendations that address (a) support for risk-based decisions, (b) OIT Risk Committee functionality, and (c) configuration management baseline rollback capabilities. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action. We redacted sensitive information in this report.

What We Found

The SEC's Office of Information Technology (OIT) has overall management responsibility for the SEC's information technology program, including information security. Since last year, OIT improved in key information security program areas, including implementing personal identity verification to the maximum extent practicable, establishing multi-factor authentication for external systems, and improving identity and access management. However, we found that:

- OIT's risk management program did not effectively monitor risks associated with system authorizations; and
- OIT's configuration management program did not ensure that system owners retained previous information system baseline configurations to support rollback.

These weaknesses existed, in part, because OIT management did not (1) effectively implement the OIT Risk Committee tasked with managing risk from individual information systems, and (2) establish adequate controls to ensure effective and consistent implementation of OIT's risk and configuration management programs.

In addition, OIT had not fully addressed some areas of potential risk identified in prior Federal Information Security Management Act evaluations. Specifically, SEC systems continued to operate without current authorizations; user accounts were not consistently reviewed for proper deactivation or termination; continuous monitoring review procedures were developed, but not consistently implemented; and some policies and procedures remained outdated or inconsistent. As a result, these areas continued to pose potential risk to the agency.

Finally, we identified three other matters of interest related to the agency's information technology environment. Specifically, we determined that the SEC did not always (1) update Business Impact Analyses to reflect major system changes, (2) update contingency planning documents to reflect changes in alternate site locations, or (3) track security awareness training. We encourage OIT management to consider these matters and ensure that sufficient controls exist.

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

TABLE OF CONTENTS

Figures and Tables

Appendices

ABBREVIATIONS

(b) (7)	[redacted]
ATO	authorization to operate
(b) (7)	[redacted]
BIA	Business Impact Analysis
COOP	Continuity of Operations Plan
DHS	U.S. Department of Homeland Security
(b) (7)(E)	[redacted]
(b) (7)	[redacted]
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
(b) (7)	[redacted]

ISCM	Information System Continuous Monitoring
ISCP	Information System Contingency Plan
IT	information technology
(b) (7)(E)	[redacted]
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
POA&M	plan of action and milestones
REV.	Revision
(b) (7)(E)	[redacted]
RMF	risk management framework
SEC or agency	U.S. Securities and Exchange Commission
SECR	SEC Administrative Regulation
(b) (7)(E)	[redacted]
SP	Special Publication
SSP	system security plan

Background and Objective

Background

Federal information security laws establish security controls to prevent unauthorized access to information systems and to protect sensitive, nonpublic information[1] from compromise and unauthorized disclosure.

Federal Information Security Modernization Act of 2014 (FISMA). On December 18, 2014, President Obama signed into law FISMA (Public Law 113-283), which amended the Federal Information Security Management Act of 2002, Title III of the E-Government Act of 2002 (Public Law 107-347). FISMA provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets and a mechanism for oversight of Federal information security programs. FISMA also requires agencies to develop, document, and implement an agency-wide information security program to provide information security for the data and information systems that support the operations and assets of the agency.

In addition, FISMA requires Inspectors General to annually assess the effectiveness of agency information security programs and practices and to report the results to the Office of Management and Budget (OMB) and the U.S. Department of Homeland Security (DHS). This assessment includes testing and assessing the effectiveness of agency information security policies, procedures, and practices and a subset of agency information systems. In support of FISMA's independent evaluation requirements, DHS issued to Inspectors General guidance on FISMA reporting for fiscal year (FY) 2015.[2]

To comply with FISMA, the U.S. Securities and Exchange Commission's (SEC or agency) Office of Inspector General (OIG) with the assistance of a contractor, Wingate, Carpenter, and Associates, P.C., assessed the SEC's implementation of FISMA information security requirements. The results of these efforts supported the OIG's FY 2015 Cyberscope submission to OMB and DHS.[3]

[1] 5 Code of Federal Regulations §2635.703(b), *Standards of Ethical Conduct for Employees of the Executive Branch*, defines "nonpublic information" as "information that the employee gains by reason of Federal employment and that he knows or reasonably should know has not been made available to the general public. It includes information that he knows or reasonably should know . . . [i]s designated as confidential by an agency; or [h]as not actually been disseminated to the general public and is not authorized to be made available to the public on request."

[2] *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics,* Version 1.2; June 19, 2015.

[3] Cyberscope is the platform Chief Information Officers, privacy officers, and Inspectors General must use to submit FISMA reporting requirements. The SEC OIG completed its FY 2015 Cyberscope submission on November 13, 2015.

Other Federal Guidance. OMB has established guidance to minimize the risk of unauthorized access to Federal agencies' information systems. Specifically, OMB Memorandum M-15-01 includes policy guidelines to improve the Federal information security posture, and provides guidance to agencies on complying with FISMA and privacy management reporting requirements.[4] OMB Memorandum M-14-03 further emphasizes ensuring the confidentiality, integrity, and availability of Federal information and information systems.[5]

Also, in furtherance of its statutory responsibilities under FISMA, the National Institute of Standards and Technology (NIST) publishes Federal guidelines specific to information technology (IT) security. NIST Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013), prescribes for information systems or organizations, security controls that are designed to: (1) protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations; and (2) satisfy a set of defined security requirements. NIST organizes the security requirements into 18 security and 8 privacy families of controls.[6]

Additionally, in 2010, NIST issued guidelines for applying a risk management framework (RMF) to Federal information systems.[7] The RMF provides a disciplined and structured process that integrates information security and risk management activities into the system development lifecycle. NIST identified key steps in this process, including security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.

SEC Regulations, Policies, and Procedures. SEC regulations, policies, and procedures also address controls over IT security. The agency's primary IT security policies appear in:

- SEC Administrative Regulation (SECR) 24-04, *Information Technology Security Program,* Rev. 2; August 12, 2015 (SECR 24-04);

[4] OMB Memorandum M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*; October 3, 2014.

[5] OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems;* November 18, 2013.

[6] The 18 security control families are access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

The eight privacy control families are authority and purpose; accountability, audit, and risk management; data quality and integrity; data minimization and retention; individual participation and redress; security; transparency; and use limitation.

[7] NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*; February 2010.

- SEC Office of Information Technology (OIT) 24-04-08-06-FM, *Information Security Controls Manual,* Rev. 2; May 13, 2015 (*Information Security Controls Manual*); and
- *SEC OIT Information Security Compliance Program*, Version 2; May 23, 2014.

SECR 24-04 defines the purpose, structure, requirements, and governance processes for the SEC's agency-wide information security program. SECR 24-04 applies to all SEC employees, contractors, and others who process, store, transmit, or have access to SEC computing resources. The *Information Security Controls Manual* describes how the SEC meets the policy requirements outlined in SECR 24-04. Finally, the SEC's *OIT Information Security Compliance Program* establishes uniform policies, authorities, responsibilities, and procedures for IT security compliance.

Prior OIG Federal Information Security Management Act Evaluations. We closed five of the seven recommendations from our 2014 Federal Information Security Management Act evaluation report[8] because OIT took steps to improve key information security program areas. These steps included: (1) implementing personal identity verification to the maximum extent practicable, (2) establishing multi-factor authentication for external systems, (3) implementing controls to enhance oversight of system authorizations, (4) improving identity and access management; and (5) developing and implementing insider threat training. However, we determined that OIT has not fully addressed certain areas of potential risk identified in prior evaluations. Specifically, some SEC systems continued to operate without current authorizations, user accounts were not consistently reviewed for proper deactivation or termination, continuous monitoring review procedures were not fully implemented, and some policies and procedures remained outdated or inconsistent. These prior year risks are addressed later in this report.

Objective

Our overall objective was to assess the SEC's information security and privacy programs in support of the OIG's response to the *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics* (hereafter referred to as "FY 2015 IG FISMA Reporting Metrics"). As required by FISMA, we assessed the SEC's information security posture based on guidance issued by OMB, DHS, and NIST, including guidance on the following performance areas:

- Configuration Management
- Contingency Planning
- Continuous Monitoring Management
- Contractor Systems

[8] U.S. Securities and Exchange Commission, Office of Inspector General, *Federal Information Security Management Act: Fiscal Year 2014 Evaluation*, Report No. 529; February 5, 2015.

- Identity and Access Management
- Incident Response and Reporting
- Plan of Action and Milestones
- Remote Access Management
- Risk Management
- Security Training

To assess the SEC's compliance with FISMA, we judgmentally selected and reviewed a non-statistical sample of 8 out of 62 FISMA-reportable information systems (or about 13 percent) at the SEC's Headquarters.[9] The systems selected were the (b) (7)(E) [redacted]

Appendices I and II include additional information on our scope and methodology (including sampled systems); review of management controls; prior coverage; and applicable Federal laws and guidance, and SEC regulations, policies, and procedures.

[9] A FISMA-reportable system is an information system that supports the operations and assets of the agency. FISMA requires agencies to implement an agency-wide information security program for such systems.

Results

Opportunities Exist to Improve the SEC's Information Security Program

To prevent the risk of unauthorized access to information systems and compromise of sensitive, nonpublic information, the SEC's OIT established an overarching policy for information security. This policy is generally consistent with applicable Federal laws and guidance. However, we identified needed improvements in the agency's information security practices. Specifically, we found that OIT's risk management program did not effectively monitor risks associated with system authorizations,[10] and OIT's configuration management program did not ensure that system owners retained previous information system baseline configurations to support rollback.[11] These weaknesses existed, in part, because OIT management did not (1) effectively implement the OIT Risk Committee tasked with managing risk from individual information systems, and (2) establish adequate controls to ensure effective and consistent implementation of OIT's risk and configuration management programs. As a result, the SEC is at increased risk of unauthorized disclosure, modification, and use of sensitive, nonpublic information. Furthermore, these weaknesses present potential risks to the availability and functionality of mission-critical information systems.

We also found that OIT had not fully addressed certain areas of potential risk identified in prior Federal Information Security Management Act evaluations. As a result, those areas continued to pose potential risk to the agency.

OIT Risk Management Program Did Not Effectively Monitor Risks Associated With System Authorizations

NIST's SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010) (NIST SP 800-37) identifies "information system authorization" as a key step in the RMF process. According to NIST SP 800-37, this step involves authorizing "information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and

[10] In response to a Government-wide request for information about open and unimplemented Inspectors General recommendations, on April 20, 2016, the SEC OIG reported to Chairman Chaffetz and Ranking Member Cummings that a prior recommendation involving authorizations to operate was one of the open recommendations that the SEC OIG considers to be the most important or urgent.

[11] NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*; August 2011, describes "rollback" as the ability to restore a previous secure and functional version of a system's baseline configuration in the event there are issues with a production release.

the Nation resulting from the operation of the information system and the decision that the risk is acceptable." Furthermore, NIST SP 800-37 states that security authorization decisions are based on the content of the security authorization package and, where appropriate, any inputs received from key organizational officials.

Security Authorization Package. The security authorization package provides relevant information on the security state of the information system, including the ongoing effectiveness of the security controls employed within or inherited by the system. According to NIST SP 800-37, a security authorization package contains the following key documents, which Table 1 describes: (1) system security plan (SSP), (2) security assessment report, and (3) plan of action and milestones (POA&M).

Table 1. Security Authorization Package Key Documents

Key Document	Description of Key Document
SSP	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
Security Assessment Report	A report on the results of an assessment of the security controls in an information system and its environment of operation that determines the extent that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.
POA&M	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Source: OIG-generated from NIST SP 800-37 and SP 800-53 definitions.

NIST SP 800-37 further states that providing orderly, disciplined, and timely updates to the SSP, security assessment report, and POA&Ms on an ongoing basis supports the concept of near real-time risk management and ongoing authorization.

The SEC's *OIT Information Security Compliance Program*, in part, establishes the uniform policies, authorities, responsibilities, and procedures for IT security compliance defined in SEC and Federal requirements. Similar to NIST guidance, the SEC's policy states that (1) the security authorization package typically includes the SSP, Risk Assessment Summary Report (that is, security assessment report), and POA&M; and (2) risk assessment activities must be reviewed and updated throughout the authorization period. Specifically, the SEC's policy states "the Information System Owner and Information Owner for each system, with the assistance of the Information Security Group, are responsible for ensuring the SSP is prepared, approved, implemented, monitored for effectiveness, reported upon throughout its life cycle, and updated as needed, at least annually."

Despite these requirements, we found the SSP for one of the eight systems we reviewed—(b) (7)(E)—had not been updated since (b) (7)(E). Furthermore, SSPs for three of the eight systems we reviewed—(b) (7)(E) [redacted]—did not include the most recent revision of security and privacy controls issued by NIST in April 2013.[12] Finally, although the SSPs for all the systems we reviewed stated security assessments will take place on a 3-year basis, the assessment reports for two of the systems we reviewed—(b) (7)(E) [redacted]—were last prepared in (b) (7)(E) [redacted] and (b) (7)(E) [redacted], respectively.

We also found that the third key component of the security authorization package—POA&Ms—were generally conducted in accordance with NIST, OMB, and SEC policy. However, all eight of the systems we reviewed had open POA&Ms that exceeded their milestone dates. (A similar observation was documented in last year's Federal Information Security Management Act evaluation under "Other Matters of Interest.")[13] Although OIT has a process for formally accepting the risk of POA&Ms that the agency cannot close, system owners did not consistently use this process. For example, system owner representatives for both (b) (7)(E) [redacted] and (b) (7)(E) [redacted] stated they were not taking efforts to close POA&Ms from 2010 because the SEC was in the process of replacing these systems. When justifying POA&Ms open past their milestone dates, OIT management stated it keeps POA&Ms open as "implicit risk acceptance" to maintain visibility on the vulnerability within the SEC's POA&M tracking system. According to OMB, "a POA&M permits agency officials and oversight authorities to identify when documented corrective actions are both timely and untimely. In either circumstance, the POA&M has served its intended purpose."[14] Nevertheless, the practice of not formally documenting the acceptance of risk or resolving open POA&M items through timely closure leads to extended risk exposure to the systems.

Authorizing officials use information in the SSP, security assessment report, and POA&M to make risk-based authorization decisions. If this information is not current, it could negatively impact officials' ability to make sound authorization decisions.

Authorization to Operate (ATO). SECR 24-04 defines the purpose, structure, requirements, and governance processes for the SEC's agency-wide information security program. Consistent with NIST, the regulation states that the ATO is "the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept any residual risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation." Moreover, SECR 24-04 states that the system security assessment and authorization process is essential to ensuring system compliance with security controls throughout the system lifecycle.

[12] According to NIST SP 800-53, modifications to policies and procedures resulting from the NIST revision are made in conjunction with established review cycles.

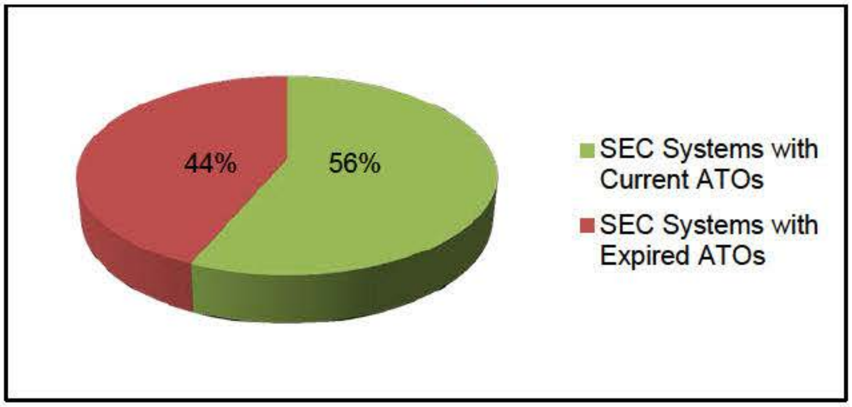
[13] U.S. Securities and Exchange Commission, Office of Inspector General, *Federal Information Security Management Act: Fiscal Year 2014 Evaluation*, Report No. 529; February 5, 2015.

[14] OMB Memorandum 14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*; November 18, 2013.

Although the SEC has adopted and implemented procedures for authorizing systems to operate, we determined that two of the eight systems we reviewed—[redacted] and [redacted]—were operating without current authorizations. Each of the individual SSPs reviewed from our sample included a statement similar to the following: "this authorization is for three years unless there is a major change in the system." However, authorizing officials last issued ATOs for [redacted] and [redacted] in [redacted] and [redacted], respectively. This is a repeat finding from last year's Federal Information Security Management Act evaluation, in which three of eight sampled systems were operating with expired ATOs.

Because this is an area of repeated concern, we reviewed the ATO status of the SEC's entire FISMA-reportable system inventory. As Figure 1 shows, we determined that 27 of the agency's 62 systems (or about 44 percent) were operating without current ATOs. The ATOs for these 27 systems expired between December 2011 and May 2015. According to OIT management, limited contractor support dedicated to preparing authorization packages negatively affected the SEC's ability to keep ATOs current. In addition, OIT management stated they are in the process of reducing the number of major applications requiring individual ATOs by reclassifying some applications as minor and consolidating those applications under the general support system or other remaining major applications.

Figure 1. SEC FISMA-Reportable Systems Total Population: Current Versus Expired ATOs



Source: OIG-generated from the SEC's FISMA-reportable system inventory data.

The ATO conveys the final security authorization decision from the authorizing official to the information system owner or common control provider, and other organizational officials, as appropriate. Because OIT has not reassessed the security controls for these 27 systems in accordance with its risk management program, new vulnerabilities could be present. As a result, the systems may have operated with unknown risk to the SEC and could have been exposed to unauthorized disclosure, modification, use, and disruption.

OIT Risk Committee. OIT has adopted a formal information security risk management strategy. The strategy includes information security risks that may "originate from processing SEC information and handling and operating SEC information systems."

Furthermore, the SEC's *Information Security Compliance Program* states that the strategy "is being implemented through regular meetings of the OIT Risk Committee."

According to the SEC's *Information Security Risk Management Strategy*,[15] the Risk Committee's focus includes "ensuring security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from a Commission-wide perspective with regard to the overall strategic goals and objectives of the SEC in carrying out its missions and business functions." The charter for the Risk Committee states its mission is to inform risk-based decision-making and investment priorities through effective operational security risk management.[16] Risk Committee membership comprises four voting members and two non-voting members. The voting members include the Chief Information Security Officer (who chairs the committee), Chief Information Officer, Chief Technology Officer, and Solutions Delivery Group Associate Director. Risk Committee responsibilities outlined in the committee's charter include, but are not limited to, the following:

- overseeing the development, maintenance, and continuous improvement of a robust risk management governance structure, strategy, and processes for dispositioning of critical security risk;
- prioritizing risk activity based on exposure, urgency, and importance of affected processes or systems, and available resources; and
- maintaining awareness of operational activities across the disparate review boards and committees, resulting audit and assessment findings, emerging threats, and identified weaknesses or vulnerabilities.

According to its charter, the Risk Committee will meet monthly, and monthly meeting agendas will revolve around risk posture trending, such as the "effectiveness of risk management activities, inclusive of corrective action plans and awareness." In addition, the charter states that the Risk Committee supports the SEC's multi-tiered enterprise risk framework, has "direct responsibility for security risk management activities at the information system level," and "ensures that identified risk with adverse impact potential at an organizational level or mission/business process level is properly coordinated with the Office of Operational Risk Management."

Nevertheless, we determined the Risk Committee is not functioning effectively in the following respects:

- As of the date of this report, two of the four voting positions on the Risk Committee are vacant without acting personnel appointed. The Chief Technology Officer position has been vacant for more than a year, and the Solutions Delivery Group Associate Director position has been vacant since May

[15] *SEC OIT Information Security Risk Management Strategy*, Version 18; March 2013.

[16] *SEC OIT Risk Committee Charter*; May 5, 2015.

2015. Furthermore, before being filled in November 2015, the Chief Information Security Officer position (also a voting position) was vacant for about 5 months.

- The Risk Committee is charged by its charter to meet every month, yet (as of the date of this report) it has had no scheduled meetings since March 2015. Therefore, implementation of the SEC's information security risk management strategy through "regular meetings of the OIT Risk Committee" did not consistently occur in 2015 and almost half of 2016.

As a result, the OIT Risk Committee was limited in its ability to manage the SEC's risk from individual information systems, including those resulting from expired ATOs, outdated key security authorization documents, and open POAMs.

OIT Did Not Ensure Retention of Previous Information System Baseline Configurations To Support Rollback

According to NIST SP 800-53, baseline configurations are documented, formally reviewed, and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. NIST SP 800-53 further states that maintaining baseline configurations requires creating new baselines as organizational information systems change over time.

In addition, according to NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems* (dated August 2011), as changes are made to baseline configurations, the new baseline becomes the current version, and the previous baseline is no longer valid but is retained for historical purposes. If there are issues with a production release, retention of previous versions allows for a rollback or restoration to a previous secure and functional version of the baseline configuration. NIST SP 800-128 also states that archiving previous baseline configurations is useful for incident response and traceability support during formal audits.

The SEC's *Information Security Controls Manual* states that "the Information Security Office, in coordination with OIT shall develop, document, and maintain, under configuration control, a current baseline configuration for information systems and constituent components." According to the Manual, OIT shall retain for moderate-impact systems the two most recent versions of baseline configurations to support rollback. Additionally, the SSPs for the majority of systems we reviewed included this control enhancement. Table 2 shows the rollback controls and their respective implementation status as reported in the SSPs for each of the systems included in our sample.

Table 2. SSP Configuration Rollback Controls for Sampled Systems

System	System Impact Category	Rollback Control as Reported in SSP	Control Status as Reported in SSP
(b)	[redacted]	The organization retains two immediate previous versions of baseline configurations to support rollback.	In Place
(b) (7)	[redacted]	The organization retains older versions of baseline configurations as deemed necessary to support rollback.	No Status
(b) (7)	[redacted]	The organization retains two immediate previous versions of baseline configurations to support rollback.	In Place
(b) (7)	[redacted]	The organization retains two immediate previous versions of baseline configurations to support rollback.	In Place
(b) (7)	[redacted]	The organization retains two immediate previous versions of baseline configurations to support rollback.	In Place
(b) (7)	[redacted]	The organization retains older versions of baseline configurations as deemed necessary to support rollback.	In Place
[redacted]	[redacted]	(b) (7)(E)	[redacted]
(b)	[redacted]	The organization retains older versions of baseline configurations as deemed necessary to support rollback.	Implemented

Source: OIG-generated based on information from sampled SSPs.

Despite NIST guidance, SEC policy, and statements in SSPs that rollback controls were in place for the majority of the systems we reviewed, during our interview with OIT management, management stated that having two previous versions of systems' baseline configurations is not required because any changes to production systems are tested and approved before deployment. Moreover, we canvassed the system owners for the systems we reviewed to determine whether the system owners retained previous versions of baseline configurations. Based on feedback from the system owners, we determined that two of the seven moderate-impact systems in our sample—(b) and (b) (7)—did not have a previous baseline configuration version. (b) (7)(E)

The SEC's draft *Configuration Management Plan*[17] addresses configuration management processes, methods, standards, and procedures. According to the draft plan, configuration management activities are planned to address objectives such as maintaining a status history of baselines and changes and restoring earlier baselines as

[17] SEC Draft Operating Procedure 24-03.01.02.01.T01 (1.2), *Configuration Management Plan*.

needed. These activities reflect the SEC's awareness of the need for rollback capabilities. However, the proposed *Configuration Management Plan* has not been approved by OIT management. Similarly, the SEC's *IT Security Baseline Configuration Management Handbook*[18]—developed by OIT to provide configuration management guidance in support of the SEC's IT security program—remained in draft form. Without this guidance in place, OIT was limited in its ability to consistently apply its rollback requirements.

We conclude that the SEC's configuration management program did not ensure that system owners retained previous versions of baseline configurations in accordance with NIST guidelines, SEC policy, and individual SSPs. This negatively impacts the agency's ability to rollback to an operational baseline if necessary, which may result in a loss of assets and an inability to provide accurate, complete, and timely information essential to the SEC's mission if system rollback is necessary.

OIT Had Not Addressed Some Potential Risks Identified in Prior Federal Information Security Management Act Evaluations

OIT had not addressed a number of potential risks identified in prior Federal Information Security Management Act evaluations. As a result, (1) FISMA-reportable systems continued to operate without current authorizations; (2) user accounts were not consistently reviewed for proper deactivation or termination; (3) continuous monitoring review procedures were not fully implemented; and (4) although OIT has made progress in revising policies identified as outdated in the FY 2014 Federal Information Security Management Act evaluation, some policies were still outdated. Consequently, these areas continued to pose potential risk to the agency.

Systems Continued to Operate Without Current ATOs. We determined that two of three production systems that were found not to have current authorizations during the FY 2014 Federal Information Security Management Act evaluation continued to operate without ATOs. Also, as previously discussed, we found that 27 of the SEC's 62 FISMA-reportable systems (or about 44 percent) were operating with expired ATOs during FY 2015, increasing the likelihood that those systems pose unknown risks to the agency.

Improper Review of User Accounts. As reported in the OIG's FY 2013 and FY 2014 Federal Information Security Management Act evaluations, OIT did not adequately review user accounts in accordance with NIST guidelines[19] and SEC policy[20] (b) (7)(E) [redacted] (b) (7)(E)

During our FY 2015 FISMA review of the SEC's security awareness training program, we judgmentally selected a non-statistical sample of SEC users with network accounts to determine whether users completed security training in accordance with SEC policy.

[18] SEC Draft Branch Owned Document 24-04.04.X, *IT Security Baseline Configuration Management Handbook*.

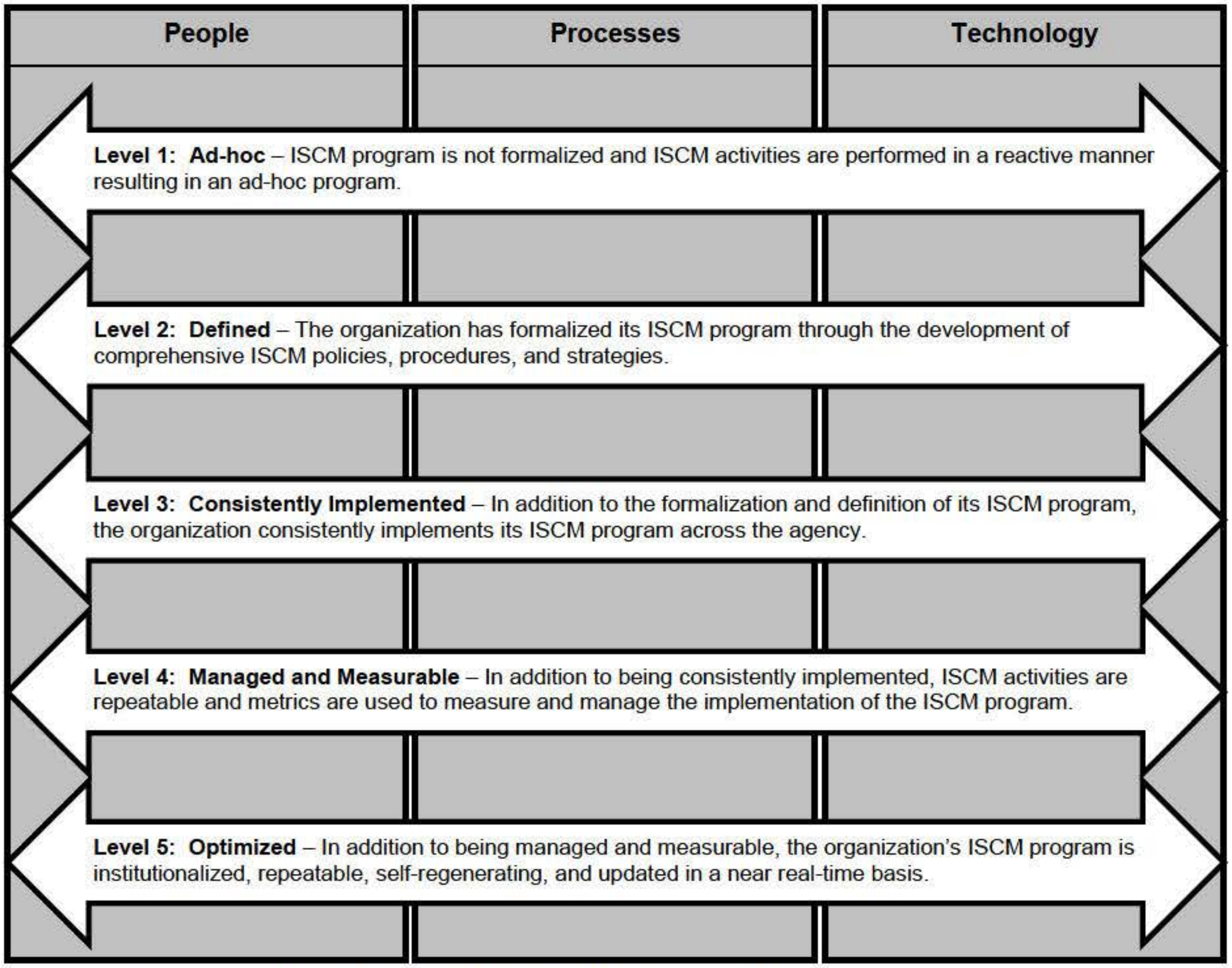
[19] NIST SP 800-53.

[20] SEC 24-04-08-06-FM, AC-2 Access Management.

Consequently, we identified (b) (7)(E) associated with former SEC personnel who had separated (b) (7)(E). Although the sample results cannot be projected to the population, this issue warrants OIT's attention as current controls allowed user accounts to remain more than (b) (7)(E) after the individuals left the agency. (See also the "Other Matters of Interest" section of this report.)

Continuous Monitoring Review Procedures Not Fully Implemented. As previously reported in the OIG's FY 2012, 2013, and 2014 Federal Information Security Management Act evaluations, OIT developed an information system continuous monitoring (ISCM) strategy in accordance with Federal standards, but had not fully implemented it. For FY 2015, the IT Committee of the Council of the Inspectors General on Integrity and Efficiency, in coordination with DHS, OMB, and other stakeholders, developed an ISCM maturity model for use during Inspector Generals' annual reviews. As Figure 2 shows, the maturity model measures an agency's ISCM program across three domains: people, processes, and technology.

Figure 2. ISCM Maturity Model



People | Processes | Technology

Level 1: Ad-hoc – ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program.

Level 2: Defined – The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies.

Level 3: Consistently Implemented – In addition to the formalization and definition of its ISCM program, the organization consistently implements its ISCM program across the agency.

Level 4: Managed and Measurable – In addition to being consistently implemented, ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program.

Level 5: Optimized – In addition to being managed and measurable, the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis.

Source: OIG-generated based on FY 2015 IG FISMA Reporting Metrics.

Based on input from OIT management, we assessed the SEC's ISCM on each of the three domains as follows:

- People - The SEC had, with varying degrees of consistent implementation, (1) defined and communicated responsibilities to ISCM stakeholders; (2) assessed skills, knowledge, and resources needed to implement an ISCM program; (3) defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions; and (4) defined how it will integrate ISCM activities. These attributes correspond to Maturity Level 2 – "Defined."

- Processes - The SEC had, with varying degrees of consistent implementation, (1) defined ISCM processes; (2) defined performance measures; and (3) defined processes for capturing lessons learned. These attributes correspond to Maturity Level 2 – "Defined."

- Technology - The SEC had, with varying degrees of consistent implementation, (1) identified and defined the ISCM technologies it plans to utilize; and (2) defined how it will use automation for inventory, authorized devices/software, and configurations. These attributes correspond to Maturity Level 2 – "Defined."

Therefore, we assessed the SEC's overall ISCM program as Maturity Level 2 – "Defined," meaning the organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with requirements and guidelines; however, ISCM policies, procedures, and strategies were not consistently implemented organization-wide. This assessment is generally consistent with prior year findings.

According to NIST SP 800-37, the implementation of a robust continuous monitoring program allows an organization to understand the security state of the information system over time and to maintain the initial security authorization in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business functions. For the SEC to increase the maturity and effectiveness of its ISCM program, efforts are needed to ensure consistent implementation.

Outdated Procedures and Inconsistent Policy. As previously reported in the OIG's Federal Information Security Management Act evaluations for FY 2011 through FY 2014, OIT had not updated all its security procedures in accordance with NIST guidelines[21] and its own policies.[22] Although OIT made progress in updating its policies and procedures, we still found outdated documents. For example:

- Implementing Instruction 24-04.03.01 (01.0), *IT Security Awareness and Training Program,* (dated December 29, 2005). The instruction states "this policy is effective beginning December 29, 2005. The anticipated review date is one year

[21] NIST SP 800-53.

[22] Revision frequencies are defined within each policy and procedure document.

from the date of approval." The instruction states the OIT Security Group has developed an IT Security Awareness Training and Awareness Program that adheres to the requirements of the Federal Information Security Management Act. However, OIT did not update the instruction when the NIST guidance prescribed by the Federal Information Security Management Act was revised. For example, the instruction did not include insider threat awareness training considerations included in the most recent NIST SP 800-53 update.

- Operating Procedure 24-04.06.03.02 (01.0), *Security Configuration of Remote Access*, (dated December 30, 2005). The procedure states, "This policy is effective beginning December 30, 2005. The anticipated review date is one year from date of approval." The procedure identifies (b) (7)(E) [redacted] technical standards "used as guidelines for implementing remote access devices at the SEC." The (b) (7)(E) [redacted] updates its "technical guidance to 'lock down' information systems/software that might otherwise be vulnerable to a malicious computer attack." (b) (7)(E) [redacted]

Furthermore, the SEC's *Information Security Controls Manual* states "Procedures shall be developed, documented, and disseminated, in conjunction with this policy, as necessary to facilitate the implementation of the personnel security policy and associated personnel security controls. Revisions shall occur in accordance with the schedule noted in Section 3.1.1." However, the Manual does not include a "Section 3.1.1" or the revision schedule it references. Because of these outdated or inconsistent policies and procedures, OIT staff may not have had adequate guidance to ensure management's expectations were met and current NIST standards were followed.

OIT Management Did Not Establish Adequate Information Security Controls

The weaknesses we observed existed, in part, because OIT management did not (1) effectively implement the OIT Risk Committee tasked with managing risk from individual information systems, and (2) establish adequate controls to ensure effective and consistent implementation of the SEC's risk and security configuration management programs. In addition, OIT had not fully addressed certain areas of potential risk identified in prior Federal Information Security Management Act evaluations. Implementing our recommended corrective actions will help minimize the risk of unauthorized disclosure, modification, use, and disruption of the SEC's sensitive, nonpublic information which could inhibit the agency's ability to accomplish its mission, as well as violate privacy laws and regulations that protect such information.

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

To improve the SEC's information security program, OIT should take steps to immediately address the outstanding recommendations from prior year Federal

Information Security Management Act evaluations. In addition, the SEC should implement the following new recommendations:

Recommendation 1: The Office of Information Technology should resolve through timely mitigation and closure open plan of action and milestone items for the systems in our sample. In situations where the Office of Information Technology does not intend to close a plan of action and milestone, the Office of Information Technology should formally document risk acceptance.

> **Management's Response.** The Office of Information Technology concurred with the recommendation. The Office of Information Technology has taken action to consolidate all plan of action and milestones into a centralized capability to enhance the management and tracking of all activity related to weakness remediation. A component of this consolidation includes completing a validation to include a review of milestones and supporting artifacts and materials, and documentation of formal risk acceptance where appropriate.
>
> **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: The Office of Information Technology should update its Risk Committee charter to address changes in committee composition when voting member vacancies occur.

> **Management's Response.** The Office of Information Technology concurred with the recommendation. The Office of Information Technology will take action to update the Member Composition section of the Office of Information Technology Risk Committee Charter to ensure adequate representation in all Committee meetings.
>
> **OIG's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 3: The Office of Information Technology should ensure that the Risk Committee meets in accordance with its charter to facilitate its mission to inform risk-based decision-making and investment priorities through effective operational security risk management.

> **Management's Response.** The Office of Information Technology concurred with the recommendation. The Office of Information Technology will ensure the Risk Committee meets at least monthly in accordance with the Office of Information Technology Risk Committee Charter.
>
> **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: The Office of Information Technology should (a) approve and distribute its configuration management plan that supports rollback; and (b) implement and follow a set of standard configuration management tools for maintaining previous versions of baseline configurations.

Management's Response. The Office of Information Technology concurred with the recommendation. The Office of Information Technology will take action to finalize and disseminate its Configuration Management Operating Procedure and IT Security Baseline Configuration Management Handbook. The Office of Information Technology will also take action to develop a capability to maintain a status history of system baselines and changes and will document associated control enhancements in the Securities and Exchange Commission Information Security Controls Manual and all applicable system security plans.

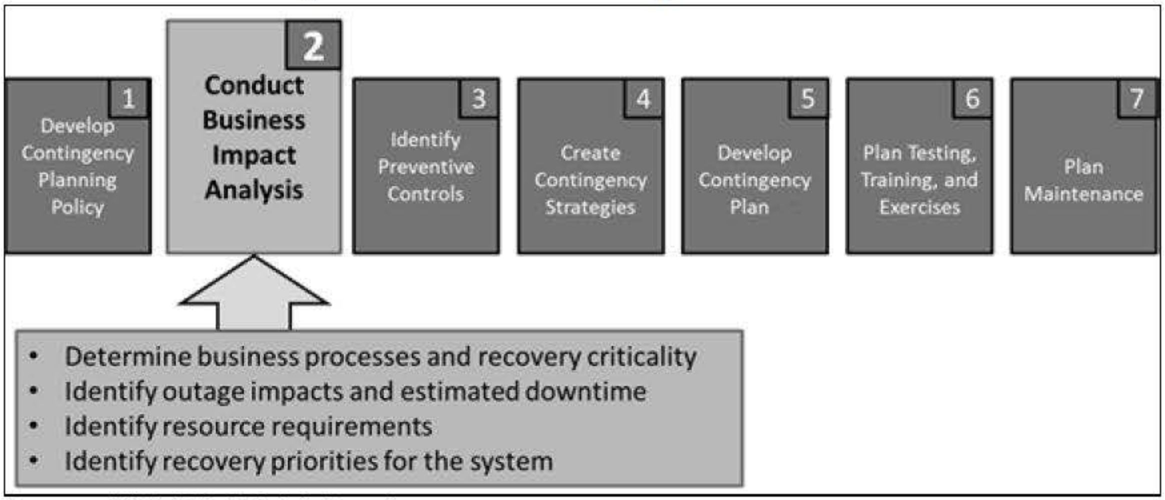
OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Other Matters of Interest

During our audit, we identified three other matters of interest related to the agency's IT environment. We encourage OIT management to consider these matters and take actions to ensure that sufficient controls exist.

OIT Did Not Update Some Business Impact Analyses to Reflect Major System Changes. NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010) identifies a seven-step process to develop and maintain effective Information System Contingency Plans (ISCP). Figure 3 depicts the seven steps.

Figure 3. NIST Seven-Step ISCP Process


1
Develop Contingency Planning Policy
2
Conduct Business Impact Analysis
3
Identify Preventive Controls
4
Create Contingency Strategies
5
Develop Contingency Plan
6
Plan Testing, Training, and Exercises
7
Plan Maintenance
• Determine business processes and recovery criticality
• Identify outage impacts and estimated downtime
• Identify resource requirements
• Identify recovery priorities for the system

Source: NIST SP 800-34, Rev. 1.

NIST describes the second step in this process, "Conduct Business Impact Analysis" (BIA), as "a key step in implementing the [Contingency Planning] controls in NIST SP 800-53, and in the contingency planning process overall." The BIA results determine how critical the system in question is to supported mission/business processes, what impact the loss of the system could have on the organization, and the system recovery time objective. Furthermore, NIST states when a significant change occurs to a system or within the organization, the BIA should be updated with the new information to identify new contingency requirements or priorities.

Similar to NIST guidance, SEC policy states that the BIA is an essential component of the agency's business continuity management program. Specifically, SEC Implementing Instruction 24-04.09.01 (02.0), *Business Impact Analysis* (August 22, 2011) states that "results from the BIA are incorporated into the analysis and strategy formulated during the [business continuity management] program development process, and serve as the primary support in creating contingency plans." Furthermore, the implementing instruction states "when the information system undergoes major revision and at regular intervals in the lifecycle of the completed system, the BIA is revisited for continued accuracy."

We reviewed BIAs for the eight systems included in our sample. As Table 3 shows, we determined that most of the BIAs were last updated more than 5 years ago. During this time, system documentation indicates that the SEC made major changes to at least two of the reviewed systems. For example, (b) (7)(E) [redacted]

Table 3. Sampled Systems' BIA Report Dates

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

Source: OIG-generated based on sample systems' BIAs

To ensure that BIAs reflect the present systems and organization in support of adequate contingency planning, OIT should consider reviewing and updating the BIAs for all systems in the SEC's inventory.

The SEC Did Not Update All Contingency Planning Documents To Include Current Alternate Site Locations. The SEC's Continuity of Operations Plan (COOP)[23] establishes procedures to sustain the agency when standard operations are not feasible. The COOP states "while the severity and consequences of an emergency cannot be predicted, effective contingency planning can minimize the impact on the SEC's missions, personnel, and facilities." One of the objectives of the COOP includes "ensuring continuity facilities are prepared to carry out essential actions." During our audit, we found that the alternate site operations center detailed in the plan (including risk assessment, maps, and driving directions) was not current as of October 2013. On May 2, 2016, subsequent to the conclusion of our fieldwork and Cyberscope reporting, agency personnel provided the OIG with an updated COOP.[24] The updated plan addressed the matters related to the alternate site operations center. However, the ISCP for one of the systems we reviewed is still outdated and does not include new recovery site locations. (b) (7)(E) [redacted]

[23] SEC Continuity of Operations Plan, Version 1.1; March 27, 2013.

[24] U.S. SEC Continuity of Operations Plan, Version 3.0; April 2016.

(b) (7)(E) [redacted] To ensure the effectiveness of the SEC's contingency planning, OIT should consider reviewing contingency planning documents and updating alternate site locations and information as appropriate.

OIT Did Not Fully Track IT Security Awareness Training. In accordance with NIST SP 800-53, the SEC's *Information Security Controls Manual* states that all personnel who have access to SEC information systems—including employees, interns, and contractors—are required to complete information security awareness training and receive a briefing on SEC information system user agreements. In addition, the Manual states that the OIT's Information Security Office shall (1) document and monitor individual information system security training activities, including basic security awareness training and specific information system security training; and (2) retain individual training records. Finally, the Manual requires users to complete information security awareness training annually.

During our review of the SEC's IT security awareness training program, we judgmentally selected a non-statistical sample of 616 out of 6,159 SEC users with Active Directory accounts as of June 10, 2015, to determine whether users completed security awareness training in accordance with SEC policy. We determined that 3 of the 616 users reviewed had not taken required security awareness training during the year. In addition, we determined that two of the systems we reviewed—(b) (7)(E) [redacted]—had open POA&M items related to contractors not receiving or having evidence of completing annual security training. Based on the information reviewed, the majority of SEC personnel received required security awareness training. However, OIT should consider enhancing tracking controls to ensure all personnel meet these requirements.

Appendix I. Scope and Methodology

We conducted this performance audit from June 2015 through June 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope. Our overall objective was to assess the SEC's information security and privacy programs and respond to the *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*. As required by FISMA, we assessed the SEC's information security posture based on guidance issued by OMB, DHS, and NIST.

The audit covered the period between October 1, 2014, and September 30, 2015, and addressed the following 10 areas specified in the DHS's reporting instructions for FY 2015:

1. Configuration Management
2. Contingency Planning
3. Continuous Monitoring Management
4. Contractor Systems
5. Identity and Access Management
6. Incident Response and Reporting
7. Plan of Action and Milestones
8. Remote Access Management
9. Risk Management
10. Security Training

Methodology. We conducted a limited-scope review of the SEC's information security posture. Specifically, to assess system security controls, we reviewed the security assessment packages for a non-statistical, judgmentally selected sample of 8 of the SEC's 62 FISMA-reportable information systems (or about 13 percent). The sample consisted of the internally-and externally-hosted systems shown in Table 4.[25]

[25] We selected the information systems based on the SEC's system of record, (b) (7)(E) [redacted]. The inventory included 62 major information systems that were FISMA-reportable. We selected samples factoring in: (1) the time since we last selected the system as a FISMA sample item, (2) the system risk categorization, (3) the system's number of open POA&Ms, (4) the system's authorization to operate status, (5) the financial system status, and (6) whether the system is hosted internally or externally.

Table 4. SEC Systems Sampled

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

Source: OIG-generated based on sampled systems' SSPs and BIAs.

We interviewed key personnel, including personnel from the OIT Policy and Compliance Branch and system owner representatives for each system we reviewed. We also examined documents and records applicable to the SEC's information security processes, including memos, security change order requests, and applicable reports.

In addition, while reviewing the SEC's identity and access program and information security training program, we judgmentally selected a non-statistical sample of SEC personnel with network accounts to assess controls related to these programs.

Because sampled items were non-statistical, we did not project our results and conclusions to the total user population or measure overall prevalence.

Types of Evidence. We collected and reviewed the following types of evidence during our fieldwork.

- Testimonial
    - Conducted interviews with OIT and the sampled system owners and/or representatives.
    - Attended a release readiness review presentation on (b) (7)(E) [redacted]
- Documentary
    - Reviewed prior year Federal Information Security Management Act evaluations.
    - Reviewed reports generated from the sampled systems' information security scans.
    - Reviewed reports from (b) (7)(E) [redacted] related to the systems we sampled.
    - Reviewed e-mails from OIT personnel in response to questions regarding FY 2015 IG FISMA Reporting Metrics.
    - Reviewed the Federal laws and guidance, and SEC regulations, policies, and procedures included in Appendix II.

Management Controls. Consistent with our audit objectives, we did not assess OIT's overall management control structure. Instead, we reviewed the SEC's controls specific to the FY 2015 IG FISMA Reporting Metrics. To understand thoroughly OIT's management controls pertaining to its policies, procedures, methods of operation, we relied on information requested from and supplied by OIT staff and information from interviews with OIT personnel.

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

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

We used (b) (7)(E) [redacted], the SEC's governance, risk and compliance tool, as a data source for obtaining documentation and reports related to the sampled systems and FISMA-reportable information systems inventory. We performed data reliability, completeness, and accuracy testing, in part, by comparing computer-processed information to testimonial evidence obtained from system and information owners. As a result of these tests, we determined that the computer-processed data we reviewed was sufficiently reliable to support our conclusions.

Prior Coverage. We reviewed prior year OIG Federal Information Security Management Act reports. The FY 2014 report included seven recommendations for corrective action. As of the date of this report, OIT has implemented five of the seven recommendations. Although OIT is working to address the outstanding recommendations, as we noted in the report, weaknesses still exist.

- *Federal Information Security Management Act: Fiscal Year 2014 Evaluation*, Report No. 529; February 5, 2015.
- *Federal Information Security Management Act: Fiscal Year 2013 Evaluation,* Report No. 522; March 31, 2014.
- *2012 FISMA Executive Summary Report,* Report No. 512; March 29, 2013.

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

Appendix II. Federal Laws and Guidance, and SEC Regulations, Policies, and Procedures

We reviewed the following Federal laws and guidance and SEC regulations, policies, and procedures:

Federal Laws and Guidance:

- Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283.
- E-Government Act of 2002, Pub. L. No. 107-347.
- Standards of Ethical Conduct for Employees of the Executive Branch, 5 Code of Federal Regulations, Part 2635.
- *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics, Version 1.2*; June 19, 2015.
- OMB Circular A-130, Revised, Transmittal Memorandum No. 4, *Management of Federal Information Resources*; November 28, 2000.
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; May 22, 2007.
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*; February 3, 2011.
- OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*; November 18, 2013.
- OMB Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*; November 18, 2013.
- OMB Memorandum M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*; October 3, 2014.
- Homeland Security Presidential Directive 12, *Policies for a Common Identification Standard for Federal Employees and Contractors*; August 27, 2004.
- Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*; February 2004.
- Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*; March 2006.

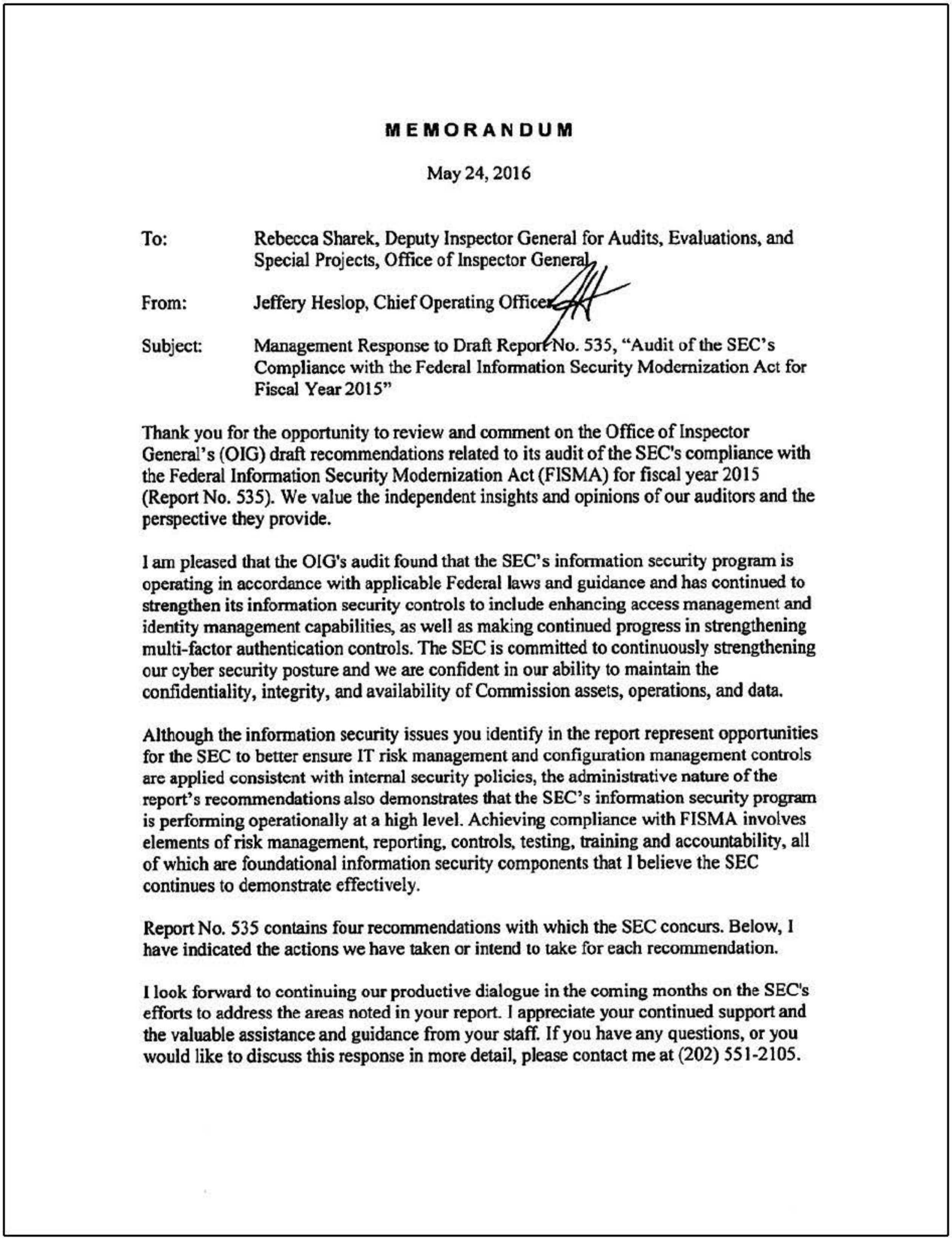
- Federal Information Processing Standards Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; August 2013.
- NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, Rev. 1; February 2006.
- NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Rev. 1; February 2010.
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*; March 2011.
- NIST SP 800-46, *Guide to Enterprise Telework and Remote Access Security: Recommendations of the National Institute of Standards and Technology*, Rev. 1; June 2009.
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*; October 2003.
- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Rev. 4; April 2013.
- NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, Rev. 4; December 2014.
- NIST SP 800-63-2, *Electronic Authentication Guide*; August 2013.
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information System*, August 2011.
- NIST SP 800-137*, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*; September 2011.
- NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*; April 2015.

SEC Regulations, Policies, and Procedures:

- SECR 24-04, *SEC OIT Information Technology Security Program*, Rev. 2; August 12, 2015.
- SECR 24-04, *SEC OIT Information Security Program*, Version 2.0; March 18, 2014.
- SECR 24-08 (01.0), *SEC OIT Management and Protection of Privacy Act Records and other Personally Identifiable Information*; April 14, 2010.
- SECR 24-04.A01, *SEC OIT Rules of the Road*, Version 8.1; May 15, 2015.

- SEC CIO-PD-12-14, Rev. 1, *OIT Property Management Program*; April 2015.
- SEC OIT 24-04-08-06-FM, *Information Security Controls Manual*, Rev. 2; May 13, 2015.
- *SEC OIT Enterprise Disaster Recovery Plan*; December 31, 2014.
- *SEC OIT Information Risk Management Strategy*, Version 18; March 2013.
- *SEC OIT Information Security Compliance Program*, Version 2; May 23, 2014.
- *SEC Information Security Continuous Monitoring Strategy*, Version 1.0; February 2014.
- *SEC OIT Security Policy Framework*, Version 2.0; March 18, 2014.
- SEC Implementing Instruction 24-04.01.03 (02.0), *Information Technology Security Policy Management*; June 9, 2011.
- SEC Implementing Instruction 24-04.03.01 (01.0), *IT Security Awareness and Training Program*; December 29, 2005.
- SEC Implementing Instruction 24-04.04.01 (01.1), *Enterprise Vulnerability Management*; March 25, 2014.
- SEC Implementing Instruction 24-04.06.01 (01.1), *Identification and Authentication*; July 9, 2008.
- SEC Implementing Instruction 24-04.07.01 (01.1), *Computer Security Incident Response Capability*; August 9, 2007.
- SEC Implementing Instruction 24-04.09.01 (02.0), *Business Impact Analysis*; August 22, 2011.
- SEC Operating Procedure 24-03.01.02.01.T01 (1.2), *Configuration Management Plan*; December 21, 2011.
- (b) (7)(E) [redacted]
- (b) (7)(E) [redacted]
- (b) (7)(E) [redacted]
- SEC 24-04-BOD-01, *Information Technology Contingency Planning Handbook*, Version 2; April 2012.

Appendix III. Management Comments



MEMORANDUM

May 24, 2016

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

From: Jeffery Heslop, Chief Operating Officer

Subject: Management Response to Draft Report No. 535, "Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015"

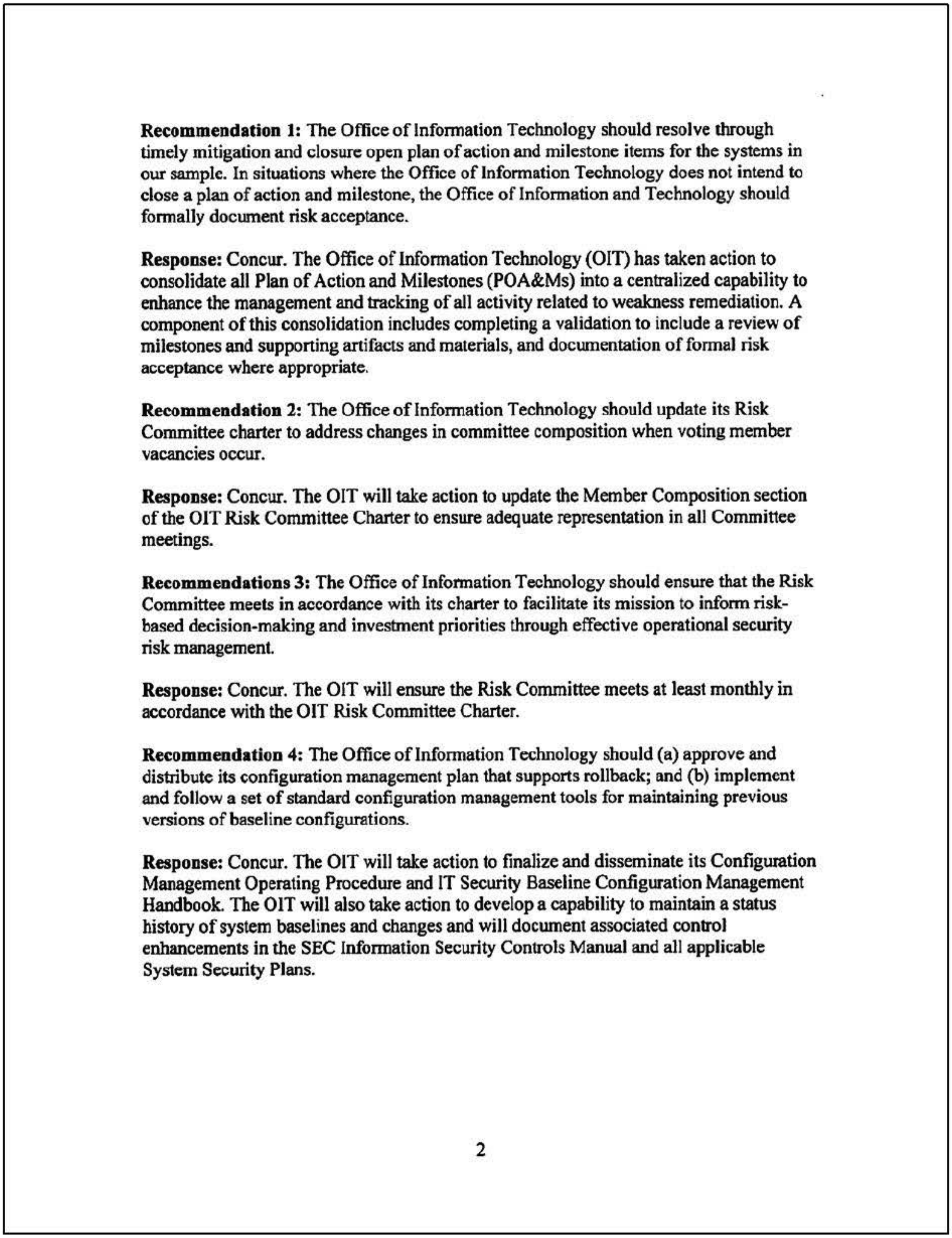
Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft recommendations related to its audit of the SEC's compliance with the Federal Information Security Modernization Act (FISMA) for fiscal year 2015 (Report No. 535). We value the independent insights and opinions of our auditors and the perspective they provide.

I am pleased that the OIG's audit found that the SEC's information security program is operating in accordance with applicable Federal laws and guidance and has continued to strengthen its information security controls to include enhancing access management and identity management capabilities, as well as making continued progress in strengthening multi-factor authentication controls. The SEC is committed to continuously strengthening our cyber security posture and we are confident in our ability to maintain the confidentiality, integrity, and availability of Commission assets, operations, and data.

Although the information security issues you identify in the report represent opportunities for the SEC to better ensure IT risk management and configuration management controls are applied consistent with internal security policies, the administrative nature of the report's recommendations also demonstrates that the SEC's information security program is performing operationally at a high level. Achieving compliance with FISMA involves elements of risk management, reporting, controls, testing, training and accountability, all of which are foundational information security components that I believe the SEC continues to demonstrate effectively.

Report No. 535 contains four recommendations with which the SEC concurs. Below, I have indicated the actions we have taken or intend to take for each recommendation.

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



Recommendation 1: The Office of Information Technology should resolve through timely mitigation and closure open plan of action and milestone items for the systems in our sample. In situations where the Office of Information Technology does not intend to close a plan of action and milestone, the Office of Information and Technology should formally document risk acceptance.

Response: Concur. The Office of Information Technology (OIT) has taken action to consolidate all Plan of Action and Milestones (POA&Ms) into a centralized capability to enhance the management and tracking of all activity related to weakness remediation. A component of this consolidation includes completing a validation to include a review of milestones and supporting artifacts and materials, and documentation of formal risk acceptance where appropriate.

Recommendation 2: The Office of Information Technology should update its Risk Committee charter to address changes in committee composition when voting member vacancies occur.

Response: Concur. The OIT will take action to update the Member Composition section of the OIT Risk Committee Charter to ensure adequate representation in all Committee meetings.

Recommendations 3: The Office of Information Technology should ensure that the Risk Committee meets in accordance with its charter to facilitate its mission to inform risk-based decision-making and investment priorities through effective operational security risk management.

Response: Concur. The OIT will ensure the Risk Committee meets at least monthly in accordance with the OIT Risk Committee Charter.

Recommendation 4: The Office of Information Technology should (a) approve and distribute its configuration management plan that supports rollback; and (b) implement and follow a set of standard configuration management tools for maintaining previous versions of baseline configurations.

Response: Concur. The OIT will take action to finalize and disseminate its Configuration Management Operating Procedure and IT Security Baseline Configuration Management Handbook. The OIT will also take action to develop a capability to maintain a status history of system baselines and changes and will document associated control enhancements in the SEC Information Security Controls Manual and all applicable System Security Plans.

2

Major Contributors to the Report

Wingate, Carpenter, and Associates, P.C.

Kelli Brown-Barnes, Audit Manager

Mike Burger, Lead Auditor

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

Web: www.reportlineweb.com/sec_oig

Telephone: (877) 442-0854

Fax: (202) 772-9265

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

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, please contact Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects at sharekr@sec.gov or call (202) 551-6061. Comments, suggestions, 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.