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 2017

March 30, 2018
Report No. 546

REDACTED FOR PUBLIC RELEASE

OFFICE OF
INSPECTOR GENERAL

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

MEMORANDUM

March 30, 2018

TO: Kenneth Johnson, 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 2017*, Report No. 546

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) compliance with the Federal Information Security Modernization Act for Fiscal Year 2017. To improve the SEC's information security program, we urge management to take action to address areas of potential risk identified in this report. The report contains 20 recommendations for corrective action that, if fully implemented, should strengthen the SEC's information security posture.

On March 9, 2018, we provided management with a draft of our report for review and comment. In its March 27, 2018, response, management concurred with our recommendations. We have included management's response as Appendix II 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
Kara M. Stein, Commissioner
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein
Michael S. Piwowar, Commissioner
Richard Grant, Counsel, Office of Commissioner Piwowar

Robert J. Jackson Jr., Commissioner
Caroline Crenshaw, Counsel, Office of Commissioner Jackson
Prashant Yerramalli, Counsel, Office of Commissioner Jackson
Hester M. Peirce, Commissioner
Jonathan Carr, Counsel, Office of Commissioner Peirce
Robert B. Stebbins, General Counsel
Bryan Wood, Director, Office of Legislative and Intergovernmental Affairs
John J. Nester, Director, Office of Public Affairs
Rick A. Fleming, Investor Advocate
Pamela C. Dyson, Director/Chief Information Officer, Office of Information Technology
Andrew V. Krug, Chief Information Security Officer, Office of Information Technology
Vance Cathell, Director, Office of Acquisitions
Lacey Dingman, Chief Human Capital Officer, Office of Human Resources
Barry Walters, Director, Office of Support Operations
Kelly Gibbs, Assistant Director/Chief of Security Services, Office of Security Services
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 2017
Report No. 546
March 30, 2018

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, non-public 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, non-public 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 assessed the SEC's implementation of FISMA information security requirements based on fiscal year (FY) 2017 guidance issued to Inspectors General (IGs) by the U.S. Department of Homeland Security.

What We Recommended

To improve the SEC's information security program, we made 20 recommendations related to the 7 *FY 2017 IG FISMA Reporting Metrics* assessment domains. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action that is fully responsive to each recommendation. This report contains non-public information about the SEC's information security program. We redacted (deleted) the non-public information to create this public version.

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 FY 2016, OIT improved aspects of the SEC's information security program. Among other actions taken, OIT implemented improved identification and authentication processes, finalized the SEC's information security continuous monitoring strategy, developed and delivered privacy and information security awareness training to SEC employees and contractors (achieving a 99 percent compliance rate), and conducted two incident response exercises and an annual test of the agency's enterprise disaster recovery plan.

Although the SEC strengthened its program since our last FISMA report, we found that the SEC's information security program did not meet the *FY 2017 IG FISMA Reporting Metrics'* definition of "effective." As shown in the following table, we determined that the SEC's maturity level for the five Cybersecurity Framework security functions (identify, protect, detect, respond, and recover) was either Level 2 ("Defined") or Level 3 ("Consistently Implemented"). None of the functions reached Level 4 ("Managed and Measurable"), which the *FY 2017 IG FISMA Reporting Metrics* identified as the level reflective of an effective information security program.

Cybersecurity Framework Security Functions	Maturity Level
Identify	Level 2: Defined
Protect	Level 2: Defined
Detect	Level 2: Defined
Respond	Level 2: Defined
Recover	Level 3: Consistently Implemented

The SEC has further opportunities to ensure that its information security program is effective across the FISMA domains in all five Cybersecurity Framework security functions. Specifically, the agency can strengthen its efforts to implement a comprehensive risk management strategy, improve its hardware and (b) (7)(E) management, and improve its configuration management activities. The SEC also has opportunities to mature its privileged users authentication mechanism, its security training program, its continuous monitoring strategy, and its incident response capabilities. Acting on these opportunities for improvement will help minimize the risk of unauthorized disclosure, modification, use, and disruption of the SEC's sensitive, non-public information, and assist the SEC's information security program reach the next maturity level.

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

TABLE OF CONTENTS

ABBREVIATIONS

DHS	U.S. Department of Homeland Security
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
FY	fiscal year
IG	Inspector General
ISA	Interconnection Security Agreement
ISCM	Information System Continuous Monitoring
IT	information technology
MOU/A	Memorandum of Understanding/Agreement
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
Rev.	Revision
SEC or agency	U.S. Securities and Exchange Commission
SOC	Security Operations Center
SP	Special Publication
SSP	system security plan
US-CERT	United States Computer Emergency Readiness Team

Background and Objectives

Background

On December 18, 2014, the President signed into law the Federal Information Security Modernization Act of 2014 (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 (IGs) 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 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 these requirements, DHS issued to IGs guidance on FISMA reporting for fiscal year (FY) 2017.[1]

As Table 1 illustrates, the *FY 2017 IG FISMA Reporting Metrics* include seven assessment domains, which are aligned with the five information security functions outlined in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework").[2]

Table 1. Cybersecurity Framework Functions Mapped to FY 2017 IG FISMA Reporting Metrics Assessment Domains

Cybersecurity Framework Functions	FY 2017 IG FISMA Assessment Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

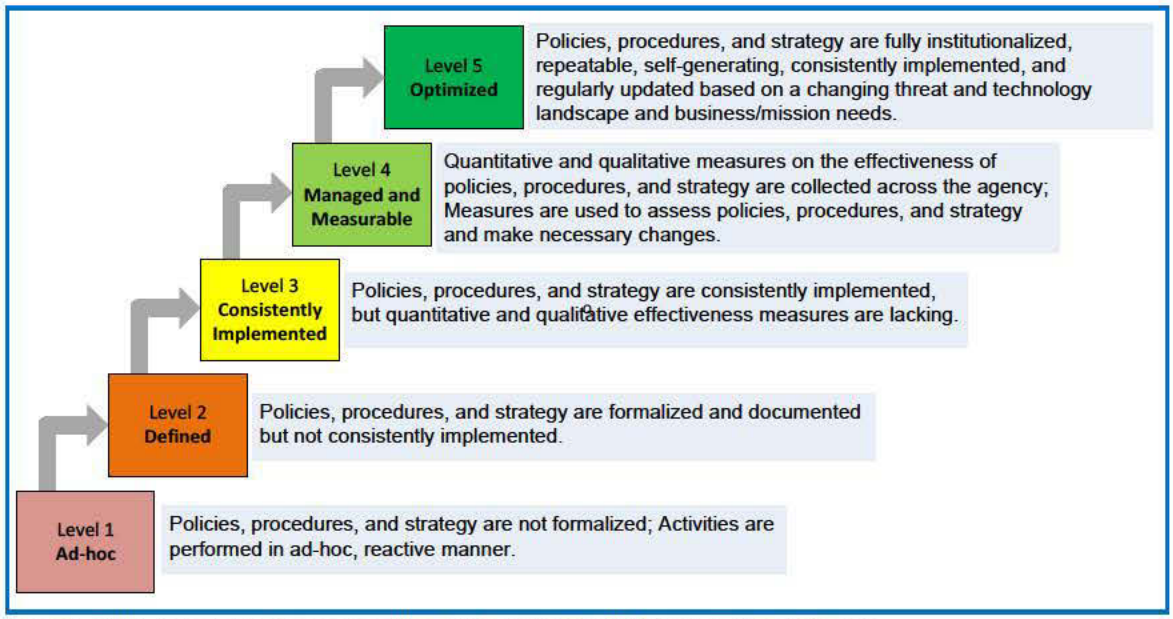
Source: Office of Inspector General (OIG)-generated from the *FY 2017 IG FISMA Reporting Metrics*.

[1] *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, Version 1.0; April 17, 2017 (hereafter referred to as the "*FY 2017 IG FISMA Reporting Metrics*").

[2] The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise, and provides IGs with the guidance for assessing the maturity of controls to address those risks.

Change in Metrics and Assessment Methodology. The IG FISMA Reporting Metrics for FYs 2015 and 2016 required IGs to assess two Cybersecurity Framework functions ("Detect" and "Respond") using a maturity model approach. In contrast, the *FY 2017 IG FISMA Reporting Metrics* require IGs to assess all seven domains included in the five Cybersecurity Framework functions using a maturity model approach. As shown in Figure 1, the foundation levels of the maturity model ensure that agencies develop sound policies and procedures, whereas the advanced levels capture the extent to which agencies institutionalize those policies and procedures.

Figure 1. IG Assessment Maturity Levels



Source: OIG-generated based on the *FY 2017 IG FISMA Reporting Metrics*.

The maturity model also summarizes the status of agencies' information security programs, provides transparency on what has been accomplished and what still needs to be implemented to improve the information security program, and helps ensure consistency across the IGs in their annual FISMA reviews. Within the context of the maturity model, Level 4 ("Managed and Measurable") represents an effective level of security at the domain, function, and overall program level.

To comply with FISMA, we assessed the U.S. Securities and Exchange Commission's (SEC or agency) implementation of FISMA information security requirements in accordance with the *FY 2017 IG FISMA Reporting Metrics*. The results of these efforts supported the OIG's FY 2017 Cyberscope submission to OMB and DHS.[3]

[3] Cyberscope is the platform Chief Information Officers, Privacy Officers, and IGs use to meet FISMA reporting requirements. The SEC OIG completed its FY 2017 Cyberscope submission to DHS and OMB on October 31, 2017.

Responsible Office. The SEC's Office of Information Technology (OIT) has overall management responsibility for the agency's information technology (IT) program, including information security. OIT establishes IT security policies and provides technical support, assistance, direction, and guidance to SEC divisions and offices. The Chief Information Officer directs OIT and is responsible for ensuring compliance with applicable information security requirements. The Chief Information Security Officer, designated by the Chief Information Officer, is responsible, in part, for developing, maintaining, centralizing, and monitoring ongoing adherence to the SEC's Information Security Program Plan and supporting the Chief Information Officer in annual reporting on the effectiveness of the SEC's information security program.

Prior Audits and Evaluations. As of the date of this report, we closed 18 of the 21 recommendations from our FY 2016 FISMA audit[4] because OIT took steps to improve key information security program areas. These steps included: (1) developing security clauses and requirements to incorporate in third party vendor contracts; (2) establishing a policy requiring that access agreements be recertified at a predetermined interval; (3) implementing improved identification and authentication processes; (4) developing and delivering privacy and information security awareness training to SEC employees and contractors (achieving a 99 percent compliance rate); (5) finalizing the SEC's information security continuous monitoring strategy; (6) conducting two incident response exercises; and (7) conducting an annual test of the enterprise disaster recovery plan. We will close the remaining recommendations upon completion and verification of corrective action taken.

Objectives

Our overall objective was to assess the SEC's compliance with FISMA for FY 2017 based on guidance issued by OMB, DHS, and NIST. Specifically, as discussed in the Results section of this report, we assessed the effectiveness of the SEC's information security program for the following seven domains in accordance with the *FY 2017 IG FISMA Reporting Metrics*:

1. Risk Management
2. Configuration Management
3. Identity and Access Management
4. Security Training
5. Information Security Continuous Monitoring
6. Incident Response
7. Contingency Planning

[4] U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Compliance With the Federal Information Security Modernization Act for Fiscal Year 2016*, Report No. 539; March 7, 2017.

To assess the SEC's compliance with FISMA, we judgmentally selected and reviewed a non-statistical sample of 5 major information systems from the agency's May 23, 2017, inventory of 41 FISMA-reportable information systems (or about 12 percent).[5] We also performed other tests and assessments. Appendix I describes our scope and methodology (including sampling), our review of internal controls and computer-processed data, and prior coverage.

[5] A major information system is a system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

Results

Domain #1: Risk Management

Risk management is the ongoing process of identifying, assessing, and responding to risk. Risk management practices include establishing the context for risk-related activities, assessing risk, responding to risk, and monitoring risk over time. NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011 (NIST SP 800-39), states to integrate the risk management process throughout the organization, a three-tiered approach is employed that addresses risk at the following levels: organizational (tier 1), mission/business processes (tier 2), and information systems (tier 3).

We assessed the SEC's risk management program and determined that the program's maturity level is Level 2 ("Defined"), meaning the SEC formalized and documented risk management policies and procedures but did not consistently implement them. Specifically, we determined that the SEC did not:

- (b) (7)(E) (***Information Systems Inventory***);
- Always authorize or document system interconnections using applicable agreements, or review and update system interconnection agreements as required (***System Interconnections***);
- Develop or maintain an accurate or complete inventory of hardware assets connected to the agency's network, or of (b) (7)(E) (***Asset Management***);
- Consistently identify or document the implementation of applicable security controls, perform annual security or risk assessments, or authorize systems to operate in accordance with agency policy (***System Security Assessments and Authorizations***);
- Institutionalize and mature its enterprise architecture program by defining or formalizing a plan to address how the agency's enterprise architecture program management will be integrated with other institutional management disciplines, such as organizational strategic planning, strategic human capital management, performance management, information security management, and capital planning and investment control (***Information Security Architecture***);
- Define and communicate the roles and responsibilities of the risk executive function, and implement a comprehensive risk management strategy (***Risk Management Roles, Responsibilities, and Strategy***);
- Consistently create or update plans of action and milestones (POA&Ms) to address known security weaknesses, or ensure that POA&M data included in internal reports were up-to-date and accurate (***POA&Ms***); and

- Always ensure that IT contracts included certain contracting language defined by OIT (***Contractor Systems Risk Mitigation***).

Each of these areas is discussed further below.

Information Systems Inventory. FISMA requires agencies to develop two information system inventories: an inventory of the agency's major information systems and an inventory of all agency information systems, regardless of categorization.[6] In addition, SEC Administrative Regulation 24-04, *Information Technology Security Program*, Rev. 3, June 29, 2017 (SECR 24-04), states that OIT's Information Security Office maintains a comprehensive inventory of information systems containing SEC data, including external systems operated on behalf of the SEC. According to SECR 24-04, the inventory should include key information for each system such as the system's Federal Information Processing Standards Publication 199 security categorization and the system's authorization status.

Although OIT developed and maintained an inventory of the SEC's major information systems, (b) (7)(E) [redacted]

Although OIT defined and implemented a process to develop and maintain a comprehensive and accurate inventory of major information systems, (b) (7)(E) [redacted]

[6] 44 U.S. Code § 3505(c). There are two paragraphs labeled "(c)" in section 3505 of title 44 of the U.S. Code. One paragraph requires a major information systems inventory, and the other paragraph requires an inventory of all information systems, regardless of categorization. In addition, according to OMB Circular A-130, *Managing Information as a Strategic Resource* (July 2016), all information systems are subject to the requirements of section 3505(c)(2), whether or not they are designated as a major information system.

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

System Interconnections. For a variety of reasons, organizations may choose to interconnect their IT systems. However, interconnecting IT systems can expose the participating organizations to risk. Federal policy requires agencies to establish interconnection agreements. Specifically, Appendix III of OMB Circular A-130, *Managing Information as a Strategic Resource*, July 2016 (OMB A-130), requires agencies to obtain written management authorization before connecting their IT systems to other systems, based on an acceptable level of risk. The written authorization should define the rules of behavior and controls that must be maintained for the system interconnection, and the authorization should be included in the applicable system security plan (SSP). Furthermore, NIST has stated that organizations should document an agreement governing system interconnections and the terms under which the organizations will abide by the agreement, based on a review of all relevant technical, security, and administrative issues.[8] Two documents may be developed: an interconnection security agreement (ISA) and a Memorandum of Understanding/Agreement (MOU/A). The ISA specifies the technical and security requirements of the interconnection, and the MOU/A defines the responsibilities of the participating organizations. Applicable SEC (b) (7)(E) (b) (7)(E) states that the SEC follows NIST guidance as a basis for ISAs, and that SEC ISAs are reviewed and updated when renewed or in accordance with the timeframe specified in each agreement.

Three of the five SEC systems we reviewed were connected to external systems that were operated either by other Federal agencies or by private entities. The three systems were: (b) (7)(E) In addition, to follow up on recommendations from our FY 2016 FISMA audit, we reviewed documentation for two other SEC systems connected to external systems (b) (7)(E) For each of the five systems we reviewed that were connected to external systems, we found that (1) (b) (7)(E) or (2) agreements existed but were outdated. For example, for two systems involving a (b) (7)(E) to commercial entity systems, (b) (7)(E) For another system interconnection, OIT annually reviewed the SEC's (b) (7)(E) but did not update the documents to remove references to an outdated version of NIST SP 800-53 and to OIT guidance that had been rescinded.[9] In another

[8] NIST guidance in this area includes NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002; and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Rev. 4, April 2013 (NIST SP 800-53 Rev. 4).

[9] We noted that the (b) (7)(E) —signed in (b) (7)(E) —referred to Rev. 3 of NIST SP 800-53, which was replaced by Rev. 4 in April 2013. In addition, the (b) (7)(E) referred to OIT's (b) (7)(E) which OIT rescinded and replaced with OIT policy (b) (7)(E)

case, OIT did not review and update the SEC's (b) (7)(E) within the 5-year timeframe specified in the agreement, which was dated (b) (7)(E)

The SEC did not consistently authorize or document the system interconnections we reviewed, in part, because OIT did not define documentation requirements for authorizing system interconnections involving (b) (7)(E). In addition, for most of FY 2017, OIT did not define and implement a process to ensure that (b) (7)(E) documenting system interconnections were timely reviewed and updated. Without effective controls over system interconnections, the SEC risks improper sharing of information and/or ineffective protections over sensitive information. OIT established a process for creating, approving, maintaining, and updating (b) (7)(E) at the end of FY 2017. We will assess the effectiveness of this new process in the FY 2018 assessment of the SEC's information security program.

Asset Management. OMB Circular A-130 requires agencies to ensure that physical devices, software applications, hardware platforms, and systems within the organization are inventoried when obtained and that inventories are updated on an ongoing basis. In addition, NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011 (NIST SP 800-137), states that asset management tools help maintain the inventory of software and hardware within the organization. Also, NIST SP 800-53 Rev. 4 requires organizations to develop and document an inventory of information system components[10] that accurately reflects current information systems, includes all components within the systems' authorization boundaries, and allows for tracking and reporting. According to NIST SP 800-53 Rev. 4, information deemed necessary for effective accountability of information system components includes hardware inventory specifications (such as manufacturer, device type, model, serial number, and physical location); software license information; software version numbers; component owners; and machine names and network addresses for networked components or devices. Finally, OIT's (b) (7)(E) requires SEC information system owners to (1) use SSPs to develop, document, and maintain an inventory of information system components, and (2) annually review each system's SSP, including the information system component inventory contained therein.

Although the SEC implemented a hardware asset inventory management solution and defined processes to develop and maintain a hardware inventory, we found that the SEC's inventory of hardware assets did not accurately and completely reflect the assets connected to the agency's network. For example, the inventory did not include

[10] Information system components include mainframes; workstations; servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name); input/output devices (e.g., scanners, copiers, printers); network components (e.g., firewalls, routers, gateways, voice and data switches, process controllers, operating systems, virtual machines, middleware); and applications.

74 (b) (7)(E) connected to the SEC's network, and contained inaccurate serial numbers for another 275 computers connected to the SEC's network.[11] Also, OIT did not always timely update hardware asset inventory records upon employees' separation from the SEC. Specifically, records showed that 23 of 173 employees (or about 13 percent) who separated from the agency between October 1, 2016, and May 17, 2017, still had computers "in-use."

Moreover, although the SEC is working to develop and, in FY 2018, deploy a centralized (b) (7)(E) management solution, we found that the SEC did not maintain an accurate or complete inventory of (b) (7)(E) . Furthermore, the SSPs for two of the five systems we reviewed (b) (7)(E) contained inaccurate (b) (7)(E) information. Specifically, the (b) (7)(E) information in the SSPs for these two systems referenced (b) (7)(E) no longer used by the SEC and several instances of incorrect (b) (7)(E) Although OIT annually reviewed the SSPs for these two systems, OIT did not ensure that the SSPs contained an accurate inventory of information system components. OIT personnel indicated that they are working to update SSPs for these two systems, including the (b) (7)(E) information contained therein. In addition, since our October 2017 Cyberscope submission, the SEC implemented a new annual system review process requiring information system owners to review and update their systems' hardware and (b) (7)(E) documented in SSPs. We will assess the effectiveness of this new process in the FY 2018 assessment of the SEC's information security program.

These conditions occurred, in part, because OIT did not define corresponding processes. Specifically, OIT did not define processes for developing and maintaining up-to-date inventories that include detailed information necessary for tracking and reporting of (1) hardware assets connected to the organization's network, and (2) (b) (7)(E)

Without accurate and complete inventories of the hardware assets connected to the agency's network and (b) (7)(E) , the SEC may not be able to identify and properly mitigate hardware (b) (7)(E) In addition, the agency may not ensure proper accountability over agency assets and risks paying for unused or underutilized IT equipment or hardware, installed (b) (7)(E)

System Security Assessments and Authorizations. According to NIST SP 800-53 Rev. 4, organizations should document system security controls in SSPs and conduct risk assessments, document risk assessment results, and update risk assessments at an organization-defined frequency. In addition, OIT's (b) (7)(E)

[11] The SEC's hardware asset inventory included over 11,000 computers, including (b) (7)(E) laptops and desktops.

(b) (7)(E) indicates that the SEC maintains a security assessment and authorization process to ensure testing and/or evaluation of the SEC's management, operational, and technical security controls to determine the extent to which the controls are implemented correctly and operating as intended. The security assessment and authorization process provides the authorizing official essential information to make risk-based decisions on whether to authorize operation of an information system.

However, four of the five systems we reviewed were either operating (1) with SSPs that did not identify or document the SEC's implementation of key security controls (b) (7)(E) (2) without having undergone a security assessment or system testing/evaluation for one to four years (b) (7)(E) and/or (3) under an expired authorization to operate for all or part of FY 2017 (b) (7)(E) For example, OIT categorized the (b) (7)(E) system as (b) (7)(E) Moreover, (b) (7)(E) most recent risk or security assessment report and authorization to operate were both dated (b) (7)(E) In addition, (b) (7)(E) was operating under an expired authorization to operate for 3 months in FY 2017.

OIT personnel stated that they experienced a gap in contracted service in FY 2017, and did not have adequate resources to consistently perform some security assessment activities. In addition, OIT personnel stated that they were working with the (b) (7)(E) contractor to update the system's SSP, and that the omissions in the (b) (7)(E) occurred because of an oversight. Nonetheless, failure to assess and/or document system risks and operating systems without current authorizations increases the possibility that the organization may not timely identify and/or address vulnerabilities in its information systems and the environments in which those systems operate.

As previously stated, since our October 2017 Cyberscope submission, the SEC implemented a new annual system review process to ensure that information system owners consistently review and update SSPs and risk assessments. We will assess the effectiveness of this new process in the FY 2018 assessment of the SEC's information security program.

Information Security Architecture. According to OMB A-130, agencies shall develop an enterprise architecture that describes the baseline architecture, target architecture, and a transition plan to get to the target architecture. OMB A-130 further states that the enterprise architecture should incorporate agency plans for significant upgrades, replacements, and disposition of information systems when the systems can no longer effectively support missions or business functions. In addition, NIST SP 800-53 Rev. 4 requires that organizations develop an information security architecture that describes how the information security architecture is integrated into and supports the enterprise architecture. Finally, OIT's (b) (7)(E) states systems' baseline configurations must not conflict with the SEC's enterprise architecture.

The SEC defined an information security architecture and a process to review the security architecture of new hardware and software before introducing systems into the

agency's development environment. However, the SEC did not define or formalize a plan to address how enterprise architecture program management will be integrated with other institutional management disciplines, such as organizational strategic planning, strategic human capital management, performance management, information security management, and capital planning and investment control. In addition, although the enterprise architecture group attends meetings at which IT investment decisions are made, the SEC did not have a process for ensuring IT initiatives undergo an enterprise architecture compliance review before funding. According to the SEC's annual enterprise architecture assessment for FY 2017, although the agency realized some improvements since FY 2016, the SEC has areas to improve to institutionalize and mature its enterprise architecture program.

Failure to establish an enterprise architecture with embedded information security architecture increases the risk that the agency's security processes, systems, and personnel are not aligned with the agency's mission and strategic plan.

Risk Management Roles, Responsibilities, and Strategy. According to NIST SP 800-137, the risk executive function oversees the organization's ISCM strategy and program, facilitates sharing of security-related information, and ensures that risk information is considered for continuous monitoring. NIST SP 800-39 further states organizations should identify external entities with which there is an actual or potential risk relationship, and establish practices for sharing risk-related information with such entities. In addition, the *FY 2017 IG FISMA Reporting Metrics* asked IGs to determine to what degree the agency has defined and communicated the roles and responsibilities of stakeholders involved in risk management, including the roles and responsibilities of "the risk executive function." The *FY 2017 IG FISMA Reporting Metrics* also asked IGs to determine whether agencies use technology to provide a centralized enterprise-wide view of information security risks across the organization. According to NIST SP 800-39, "an integrated, enterprise-wide risk management includes for example consideration of (i) the strategic goals/objectives of organizations; (ii) organizational mission/business functions prioritized as needed; (iii) mission/ business processes; (iv) enterprise and information security architectures; and (v) system development life cycle processes."

The SEC did not clearly define and communicate the roles and responsibilities of certain stakeholders involved in risk management. Specifically, the SEC did not define and communicate the roles and responsibilities of the risk executive function, or implement a comprehensive risk management strategy. In addition, the roles and responsibilities for tier 1 and tier 2 risks were not clearly defined. Also, although the SEC used an enterprise-wide solution (b) (7)(E) to provide a centralized view of program and process-level operating risks, the agency did not identify and define its requirements for an automated solution to provide a centralized enterprise-wide view of information security risks across the organization including, for example, the considerations identified by NIST. In our 2016 FISMA audit report, we recommended that the Office of the Chief Operating Officer, in coordination with OIT, develop a comprehensive risk management strategy in accordance with NIST SP 800-39. The SEC is continuing its efforts to implement this recommendation.

Without a comprehensive risk management strategy, the agency may not ensure that the appropriate assurance levels are achieved for the information systems and system components deployed in the SEC's environment.

POA&Ms. NIST SP 800-53 Rev. 4 requires organizations to develop POA&Ms to document the organization's planned remedial actions, correct weaknesses or deficiencies noted during the assessment of security controls, and reduce or eliminate known system vulnerabilities. NIST SP 800-53 Rev. 4 further states that organizations should update existing POA&Ms at an organization-defined frequency based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. OIT's (b) (7)(E) mirrors these requirements.

We found that OIT defined policies and procedures for using POA&Ms to mitigate security weaknesses. In addition, OIT uses a centralized tool (b) (7)(E) to manage POA&Ms as part of its overall security assessment and authorization process. However, for three of the five systems we reviewed (b) (7)(E) OIT either did not (1) develop POA&Ms in (b) (7)(E), or (2) periodically update POA&Ms to address security weaknesses identified during the systems' FY 2017 security assessments or during continuous monitoring activities. For the remaining two systems (b) (7)(E) OIT adequately implemented POA&Ms in accordance with agency policies and procedures.

We also found that OIT did not ensure that POA&M data included in internal reports were up-to-date and accurate. Specifically, according to reports we generated through (b) (7)(E) there were 467 open POA&Ms in August 2017. These included 150 overdue POA&Ms related to the SEC's general support system, including 7 that were over 2 years overdue and 66 that were over 30 days overdue. However, according to OIT management's internal POA&M status reports, there were no overdue POA&Ms for the general support system.

According to OIT personnel, the SEC did not consistently implement its POA&M activities, in part, because OIT did not have adequate resources to timely complete the activities. OIT personnel stated that they on-boarded a new contractor in (b) (7)(E) to support the management of all system- and application-level POA&Ms, and that, during our audit, they were catching up on documenting POA&Ms in (b) (7)(E)

Given the increasing emphasis on organization-wide risk management across all three tiers, without up-to-date and accurate POA&M information, the agency may not have sufficient information to prioritize risk response actions and ensure consistency with the goals and objectives of the organization.

Contractor Systems Risk Mitigation. NIST SP 800-53 Rev. 4 requires organizations to include specific requirements, descriptions, and criteria, explicitly or by reference, in contracts for information systems, system components, or information system services. In addition, the Federal Acquisition Regulation includes sections/clauses to integrate in

IT-related contracts. NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing,* December 2011, also states that the organization should ensure that all contractual requirements, including privacy and security provisions, are explicitly stated in the service agreement, and that the requirements are endorsed by the cloud provider, where applicable. In addition, OIT's (b) (7)(E) states that OIT defined specific contracting language, such as information security and privacy requirements, material disclosures, Federal Acquisition Regulation clauses, and clauses on protection, detection, and reporting of information.

We found that the SEC defined specific contract language to include in contracts and service level agreements to mitigate and monitor the risks related to contractor systems and services. In addition, the SEC defined processes to ensure that security controls of systems or services provided by contractors or other entities on behalf of the agency meet FISMA requirements, OMB policy, and applicable NIST guidance. However, the SEC did not always ensure that such language was included in IT contracts. Specifically, we reviewed three contracts for IT systems and services. Two of the three contracts were for systems included in our sample (b) (7)(E) and the SEC awarded the contracts in (b) (7)(E), respectively. The SEC awarded the remaining contract for management support services (b) (7)(E) in (b) (7)(E) Based on our review, the contracts did not include all required security clauses specified by OIT. For example, we found that the contracts did not include provisions related to (1) communicating non-public or sensitive information, (2) unauthorized access protection and disaster recovery, (3) IT-related records management requirements, or (4) Federal Risk and Authorization Management Program (FedRAMP)[12] security requirements applicable to cloud services.

SEC contracts lacked provisions intended to address IT security risks because the SEC did not define and implement a process to properly coordinate acquisitions of IT services and products and ensure that OIT-defined security clauses were incorporated into contracts. Personnel from the Office of Acquisitions explained that the contract awarded in (b) (7)(E) that we reviewed did not include the required security clauses because, at the time of contract award, the Office of Acquisitions and the Contracting Officer's Representative were unaware of the extent to which the contractor would be exposed to SEC systems and information. Office of Acquisitions personnel added that they planned to modify the contract by adding the omitted clauses before contractor personnel accessed any SEC systems. Without ensuring that IT contracts include appropriate security clauses, the SEC may lack assurance that contractors are adequately protecting sensitive, non-public SEC information and complying with requirements applicable to Federal systems.

[12] FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

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

To mature the agency's risk management program from Level 2 ("Defined") to Level 3 ("Consistently Implemented"), we recommend that the Office of Information Technology:

Recommendation 1: Define and implement a process that includes clear roles and responsibilities for developing and maintaining a comprehensive and accurate inventory of agency information systems (b) (7)(E) [redacted]

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will (b) (7)(E) [redacted] The Chief Operating Officer further stated that the Office of Information Technology plans to (b) (7)(E) [redacted] Management's complete response is printed in Appendix II.

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: Define and implement a process (b) (7)(E) [redacted]

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will (b) (7)(E) [redacted] Management's complete response is printed in Appendix II.

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: Define and implement a process to develop and maintain up-to-date inventories that include detailed information necessary for tracking and reporting of hardware assets connected to the agency's network, and (b) (7)(E) [redacted]

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will (b) (7)(E) [redacted]

(b) (7)(E) Management's complete response is printed in Appendix II.

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: Perform a comprehensive review of its processes and resource needs to adequately support the agency's security assessment and authorization program (including creating and managing plans of action and milestones) and, based on the results, take corrective action to ensure plans of action and milestones are timely documented, periodically updated, and accurately reflected in internal reports.

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will perform a review to evaluate if current resource levels are sufficient to support the completion and management of security assessments, authorizations, and processes that ensure plans of action and milestones are timely documented, periodically updated, and accurately reflected in internal reports. Management's complete response is printed in Appendix II.

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: (a) Continue efforts to define and formalize a plan addressing how enterprise architecture program management will be integrated with other institutional management disciplines, such as organizational strategic planning, strategic human capital management, performance management, information security management, and capital planning and investment control; and (b) define and implement a process to ensure information technology initiatives undergo an enterprise architecture compliance review before funding.

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will continue refining the SEC's enterprise architecture and define and implement a process designed to ensure information technology initiatives go through enterprise architecture reviews, including application of the (b) (7)(E), prior to funding. The Chief Operating Officer also stated that the Office of Information Technology will continue to engage the SEC business community to see that all information technology decisions and initiatives are governed by the (b) (7)(E), one of the foundational elements of which is architectural compliance. Management's complete response is printed in Appendix II.

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: Continue efforts to implement a comprehensive risk management strategy by (a) clearly defining and communicating roles and responsibilities for tier 1 and tier 2 information security risks and the risk executive function; and (b) identifying and defining requirements for an automated enterprise-wide solution to provide a centralized view of information security risks across the organization.

Management's Response. The Office of Information Technology, in coordination with the Office of the Chief Operating Officer, concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will coordinate with the Office of the Chief Operating Officer to identify, define requirements for, and implement an automated solution to provide a centralized enterprise-wide view of information security risks across the organization, including considerations identified by the National Institute of Standards and Technology. Management's complete response is printed in Appendix II.

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

Management's Response. The Office of Acquisitions and the Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that (a) the Office of Acquisitions and the Office of Information Technology will develop a risk-based approach to review and update existing, applicable technology contracts to ensure all appropriate provisions are included; (b) the Office of Information Technology will review its processes for ensuring all information technology-related requirements in statements of work and purchase request packages include complete and up to date provisions; and (c) the Office of Information Technology will review its processes for ensuring applicable changes and updates (such as references to the latest versions of National Institute of Standards and Technology and Office of Management and Budget guidance) are

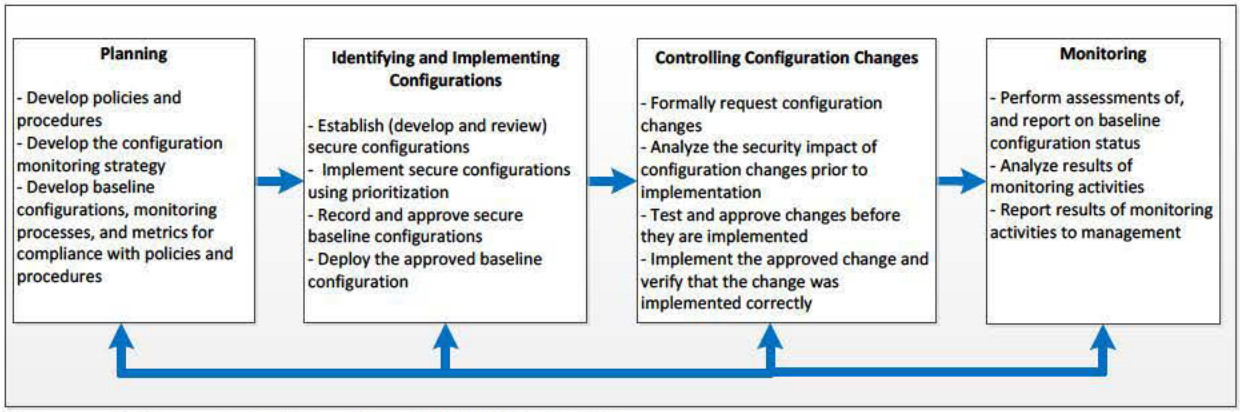
made to existing technology contracts. Management's complete response is printed in Appendix II.

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.

Domain #2: Configuration Management

According to NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011 (NIST SP 800-128), configuration management is an important process for establishing and maintaining secure information system configurations, and provides important support for managing security risks in information systems. Configuration management activities include establishing baseline configurations,[13] developing a configuration change control process, and developing a process for configuration monitoring and reporting. NIST SP 800-53 Rev. 4 requires that organizations develop, document, and maintain under configuration control a current baseline configuration of information systems. The approved baseline configuration for an information system and associated components represents the most secure state consistent with operational requirements and constraints. In addition, as described in Figure 2, security-focused configuration management of information systems involves a set of activities that can be organized into the following four major phases: (1) planning, (2) identifying and implementing configurations, (3) controlling configuration changes, and (4) monitoring.

Figure 2. Security-Focused Configuration Management Phases



Source: OIG-generated based on NIST SP 800-128.

[13] NIST SP 800-128 defines a baseline configuration as a set of specifications for a system or part or a system that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

We assessed the SEC's configuration management program and determined that the program's maturity level is Level 2 ("Defined"), meaning the SEC formalized and documented configuration management policies and procedures, but did not consistently implement them. Specifically, we determined that the SEC did not:

- Fully (b) (7)(E) , or review and update SSPs (which include systems' baseline configurations) at least annually or within established schedules, as previously discussed under Domain #1 (Risk Management) (***Baseline Configurations***);
- Adequately implement (b) (7)(E) (***Configuration Monitoring and Reporting***); and
- Consistently perform and document security impact analyses before implementing configuration changes (***Configuration Change Control***).

Each of these areas is discussed further below.

Baseline Configurations. According to NIST SP 800-53 Rev. 4, organizations should establish baseline configurations for information systems and their constituent components. The organization should also document configuration settings that reflect the most restrictive modes consistent with operational requirements. In addition, OIT's (b) (7)(E) states that OIT shall develop a continuous monitoring strategy (including establishing approved baseline configurations for each environment), and develop, document, and maintain, under configuration control, a current baseline configuration for SEC information systems and constituent components. The (b) (7)(E) further states that OIT shall review and update baseline configurations (documented in SSPs) at least annually.

As of July 2017, there were 61 systems on the (b) (7)(E) (b) (7)(E) (b) (7)(E) (b) (7)(E) to develop (b) (7)(E) device policies, OIT did not finalize those device settings and baselines; (2) the operating system lockdown baseline for a key system (b) (7)(E) had an incorrect (b) (7)(E) and (3) in one instance, OIT did not document configuration settings that reflected the (b) (7)(E) Specifically, the SEC-approved baseline for the (b) (7)(E) required a minimum (b) (7)(E) although the current (b) (7)(E) requires a minimum (b) (7)(E)

(b) (7)(E)

We also determined that OIT did not always timely review and update baseline configurations at least annually, in accordance with its own guidance. Specifically, for 10 of the 25 SEC systems tracked on OIT's (b) (7)(E) (or 40 percent), OIT did not review and update the systems' SSP at least annually or within the established schedule. As of September 2017, OIT had initiated, but not finalized, a review of the SSPs for 4 of these 10 systems, yet the remaining 6 systems were operating without an updated SSP. On average, these SSPs were 1 to 2 months beyond their required review dates. Without adequate configuration management controls, including baseline configurations, agency systems or devices may be misconfigured and, therefore, vulnerable to malicious attacks which could exploit those misconfigurations.

As previously discussed under Domain #1 (Risk Management), according to OIT personnel, these conditions occurred, in part, because OIT did not have adequate resources to timely complete activities. OIT personnel stated that they on-boarded a new contractor in (b) (7)(E) and were catching up on reviewing and updating SSPs. Also, as previously stated, since our October 2017 Cyberscope submission, the SEC implemented a new annual system review process to ensure that information system owners consistently review and update baseline configurations documented in SSPs. We will assess the effectiveness of this new process in the FY 2018 assessment of the SEC's information security program.

Configuration Monitoring and Reporting. According to FISMA, agencies should comply with minimally acceptable system configuration requirements as determined by the agency. In addition, NIST SP 800-53 Rev. 4 requires organizations to monitor and control changes to system configuration settings in accordance with organizational policies and procedures. Also, agencies should routinely monitor configuration information for accuracy, and ensure such monitoring addresses the current baseline and operational configuration of the hardware, software, and firmware that comprise each information system. As previously stated, OIT's (b) (7)(E) states that OIT shall review and update baseline configurations at least annually, when required because of patches and common vulnerability enumeration announcements, and as an integral part of information system component installations and upgrades.

OIT performs discovery, compliance scans, and automated vulnerability scans on SEC systems at established frequencies. However, we determined that OIT did not adequately (b) (7)(E) For example, OIT did not perform (b) (7)(E) in each of the SEC's environments of operation (b) (7)(E) According to OIT personnel, OIT primarily focused on (b) (7)(E) and the agency is evaluating whether to perform (b) (7)(E)

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

Furthermore, although OIT made progress in mitigating vulnerabilities, OIT did not always timely address vulnerabilities identified through its internal vulnerability scans. Also, according to agency personnel, OIT did not document periodic reviews performed to verify that security vulnerabilities and compliance issues identified during those scans were timely mitigated. For example, in August 2017, the SEC identified about (b) (7)(E) [redacted] (b) (7)(E) identified numerous critical and high vulnerabilities needing mitigation, including vulnerabilities that existed because of missing security patches and vulnerabilities impacting systems running unsupported tools and software versions.

While we cited the SEC's internal vulnerability scanning results above, according to the DHS' Federal Cyber Exposure Scorecard of September 2017, the SEC does not have critical vulnerabilities on its public-facing systems. SEC officials stated that the Information Security team is constantly working with system owners and operational teams on vulnerability management.

OIT recently implemented the (b) (7)(E) [redacted] tools in use and is working to address deficiencies in hardware and (b) (7)(E) [redacted] management. In addition, OIT personnel stated that they have not yet defined the roles and responsibilities to review (b) (7)(E) [redacted] reports and (b) (7)(E) [redacted] within agency-defined timeframes. However, OIT management periodically met to discuss vulnerability dashboard reports, and held periodic information security meetings with agency senior officials. Without fully defined roles and responsibilities for (b) (7)(E) [redacted] and effective review and tracking of (b) (7)(E) [redacted] reports, the SEC may not be able to maintain awareness of threats

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

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

and vulnerabilities affecting agency systems, increasing the risk that its systems and information may be compromised.

Configuration Change Control. According to NIST SP 800-128, the challenge for organizations is not only to establish an initial baseline configuration that represents a secure state but also to maintain a secure configuration given the continually evolving nature of an information system and the mission it supports. To control configuration changes, NIST SP 800-128 states that organizations ensure that such changes are formally identified, proposed, reviewed, analyzed for security impact, tested, and approved before being implemented. NIST SP 800-128 further states that conducting security impact analyses—during which changes are examined for impact on security, and for mitigating controls that can be implemented to reduce any resulting vulnerability—is one of the most critical steps in the configuration change control process. In addition, NIST SP 800-53 Rev. 4 requires that organizations analyze changes to information systems to determine potential security impacts before change implementation.

The SEC developed, documented, and disseminated its policies and procedures for managing configuration change control, including conducting security impact analyses. According to OIT's (b) (7)(E) the Information System Office is responsible for performing and documenting security impact analyses. In addition, OIT's (b) (7)(E) states that the configuration change control shall "review proposed configuration-controlled changes to the information systems, and approves or disapproves such changes with explicit consideration for security impact analyses."

However, we determined that the SEC did not consistently perform and document security impact analyses before implementing configuration changes. For example, in FY 2017, the Configuration Control Board approved eight configuration changes to two of the systems we reviewed (b) (7)(E) despite the fact that OIT Security did not perform and document security impact analyses for three of the eight changes (or about 38 percent).[17]

This occurred because, according to OIT officials, OIT Security completed security impact analyses as part of the Configuration Control Board process. However, the Configuration Control Board's meeting minutes we reviewed did not indicate that the Configuration Control Board approved configuration changes with explicit consideration given to security impact analyses. Without documented security impact analyses, implemented changes could expose the organization to attack.

[17] For the other five changes we reviewed, OIT provided documented security impact analyses.

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

To mature the agency's configuration management program from Level 2 ("Defined") to Level 3 ("Consistently Implemented"), we recommend that the Office of Information Technology:

Recommendation 8: Develop, review, and approve secure baselines for all systems included in the (b) (7)(E) [redacted]

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will develop a (b) (7)(E) [redacted] Management's complete response is printed in Appendix II.

OIG's Evaluation of Management's Response. We are pleased that management concurred with the recommendation. However, as stated in the recommendation, management should also (b) (7)(E) [redacted] (b) (7)(E) [redacted] We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is fully responsive to the recommendation.

Recommendation 9: Define and implement a process, including roles and responsibilities, to routinely: (a) (b) (7)(E) [redacted] (b) perform (b) (7)(E) [redacted] of all devices within the agency's network; and (c) document, track, and address the (b) (7)(E) [redacted] including those issues and vulnerabilities identified as unmitigated at the time of our audit.

Management's Response. The Office of Information Technology concurred with the recommendation. (b) (7)(E) [redacted] Management's complete response is printed in Appendix II.

OIG's Evaluation of Management's Response. We are pleased that management concurred with the recommendation. However, as stated in the recommendation, management should (b) (7)(E) [redacted] We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is fully responsive to the recommendation.

Recommendation 10: Update its existing processes to ensure that the Information Security Office consistently performs and documents security impact analyses for proposed configuration changes before implementation.

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will review and update Change Control Board procedures, as applicable, to clarify the manner in which security impact analyses should be captured. Management's complete response is printed in Appendix II.

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.

Domain #3: Identity and Access Management

NIST SP 800-53 Rev. 4 requires organizations to develop, document, and disseminate an access control policy and an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The SEC employs an access management program to ensure that only authorized individuals have access to SEC information systems; users are restricted to authorized transactions, functions, and information; access is assigned according to the principles of separation of duties and least privilege; and users are individually accountable for their actions. Furthermore, an identification and authentication process confirms the identity of users before granting access to SEC information and information systems.

We assessed the SEC's identity and access management program and determined that the program's maturity level is Level 2 ("Defined"), meaning the SEC formalized and documented identity and access management policies and procedures, but did not consistently implement them. Specifically, we determined that the SEC did not:

- Develop a transition plan to include milestones and priorities for aligning its identity, credential, and access management strategy with Federal initiatives (***Identity, Credential, and Access Management Strategy***);

- (b) (7)(E) ***Strong Authentication***);
- Employ automation to centrally document, track, and share risk designations and screening information with necessary parties (***Personnel Risk Designations***); and
- (b) (7)(E) (***Remote Access Connections***).

Each of these areas is discussed further below.

Identity, Credential, and Access Management Strategy. According to the *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, Federal agencies must ensure that sufficient resources are available for identity, credential, and access management activities, and must develop transition plans including milestones and priorities to guide agency budget requests. The *FY 2017 IG FISMA Reporting Metrics* asked IGs to determine whether agencies defined their identity, credential, and access management strategies, and developed milestones for how agencies plan to align with Federal initiatives, including strong authentication; the Federal Identity, Credential, and Access Management segment architecture; and phase 2 of DHS' Continuous Diagnostics and Mitigation program, as appropriate.

Although the SEC documented its identity, credential, and access management strategy, the agency did not develop a transition plan or strategy to include milestones and priorities for aligning the SEC's identity, credential, and access management strategy with Federal initiatives. According to agency officials, OIT decided to delay developing a transition plan until a DHS tool becomes available.[18] Without implementing a transition plan to align the SEC's strategy with Federal initiatives, the SEC may be unable to ensure sufficient resources are available for identity, credential, and access management activities.

Strong Authentication. In June 2015, OMB launched a 30-day *Cybersecurity Sprint* to further improve Federal cybersecurity and protect systems against evolving threats. As part of OMB's *Cybersecurity Sprint*, agencies are required to implement multifactor authentication, especially for privileged users using personal identity verification (PIV) or a comparable solution. The *Cybersecurity Sprint* also requires agencies to limit functions that can be performed with privileged accounts. In addition, OMB M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, October 2015, states that agencies should continue to target the administration cybersecurity goal of 100-percent strong authentication for privileged

[18] At the time of our audit, DHS was developing an enterprise tool that will help agencies manage credentials for all privileged users. DHS did not have a timeline for making this tool available.

users, and 85-percent strong authentication for non-privileged users. However, according to the *FY 2017 IG FISMA Reporting Metrics*, to achieve an effective level of security, agencies should implement strong authentication mechanisms (such as PIV) for 100 percent of their non-privileged users.

The SEC consistently implemented strong authentication for privileged and non-privileged users' access to the agency network in accordance with Federal guidance. Specifically, the SEC implemented strong authentication for 100 percent of privileged users, and reached the 85 percent Federal target for non-privileged users. (b) (7)(E) Also, in accordance with NIST best practices, the SEC should consider taking steps to ensure that (b) (7)(E) (b) (7)(E)

(b) (7)(E) We will assess the effectiveness of this new process in the FY 2018 assessment of the SEC's information security program. (b) (7)(E) Requiring the use of strong authentication for all users and limiting functions that can be performed with (b) (7)(E)

Personnel Risk Designations. According to NIST 800-53 Rev. 4, agencies should assign a risk designation to all positions and ensure they screen individuals before authorizing access to information systems. In addition, according to the *FY 2017 IG FISMA Reporting Metrics*, to achieve an effective level of security, the organization must employ automation to centrally document, track, and share risk designations and screening information with necessary parties as appropriate. At the SEC, personnel are assigned a risk designation based on their position description. The (b) (7)(E) within the Office of Security Services is responsible for managing personnel screening.

The SEC defined processes for ensuring that all personnel are assigned a risk designation and are appropriately screened (and rescreened periodically) before being granted system access. However, the SEC did not employ automation to centrally document, track, and share risk designations and screening information with necessary

(b) (7)(E)

parties, as appropriate. Rather, the agency used a (b) (7)(E) [redacted] We could not verify that this (b) (7)(E) [redacted] captured all personnel that should be rescreened periodically.

The SEC did not employ automation to centrally document, track, and share risk designations, in part, because the agency had not implemented a system to automatically track screening information. According to SEC officials from the Office of Security Services, they are working with OIT to draft business requirements for an improved case management system. However, the agency has not approved funding for the system. Risk designations are more likely to be appropriately assigned with automated controls, as automated controls tend to be more reliable because they are less susceptible to human error.

Remote Access Connections. Federal Information Processing Standards Publication 201-2 requires agencies to implement a cryptographic module that complies with Federal Information Processing Standards Publication 140-2 for user authentication on all connections. Furthermore, according to NIST 800-53 Rev. 4, agencies must define when information systems terminate a user's session, and monitor the use of information systems by users. (b) (7)(E) [redacted]

The SEC defined its configuration and connection requirements for remote access connections. However, the SEC (b) (7)(E) [redacted]

In addition, in response to our FY 2016 FISMA audit report, the SEC developed processes requiring users to read and agree to SEC Information User Agreements when beginning work at the agency. The SEC also developed a policy requiring access agreements to be recertified at a predetermined interval (through the annual certification of adherence to any official SEC Information Systems User Agreements).[20] However, the SEC had not ensured that users consistently completed access agreements before gaining access to SEC systems, and recertified the access agreements at a predetermined interval thereafter. For example, the SEC did not maintain access

[20] In our FY 2016 FISMA audit report, we recommended that OIT, in coordination with the Office of Human Resources, (1) develop a process to document and track all users' initial access agreements and training before granting access to agency information systems; and (2) develop a policy requiring access agreements to be recertified at a predetermined interval. As of the date of this report, the agency had implemented the second recommendation but had not implemented the first recommendation, although efforts were underway to implement it in FY 2018.

agreements for 16 of 50 SEC employees and contractors we judgmentally selected for review (or 32 percent).[21]

If not timely and properly addressed, the opportunities for improvement we identified may increase the risk of unauthorized access to the SEC's network, information systems, and data.

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

To mature the agency's identity and access management program from Level 2 ("Defined") to Level 3 ("Consistently Implemented"), we recommend that the Office of Information Technology:

Recommendation 11: Develop and implement a transition plan or strategy, including milestones and priorities, for aligning the agency's identity, credential, and access management strategy with Federal initiatives.

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will develop a strategy document that describes how the SEC currently complies with Federal identity, credential, and access management standards. Management's complete response is printed in Appendix II.

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

Management's Response. The Office of Information Technology concurred with the recommendation. (b) (7)(E) [redacted] Management's complete response is printed in Appendix II.

[21] In total, between October 1, 2016, and June 30, 2017, the SEC had 248 new employees and 848 new contractor personnel.

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

Management's Response. The Office of Information Technology concurred with the recommendation. (b) (7)(E) [redacted] Management's complete response is printed in Appendix II.

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.

We also recommend that the Office of Security Services:

Recommendation 14: Consider implementing an automated mechanism to centrally document, track, and share risk designations and screening information with necessary parties, as appropriate.

Management's Response. The Office of Security Services concurred with the recommendation. The Chief Operating Officer stated that the Office of Security Services will consider the costs and benefits of implementing an automated mechanism to centrally document, track, and share risk designations and screening information with necessary parties and document the results of their findings. Management's complete response is printed in Appendix II.

OIG's Evaluation of Management's Response. Although management's response states that the Office of Security Services will consider the costs and benefits of implementing an automated mechanism as recommended, on February 26, 2018, after the OIG's exit conference with agency management, the Office of Security Services reported to the OIG that the Office of Information Technology's Information Technology Capital Planning Committee denied the Office of Security Service's request for funding for this requirement. According to documents provided by the Office of Security Services, the Information Technology

Capital Planning Committee determined that the recommended automated mechanism was not a "need to have." Management's completed action is responsive; therefore, the recommendation is resolved and closed for reporting purposes.

Domain #4: Security Training

FISMA requires agencies to establish an information security program that includes security awareness training. Such training informs personnel, including contractors, of information security risks associated with their activities, and their responsibilities for complying with agency policies and procedures. NIST SP 800-53 Rev. 4 states that individuals with significant security responsibilities are to receive specialized security training before gaining access to information systems or before performing assigned duties. In addition, NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (October 2003), states that organizations must monitor their information security training program for compliance and effectiveness, and that failure to give attention to IT security training puts an enterprise at greater risk because the security of agency resources is as much a human issue as it is a technology issue.

We assessed the SEC's information security training program and determined that the program's maturity level is Level 2 ("Defined"), meaning the SEC formalized and documented security training policies and procedures, but did not consistently implement them. Specifically, OIT's (b) (7)(E) [redacted] establishes the policies, procedures, roles, and responsibilities for the SEC's IT security training program. Furthermore, OIT defined processes to assess the agency's cybersecurity workforce, implement its security awareness and specialized training plan, and define and tailor its security awareness and specialized training material content. However, we determined that 109 of 691 individuals with significant security responsibilities (or about 16 percent) did not receive specialized security training before accessing agency information systems or before performing assigned duties. In addition, as of the end of FY 2017, OIT had not implemented recommendations from our FY 2016 FISMA audit related to cybersecurity workforce assessments and privacy information security awareness training.[22]

[22] In our FY 2016 FISMA audit report, we recommended that OIT, in coordination with the Office of Human Resources, (1) fully implement a process to evaluate the skills of users with significant security and privacy responsibilities and provide additional security and privacy training content, or implement strategies to close identified skills gaps; (2) develop a process to document and track all users' initial access agreements and training before granting access to agency information systems; and (3) update procedures to ensure all users receive privacy information security awareness training annually (every 12 months). As of the date of this report, the agency had implemented the third recommendation but had not implemented the first two recommendations, although efforts were underway to implement them in FY 2018.

This occurred, in part, because OIT did not define a process to ensure individuals with significant security responsibilities received specialized security training before gaining access to information systems or before performing assigned duties. Also, according to OIT management, although the SEC established resource requirements for consistently implementing the SEC's security training program, OIT did not have adequate resources (processes and technology) to consistently implement security awareness and training responsibilities. OIT management personnel explained that they will have adequate resources once they update the SEC training system so that new employees can be assigned privacy information security awareness training with access agreements. This new capability is scheduled to be implemented in FY 2018.

Without an effective security training program, users may be unaware of their security responsibilities and, therefore, may not effectively protect the SEC's sensitive, non-public information. In addition, the SEC increases its risk of a computer security incident and/or loss, destruction, or misuse of sensitive Federal data assets.

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

To mature the agency's information security training program from Level 2 ("Defined") to Level 3 ("Consistently Implemented"), we recommend that the Office of Information Technology:

Recommendation 15: Develop and implement a process to ensure that all individuals with significant security responsibilities receive required specialized training before gaining access to information systems or before performing assigned duties.

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Human Resources has invested in a technical solution to facilitate the tracking and completion of security training prior to authorizing network access and is in the process of implementing this solution. The Chief Operating Officer also stated that Office of Information Technology will continue to work with the Office of Human Resources to implement this capability to ensure that personnel with significant security responsibilities complete training before performing their assigned duties. Further, the Office of Information Technology will adjust account management protocols to ensure training is completed prior to granting privileged access to the SEC's network of information systems. Management's complete response is printed in Appendix II.

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.

Domain #5: Information Security Continuous Monitoring

ISCM refers to the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. An effective ISCM program results in ongoing updates to the organization's security plans, security assessment reports, and POA&Ms, which are the three principal documents in a system's security authorization package. According to NIST SP 800-137, organizations should take steps to establish, implement, and maintain an ISCM program, including defining an ISCM strategy, analyzing and reporting findings, and reviewing and updating the ISCM strategy and program as necessary. In addition, OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems*, November 2013 (OMB M-14-03), states that agencies were to implement continuous monitoring of security controls as part of a phased approach through FY 2017.

We assessed the SEC's ISCM program and determined that the program's maturity level is Level 2 ("Defined"), meaning the SEC formalized and documented ISCM policies and procedures, but did not consistently implement them. Specifically, we determined that:

- The SEC ISCM strategy was not comprehensive, and the SEC did not establish procedures for reviewing and modifying all aspects of the ISCM strategy (***ISCM Strategy and Review Procedures***); and
- The SEC did not perform ongoing authorizations of its information systems and the environments in which they operate (***Ongoing Authorizations***).

Both of these areas are discussed further below.

ISCM Strategy and Review Procedures. NIST SP 800-137 requires organizations to develop a comprehensive ISCM strategy encompassing technology, processes, procedures, operating environments, and people to support risk management in accordance with organizational risk tolerance. According to this publication, an effective ISCM strategy addresses ISCM requirements and activities at each organizational tier (organization, mission/business processes, and information systems). In addition, NIST SP 800-137 states that the ISCM strategy should include metrics that provide meaningful indications of security status of all organizational tiers, ensure the effectiveness of all security controls, and help to maintain visibility into the security of the organization's assets. Finally, NIST SP 800-137 requires that organizations establish procedures for reviewing and modifying all aspects of the ISCM strategy, including relevance of the overall strategy, accuracy in reflecting organizational risk tolerance, accuracy/correctness of measurements, and applicability of metrics, reporting requirements, and monitoring and assessment frequencies.

The SEC established an (b) (7)(E) [redacted] In addition, the SEC defined and communicated its policies and procedures for ongoing assessment and monitoring of security controls; granting system

authorizations; collecting security-related information required for metrics, assessments, and reporting; and analyzing ISCM data. However, the SEC did not develop a comprehensive ISCM strategy. Specifically, as previously discussed under Domain #1 (Risk Management), the SEC did not (1) define the risk executive function roles and responsibilities, including his or her responsibilities in relation to the ISCM strategy; and (2) consistently identify or document the implementation of applicable security controls, perform annual security or risk assessments, or authorize systems to operate in accordance with agency policy. Moreover, the SEC's ISCM strategy did not address ISCM requirements and activities at each organizational tier in accordance with NIST SP 800-137. For example, the ISCM strategy did not support ongoing authorization at the information system tier. In addition, the SEC did not (1) define the quantitative and qualitative performance measures that will be used to assess the effectiveness of the agency's ISCM program, achieve situational awareness, and control ongoing risk; or (2) establish procedures for reviewing and modifying all aspects of the ISCM strategy. This occurred, in part, because the SEC has not defined a process to review and update the existing ISCM strategy.

Without a comprehensive ISCM strategy and defined quantitative and qualitative performance measures, the agency may not maintain visibility into the security status of all organizational tiers. In addition, reviewing all aspects of the ISCM strategy may uncover ways to improve organizational insight into the agency's security posture, and improve the agency's ability to respond to known and emerging threats.

Ongoing Authorizations: OMB M-14-03 states that, to fully implement ISCM, agencies shall establish an ISCM program that addresses how the agency will conduct ongoing authorizations of information systems and the environments in which those systems operate. Agencies must then conduct ongoing authorizations in accordance with their established program. However, according to information the agency provided to DHS, the SEC did not perform ongoing authorizations of its information systems and the environments in which they operate. This occurred because the SEC had not defined its ongoing authorization process. Making ongoing authorization decisions helps maintain situational awareness of the security of agency systems.

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

To mature the agency's information security continuous monitoring program from Level 2 ("Defined") to Level 3 ("Consistently Implemented"), we recommend that the Office of Information Technology:

Recommendation 16: Update the existing continuous monitoring strategy to define (a) qualitative and quantitative performance measures or data that should be collected to assess the effectiveness of the agency's continuous monitoring program; (b) procedures for reviewing and modifying all aspects of the agency's continuous monitoring strategy; and (c) the agency's ongoing authorization process.

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will update existing policies and procedures to define qualitative and quantitative performance measures on the continuous monitoring program. The Chief Operating Officer also stated that the Office of Information Technology will create an ongoing authorization strategy that will define timeframes and a roadmap to achieve ongoing authorization. Management's complete response is printed in Appendix II.

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.

Domain #6: Incident Response

FISMA requires agencies to develop and implement an agency-wide information security program that includes procedures for detecting, reporting, and responding to security incidents, including mitigating the risks of such incidents before substantial damage is done. According to NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*, August 2012 (NIST SP 800-61), key phases in the incident response process are: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity.

We assessed the SEC's incident response program and determined that the program's maturity level is Level 2 ("Defined"), meaning the SEC formalized and documented incident response policies and procedures, but did not consistently implement them. For example, the SEC established and communicated an enterprise-level incident response plan, defined an (b) (7)(E) and conducted three incident response plan tests during FY 2017. However, we determined that the SEC did not:

- Maintain up-to-date and comprehensive incident response plans, policies, procedures, and strategies (***Incident Response Plans, Policies, Procedures, and Strategies***);
- Fully and consistently implement incident detection and analysis processes and technologies (***Incident Detection and Analysis***); and
- Timely report incidents to the United States Computer Emergency Readiness Team (US-CERT) (***Incident Coordination, Information Sharing, and Reporting***).

Each of these areas is discussed further below.

Incident Response Plans, Policies, Procedures, and Strategies. According to NIST SP 800-61, elements of the organization's incident response plan should be reviewed and updated at least annually, and the plan should include metrics for measuring the

organization's incident response capability and effectiveness, how the incident response team will coordinate with the rest of the organization and with other organizations, and a roadmap for maturing the organization's incident response capability. NIST SP 800-61 also states the incident response plan indicates how often incident handlers should be trained and the requirements for incident handlers. Moreover, procedures should provide detailed steps for responding to an incident, adding that organizations should be generally prepared to handle incidents that use common attack vectors, and that different incidents merit different response strategies. After an incident is adequately handled, the organization should use reports that detail the cost of the incident, among other pieces of information.

We reviewed the SEC's incident response plan (b) (7)(E) and the agency's incident response procedures and strategies and determined that the documents were not comprehensive. For example, OIT had not finalized or completed its incident handling procedures, existing procedures did not address all common threat and attack vectors, and containment strategies documented in the incident response plan did not address the characteristics of each particular situation. In addition, the plan did not align with elements specified in NIST SP 800-61. Specifically, as further described below, the SEC's incident response plan did not (a) include metrics for measuring the agency's incident response capability and effectiveness; (b) clearly define protocols for how the agency's incident response team will coordinate with the rest of the organization and with other organizations; and (c) indicate incident handler training requirements, including how often incident handlers should be trained.

Incident Response Metrics. Although the SEC monitors certain metrics (b) (7)(E) and tracks those metrics in weekly reports prepared by the agency's (b) (7)(E) none of the metrics have been defined in the agency's incident response plan, policies, procedures, or strategies in accordance with NIST SP 800-61. Moreover, the ad hoc metrics tracked did not include incident response costs. Also, the SEC did not document the process used to ensure that data supporting the metrics were obtained accurately, consistently, and in a reproducible format. This occurred, in part, because according to (b) (7)(E) they allowed the incident response metrics to evolve on an ad hoc basis over time and based on feedback.

Incident Response Communication Protocols. Although the SEC defined how the agency's incident response team notifies agency officials, law enforcement, the OIG, and the Congress, the communication protocols were not clearly defined. According to the SEC, the agency plans to develop (a) a protocol to specify incident management conditions warranting communications between points of contact, and (b) protocols for notifying affected stakeholders of common types of information security events. Without properly defined information sharing protocols, sensitive information regarding incidents may not be timely provided to authorized parties, or may be provided to unauthorized parties,

potentially leading to disruptions and financial loss. As of the end of FY 2017, the SEC was working to address a recommendation from our FY 2016 FISMA audit report for improved incident reporting to the OIG.

Incident Handlers' Training. SEC incident handlers are (b) (7)(E) The (b) (7)(E) indicates that the (b) (7)(E) shall provide at all times no less than one certified security analyst physically on site at the SEC's (b) (7)(E) However, neither the (b) (7)(E) nor the SEC's incident response plan specified incident handler training requirements, including how often incident handlers should be trained. This occurred, in part, because the (b) (7)(E) was in the process of running a pilot of its proposed incident handler training program and was not prepared at the time of our audit to formalize the program. Creating a training program would allow the SEC to assess incoming analysts' capabilities and gauge analysts' preparedness to perform incident handling activities.

In addition, we determined that the SEC's incident response plan, procedures, and strategies were not up-to-date. For example, OIT did not review and update elements of the SEC's incident response plan at least annually as required by NIST SP 800-61.[23] Also, OIT's (b) (7)(E) describes the roles and responsibilities of the agency's (b) (7)(E) and the Team's manager. However, according to OIT personnel, (b) (7)(E) (b) (7)(E) is an outdated term for the SEC's (b) (7)(E). Also, the SEC's (b) (7)(E) referred to outdated or unavailable SEC procedures and documents.

We noted that, in DHS/OMB's FY 2017 Annual Cybersecurity Risk Management Assessment, the agency is rated as "at-risk" for incident response. Without comprehensive and updated incident response plans, policies, procedures, and strategies, including metrics, communication protocols, and incident handler training requirements, the SEC may not respond to incidents effectively.

Incident Detection and Analysis. According to NIST SP 800-61, documenting system events, conversations, and observed changes in files can lead to more efficient, more systematic, and less error-prone handling of incidents when they occur. Furthermore, every step taken from the time the incident was detected to its final resolution should be documented and time-stamped. NIST SP 800-61 also states that an incident analysis should document indicators of the incident and the organization should maintain a knowledge base of those indicators and other information for incident handlers' reference when performing incident analysis.

[23] Before (b) (7)(E), the (b) (7)(E) was last updated in (b) (7)(E)

The SEC defined processes and supporting technologies for detecting, analyzing, and prioritizing incidents. (b) (7)(E) [redacted] Specifically, as further described below, we identified opportunities for improvement in the areas of (a) incident documentation, (b) indicators of compromise, and (c) incident response tools.

Incident Documentation. We judgmentally selected and reviewed 12 incidents that, according to SEC records, occurred between (b) (7)(E) [redacted] as well as supporting incident tickets, incident logs, and quality assurance reviews of ticket documentation.[24] We determined that incident tickets for the 12 incidents we reviewed did not consistently document and timestamp all steps in the incident response process from detection to resolution. Furthermore, these inconsistencies included a lack of incident detail on resolution activities, affected employees, infection confirmation, and US-CERT notification. Finally, although OIT performed quality assurance reviews of incident ticket documentation, we found one instance in which the incident ticket creator was also the quality assurance reviewer. These conditions occurred, in part, because the (b) (7)(E) [redacted] did not have an effective incident response quality review process that included controls to ensure the incident logs adequately documented and time stamped all the steps taken to resolve the ticket from detection to resolution. In addition, the system used to track the incident tickets did not contain a control to restrict the ticket creator from reviewing the quality of their own work.

Indicators of Compromise. The SEC defined processes for SEC (b) (7)(E) [redacted] to review daily Indicator of Compromise lists, which include the signs of intrusion received and processed by the (b) (7)(E) [redacted]. The (b) (7)(E) [redacted] compiles Indicator of Compromise lists from internal SEC incident response tools and information received from external parties (such as cyber intelligence from various U.S. Government, industry, and open source feeds). (b) (7)(E) [redacted]

Incident Response Tools. In FY 2017, the SEC continued its implementation of multiple incident response tools. (b) (7)(E) [redacted]

[24] Appendix I describes our sampling methodology.

(b) (7)(E)

[redacted]

Documenting system events, conversations, and observed changes in files can lead to a more efficient, more systematic, and less error-prone handling of the problem. (b) (7)(E)

[redacted]

Incident Coordination, Information Sharing, and Reporting. The US-CERT April 2017 *Federal Incident Notification Guidelines* requires agencies to report certain information security incidents to US-CERT within 1 hour of being identified by the agency's computer security incident response team, SOC, or IT department.[26] We determined that the SEC defined processes for reporting suspected security incidents to the agency's incident response capability and for reporting security incident information to US-CERT, law enforcement, Congress, and the OIG. In addition, the SEC determined how it will collaborate with DHS and other parties, and leverage certain DHS capabilities to supplement the SEC's intrusion detection and prevention resources. However, OIT did not always timely report incidents to US-CERT. Specifically, OIT did not report to US-CERT 4 of the 12 incidents we reviewed (or 33 percent) within 1 hour as required. Two of the four incidents were reported to US-CERT within about an hour and a half after the [redacted] was notified, whereas the remaining two incidents were reported to US-CERT about 12 hours and 15 hours, respectively, after the [redacted] was notified.[27]

According to OIT personnel, these delays occurred because, before March 2017, reporting to US-CERT was a manual process, which hindered the SEC's ability to report incidents in a timely manner. However, three of the four incidents that we determined

(b) (7)(E)

[redacted]

[26] Information security incidents that agencies must report to US-CERT within 1 hour of detection are those incidents in which the confidentiality, integrity, or availability of a Federal information system was potentially compromised.

[27] The remaining eight incidents were reported to US-CERT as required.

were not timely reported occurred after the agency implemented an automated reporting solution. As previously stated, OIT did not clearly define protocols for how the agency's incident response team will coordinate with the rest of the organization and with external stakeholders. Therefore, additional improvements are needed to ensure the SEC timely reports incidents as required. According to OIT personnel, the agency is planning to develop protocols related to agency communications with identified internal and external stakeholders.

The SEC can mature its incident response program by addressing the areas identified above. Weaknesses in the SEC's incident response program could prevent the timely detection, prevention, or reporting of unauthorized access and disclosure of SEC data.

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

To mature the agency's incident response program from Level 2 ("Defined") to Level 3 ("Consistently Implemented"), we recommend that the Office of Information Technology:

Recommendation 17: Review and update incident response plans, policies, procedures, and strategies to (a) address all common threat and attack vectors and the characteristics of each particular situation; (b) identify and define performance metrics that will be used to measure and track the effectiveness of the agency's incident response program; (c) develop and implement a process to ensure that incident response personnel obtain data supporting the incident response metrics accurately, consistently, and in a reproducible format; (d) define incident response communication protocols and incident handlers' training requirements; and (e) remove outdated terminology and references.

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will review and update existing incident policies and procedures to ensure they align with requirements from National Institute of Standards and Technology Special Publication 800-61. The Chief Operating Officer also stated that the Office of Information Technology (a) will update applicable policies and procedures to define protocols for common threat and attack vectors; (b) will review and update the procedures that describe how performance metrics are used to measure and track the effectiveness of the agency's incident response program; (c) will review training requirements for incident handlers; and (d) is currently updating the agency's Incident Management Plan to ensure that outdated terminology and references are removed. Management's complete response is printed in Appendix II.

OIG's Evaluation of Management's Response. We are pleased that management concurred with the recommendation. However, as stated in the recommendation, management should also develop and implement a process to ensure that incident response personnel obtain data supporting the incident response metrics accurately,

consistently, and in a reproducible format; and define incident response communication protocols. We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is fully responsive to the recommendation.

Recommendation 18: Fully implement processes to (a) consistently document and timestamp every step in the incident response process from detection to resolution; and (b) ensure a person other than the incident ticket creator reviews incident documentation (including logs and tickets), and confirms that consistent and complete information is maintained for every step in the incident response process.

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will define key milestones that need to be supplied to the incident response system and will develop supporting procedures to ensure that analysts follow the process. Further, the Office of Information Technology will revisit existing quality control processes and update the processes to ensure they are effective. Management's complete response is printed in Appendix II.

OIG's Evaluation of Management's Response. We are pleased that management concurred with the recommendation. However, as stated in the recommendation, management should also fully develop a process to consistently document and timestamp ***every*** step in the incident response process from detection to resolution. We will review the agency's corrective action plan when management submits it to the OIG to determine whether the planned corrective action is fully responsive to the recommendation.

Recommendation 19: Improve its ability to review indicators of compromise by (b) (7) (E) [redacted]

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will (b) (7)(E) [redacted] Management's complete response is printed in Appendix II.

OIG's Evaluation of Management's Response. We are pleased that management concurred with the recommendation. However, as stated in the recommendation, management (b) (7)(E) We will review the agency's corrective action plan management submits it to the OIG to determine whether the planned corrective action is fully responsive to the recommendation.

Recommendation 20: Perform an assessment of existing incident response reporting mechanisms, and develop a process to periodically measure and ensure the timely reporting of incidents to agency officials and external stakeholders.

Management's Response. The Office of Information Technology concurred with the recommendation. The Chief Operating Officer stated that the Office of Information Technology will complete (b) (7)(E) and evaluate the associated recommendations and/or corrective actions. Management's complete response is printed in Appendix II.

OIG's Evaluation of Management's Response. We are pleased that management concurred with the recommendation. However, as stated in the recommendation, management should also develop a process to periodically measure and ensure the timely reporting of incidents to agency officials and external stakeholders. We will review the agency's corrective action plan management submits it to the OIG to determine whether the planned corrective action is fully responsive to the recommendation.

Domain #7: Contingency Planning

FISMA requires agencies to develop, document, and implement plans and procedures to ensure continuity of operations for information systems supporting the operations and assets of the organization. According to NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, Rev. 1, May 2010, such contingency planning activities include developing the planning policy, creating contingency strategies, testing contingency plans, conducting exercises, maintaining contingency plans, and conducting business impact analyses. Business impact analyses help organizations identify and prioritize information systems and components critical to supporting the organization's operations. NIST SP 800-53 Rev. 4 also requires organizations to perform periodic testing of contingency plans to determine effectiveness and organizational readiness.

In FY 2017, the SEC had 23 externally hosted FISMA reportable systems. OIT's (b) (7)(E) requires providers of external information system services to comply with SEC information security requirements and employ Federal

information security controls, such as contingency planning controls, in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The SEC's business impact analyses state that a business impact analysis is required for all SEC FISMA-reportable systems. In addition, information system owners, including owners of external systems, are accountable for testing their information systems and applications and for documenting the results of their disaster recovery exercises.

We assessed the SEC's contingency planning program and determined that the program's maturity level is Level 3 ("Consistently Implemented"), meaning the SEC consistently implemented contingency planning policies and procedures. Although the SEC defined policies, procedures, and strategy related to contingency planning and, during FY 2017, tested its system-specific contingency plans and enterprise disaster recovery plan, we determined that for the externally hosted systems reviewed, the SEC did not ensure that information system owners implemented contingency planning activities in accordance with applicable NIST guidance and OIT policy.

Specifically, OIT did not complete the business impact analysis process for one of the two externally hosted systems we reviewed (b) (7)(E) Moreover, as of the end of FY 2017, OIT had not documented an Information System Contingency Plan for the system,[28] and the system was not incorporated in the SEC's Enterprise Disaster Recovery Plan. In addition, although the other externally hosted system we reviewed (b) (7)(E) had an Information System Contingency Plan, OIT did not test the Plan.

Without strong contingency planning controls for externally hosted systems, the SEC's contingency plans might not provide adequate coverage of all system components, incorporate lessons learned from testing exercises, or address all potentially mission and business critical processes and their interdependencies. In addition, ensuring that externally hosted systems' contingency plans are periodically tested will provide the SEC with additional assurance that system recovery capabilities can be implemented effectively.

As previously stated, since our October 2017 Cyberscope submission, the SEC implemented a new annual system review process to ensure that information system owners consistently implement contingency planning activities including contingency plans, testing exercises, and business impact analyses. We will assess the effectiveness of this new process in the FY 2018 assessment of the SEC's information security program. However, as a result of the agency's implementation of the new process, we are not making a recommendation for this domain at this time.

[28] In November 2017, OIT provided us the (b) (7)(E) Information System Contingency Plan.

Overall Conclusion

Overall, the SEC improved aspects of its information security program. For example, since our FY 2016 FISMA audit, the SEC implemented improved identification and authentication for all users and finalized its information security continuous monitoring strategy. OIT also conducted two incident response exercises and an annual test of the agency's enterprise disaster recovery plan. Furthermore, the SEC continues to enhance capabilities and develop tools in areas such as vulnerability management and configuration management. However, we found that the SEC's information security program did not meet the *FY 2017 IG FISMA Reporting Metrics'* definition of "effective" because the program's overall maturity did not reach Level 4 ("Managed and Measurable"). Implementing our recommended corrective actions will help minimize the risk of unauthorized disclosure, modification, use, and disruption of the SEC's sensitive, non-public information; improve compliance with FISMA requirements; and assist the SEC's information security program reach the next maturity level.

Appendix I. Scope and Methodology

We conducted this performance audit from April 2017 through March 2018 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 compliance with FISMA and respond to the *FY 2017 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.

The audit covered the period between October 1, 2016, and September 30, 2017, and addressed the following seven domains specified in DHS's reporting instructions for FY 2017:

1. Risk Management
2. Configuration Management
3. Identity and Access Management
4. Security Training
5. Information Security Continuous Monitoring
6. Incident Response
7. Contingency Planning

Methodology. We conducted a limited-scope review of the SEC's information security posture sufficient to address our objective. Specifically, to assess system security controls, we reviewed the security assessment packages for a non-statistical, judgmentally selected sample of 5 of the SEC's 41 FISMA-reportable systems (or about 12 percent). The sample consisted of the internally and externally hosted systems shown in Table 2.[29] In addition, to address the requirements of the *FY 2017 IG FISMA Reporting Metrics* for the identity and access management, security training, and

[29] We selected information systems based on the SEC's inventory of FISMA-reportable systems maintained in OIT's system of record as of May 23, 2017. The inventory included 31 major information systems (19 SEC-operated and 12 contractor-operated) and 10 minor applications. We selected five major information systems factoring in: (1) whether the system was included in prior FISMA audits or covered in audits conducted by the OIG in the past 2 years, (2) whether the system was internally hosted or externally hosted, (3) the system risk categorization, and (4) the system's authorization to operate status. We also solicited OIT's input for our sample selection.

incident response domains, we judgmentally selected and reviewed a non-statistical sample of controls related to those domains. Because sampled items were non-statistical, we did not project our results and conclusions to the total user population or measure overall prevalence.

Table 2. SEC Systems Sampled

System Name	System Description	Internally/ Externally Hosted	System Categorization
[redacted]	(b) (7)(E) [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.

To assess the SEC's procedures for detecting, reporting, and responding to security incidents, we selected and reviewed a non-statistical, judgmental sample of incidents, as well as supporting documents. Specifically, we selected incidents that:

- Occurred between (b) (7)(E) [redacted];

- Were confirmed as having compromised the confidentiality, integrity, or availability of information;
- Were from all nine US-CERT threat taxonomies where a confirmed incident occurred; and
- Were representative of each incident priority type (high, medium, or low) as classified by OIT.

According to OIT's records, a total of 739 incidents occurred between (b) (7)(E) [redacted]. OIT confirmed that 81 of these 739 incidents impacted the confidentiality, integrity, or availability of agency information. Based on our established criteria, we selected and reviewed 12 of these 81 incidents.

To rate the maturity level of the SEC's information security program and functional areas, we used the scoring methodology defined in the FY 2017 FISMA Reporting Metrics. We interviewed key personnel, including personnel from (b) (7)(E) [redacted] We also examined documents and records applicable to the SEC's information security program, including applicable Federal laws and guidance; SEC administrative regulations, policies, and procedures; system-level documents; and reports. As discussed throughout this report, these included, but were not limited to, the following:

- Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283;
- E-Government Act of 2002, Pub. L. No. 107-347;
- Applicable OMB guidance, including OMB Circular A-130 and OMB M-16-04;
- Various NIST SPs;
- SECR 24-04; and
- SEC OIT policies.

Finally, we reviewed the SEC's progress towards implementing recommendations from prior FISMA reports.

Internal Controls. Consistent with our audit objective, we did not assess OIT's overall management control structure. Instead, we reviewed the SEC's controls specific to the *FY 2017 IG FISMA Reporting Metrics*. To understand OIT's management controls pertaining to its policies, procedures, and methods of operation, we relied on information requested from and supplied by OIT staff and information from interviews with OIT personnel. We found that the SEC generally complied with applicable FISMA and agency policies and procedures, except as identified in this report. Our recommendations, if implemented, should address the areas of improvement we

identified, and assist the SEC's information security program reach the next maturity level.

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 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 also used the SEC's training management system. We performed data reliability, completeness, and accuracy testing, in part, by comparing computer-processed information to testimonial evidence obtained from system and information owners, and by comparing system outputs for consistency. As a result of these tests, we determined that the computer-processed data we reviewed was sufficiently reliable to support our conclusions.

Prior Coverage. Our FY 2016 FISMA audit report included 21 recommendations for corrective action.[30] As of the date of this report, OIT had implemented 18 of the 21 recommendations. Although OIT addressed these recommendations, as we noted in this report, areas for improvement still exist. Unrestricted SEC OIG audit and evaluation reports, including our FY 2016 FISMA audit report, can be accessed at: http://www.sec.gov/about/offices/oig/inspector_general_audits_reports.shtml.

[30] U.S. Securities and Exchange Commission, Office of Inspector General, *Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2016*, Report No. 539; March 7, 2017.

Appendix II. Management Comments

MEMORANDUM

March 27, 2018

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

From: Kenneth Johnson, Chief Operating Officer

KENNETH JOHNSON Digitally signed by KENNETH JOHNSON Date: 2018.03.27 12:37:08 -04'00'

Subject: Management Response to Draft Report No. 546, "Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2017"

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 of 2014 (FISMA) for fiscal year (FY) 2017 (Report No. 546). The report provides a snapshot of the SEC's FISMA program as of September 30, 2017. Since that date, the agency has completed or undertaken a broad range of actions, pursuant to Chairman Clayton's cybersecurity uplift initiative, to strengthen and improve the agency's cybersecurity protections.

The report evaluates the SEC's Information Security Program in accordance with the FY17 Inspector General FISMA Reporting Metrics[1], which are designed to assist IGs in assessing the maturity levels of controls across seven domains aligned to the NIST Framework for Improving Critical Infrastructure Cybersecurity.

I am pleased that you found that the SEC improved its information security program and made progress towards implementing previous OIG recommendations. Since the end of the evaluation period, we completed corrective actions for two of the remaining four open recommendations from your FY16 FISMA report. Corrective action is expected to be completed in early spring on the other two recommendations.

We appreciate the professionalism and courtesies provided by the OIG staff during this audit and we look forward to working with your office to address the areas noted in your report.

Below, we have outlined the actions we intend to take pertaining to each recommendation issued in your draft report.

[1] U.S. Department of Homeland Security, *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, Version 1.0; April 17, 2017.

Recommendation 1: Define and implement a process that includes clear roles and responsibilities for developing and maintaining a comprehensive and accurate inventory of agency information systems whether or not the systems are designated as major information systems.

Response: OIT concurs that it is important to maintain a comprehensive and accurate inventory of SEC information systems (including cloud systems, public facing websites, and third party systems), and system interconnections. While the SEC has compiled and maintains a centralized inventory of all major information systems pursuant to FISMA, (b) (7)(E) (b) (7)(E) OIT recently worked with stakeholders across SEC offices and divisions to compile an inventory of agency systems, applications, and datasets. (b) (7)(E) (b) (7)(E)

Recommendation 2: Define and implement a process (b) (7)(E) (b) (7)(E)

Response: OIT concurs that it is important to maintain a comprehensive and accurate inventory of system interconnections. In late FY 2017, OIT implemented a new process for creating, approving, maintaining, and updating Interconnection Security Agreements (ISAs) and Memoranda of Understanding (MOU). (b) (7)(E) (b) (7)(E)

Recommendation 3: Define and implement a process to develop and maintain up-to-date inventories that include detailed information necessary for tracking and reporting of hardware assets connected to the agency's network, and (b) (7)(E) (b) (7)(E)

Response: OIT concurs that it is important to maintain up-to-date hardware (b) (7)(E) (b) (7)(E) As you noted in your report, OIT has defined policies and procedures in place for maintaining the agency's hardware inventory and is continuing to mature its (b) (7)(E) Pursuant to this recommendation, OIT will continue to work towards implementing its (b) (7)(E) (b) (7)(E)

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

Recommendation 4: Perform a comprehensive review of its processes and resource needs to adequately support the agency's security assessment and authorization program (including creating and managing plans of action and milestones) and, based on the results, take corrective action to ensure plans of action and milestones are timely documented, periodically updated, and accurately reflected in internal reports.

Response: OIT concurs that it is important to have the necessary processes and resources to carry out the agency's security assessment and authorization program. Pursuant to this recommendation, OIT will perform a review to evaluate if current resource levels are sufficient to support the completion and management of security assessments, authorizations, and processes that ensure POA&Ms are timely documented, periodically updated, and accurately reflected in internal reports.

Recommendation 5: (a) Continue efforts to define and formalize a plan addressing how enterprise architecture program management will be integrated with other institutional management disciplines, such as organizational strategic planning, strategic human capital management, performance management, information security management, and capital planning and investment control; and (b) define and implement a process to ensure information technology initiatives undergo an enterprise architecture compliance review before funding.

Response:
OIT concurs that that the overall value proposition of EA is intrinsically linked to its ability to support enterprise architecture across strategic, business, data, application, infrastructure, and security levels. In January 2018, the agency updated SECR 24-1.6 (Rev. 2) "SEC Regulation for Enterprise Architecture" which specifically states: "The EA shall be fully integrated with the SEC's IT capital planning process, serving to inform, guide, and manage IT investment decisions." Also in May 2017, the Agency released SECR 24-02 (Rev. 2.1) which defines the SEC's information technology (IT) capital planning and investment control (CPIC) policy and processes, and the responsibilities for complying with key provisions in regards to enterprise architecture and security compliance. OIT is firmly committed to aligning the strategic direction for EA, captured in the annually updated SEC EA Strategic Plan, to these and other critical drivers.

Pursuant to this recommendation, OIT will continue refining the SEC's enterprise architecture to include completion of the (b) (7)(E) [redacted] that will address how security elements of the SEC's enterprise architecture are integrated across the enterprise, business process, and system levels. OIT will also define and implement a process designed to ensure IT initiatives go through EA reviews, including application of the (b) (7)(E) [redacted] prior to funding. Additionally, OIT will link the (b) (7)(E) [redacted] to components within the enterprise and to the IT strategic plan in order to

illustrate how business functions are currently supported and how future investments will support these functions. Finally, OIT will continue to engage the SEC business community to see that all information technology decisions and initiatives are governed by the (b) (7)(E) one of the foundational elements of which is architectural compliance.

Recommendation 6: Continue efforts to implement a comprehensive risk management strategy by (a) clearly defining and communicating roles and responsibilities for tier 1 and tier 2 information security risks and the risk executive function; and (b) identifying and defining requirements for an automated enterprise-wide solution to provide a centralized view of information security risks across the organization.

Response: OIT, in coordination with the Office of the Chief Operating Office (OCOO), concurs that it is important that roles and responsibilities for tier 1 and tier 2 information security risks as well as the risk executive function be clearly defined. To meet a related recommendation from the FY16 FISMA report, the OCOO, in coordination with OIT, developed an enterprise risk management strategy that details how the agency's risk management program conforms to guidance specified in NIST SP 800-39 and outlines roles and responsibilities, including those associated with the risk executive function. Also, pursuant to this recommendation, OIT will coordinate with OCOO to identify, define requirements for, and implement an automated solution to provide a centralized enterprise-wide view of information security risks across the organization, including considerations identified by NIST.

Recommendation 7: Improve the agency's acquisition of information systems, system components, and information system services by coordinating with the Office of Acquisitions to (a) identify, review, and modify as necessary the agency's existing information technology contracts (including those we reviewed) to ensure the contracts include specific contracting language, such as information security and privacy requirements, material disclosures, Federal Acquisition Regulation clauses, and clauses on protection, detection, and reporting of information; and (b) define and implement a process to ensure that future acquisitions of information technology services and products include such provisions.

Response: The Office of Acquisitions (OA) and OIT concur that it is important to ensure that all applicable agency contracts include specific contracting language, such as information security and privacy requirements, material disclosures, Federal Acquisition Regulation clauses, and clauses on protection, detection, and reporting of information. While OA has procedures in place to ensure that all new contracts have the required clauses and provisions and other required contract terms and conditions, older contracts may not contain the most updated security and privacy-related provisions. Pursuant to this recommendation, (a) OA and OIT will develop a risk-based approach to review and update existing, applicable technology contracts to ensure all appropriate provisions are included, (b) OIT will review its processes for ensuring all IT related requirements in statements of work and purchase request packages include complete and up to date provisions, and (c) OIT will review its processes for ensuring applicable changes and

updates (such as references the latest versions of NIST and OMB guidance) are made to existing technology contracts.

Recommendation 8: Develop, review, and approve secure baselines for all systems included in the (b) (7)(E)
(b) (7)(E)

Response: OIT concurs that it is important to define security baselines for its enterprise systems and platforms. Currently, (b) (7)(E)
(b) (7)(E) of the SEC environment. The SEC's
(b) (7)(E) represents an internal accounting of planned and completed security baseline development efforts. Pursuant to this recommendation, OIT will develop (b) (7)(E)
(b) (7)(E)

Recommendation 9: Define and implement a process, including roles and responsibilities, to routinely: (a) (b) (7)(E)
(b) (7)(E) (b) perform (b) (7)(E) of all devices within the agency's network; and (c) document, track, and address the (b) (7)(E)
(b) (7)(E) including those issues and vulnerabilities identified as unmitigated at the time of our audit.

Response: (b) (7)(E)
(b) (7)(E)

(b) (7)(E)

Recommendation 10: Update its existing processes to ensure that the Information Security Office consistently performs and documents security impact analyses for proposed configuration changes before implementation.

Response: OIT concurs that is important to ensure proposed configuration changes are reviewed for information security risks prior to implementation. Information security personnel serve on OIT's Change Control Board (CCB), and consider the security impact of all changes during CCB meetings. Although most decisions are formally documented through security impact analyses and related documents, certain configuration changes are reviewed and discussed orally and may not be captured in meeting minutes. Pursuant to this recommendation, OIT will review and update CCB procedures, as applicable; to clarify the manner in which security impact analyses should be captured.

Recommendation 11: Develop and implement a transition plan or strategy, including milestones and priorities, for aligning the agency's identity, credential, and access management strategy with Federal initiatives.

Response: OIT concurs that it is important to have an identity, credential, and access management (ICAM) strategy in place to guide ICAM processes. OIT has developed identity and access management policies, procedures, and processes, many of which are in place. However, the current policies and procedures do not describe how OIT meets the federal government-wide identity, credential, and access management (FICAM) standards. Pursuant to this recommendation, OIT will develop a strategy document that describes how the SEC currently complies with FICAM standards.

Recommendation 12: (b) (7)(E)
(b) (7)(E)

Response: (b) (7)(E)
(b) (7)(E)

Recommendation 13: (b) (7)(E)
(b) (7)(E)

Response: (b) (7)(E)
(b) (7)(E)

(b) (7)(E)

Recommendation 14: Consider implementing an automated mechanism to centrally document, track, and share risk designations and screening information with necessary parties, as appropriate.

Response: The Office of Security Services (OSS) concurs that the agency should consider employing a fully automated risk designation tracking system. (b) (7)(E)
(b) (7)(E)

(b) (7)(E) Pursuant to this recommendation, the OSS will consider the costs and benefits of implementing an automated mechanism to centrally document, track, and share risk designations and screening information with necessary parties and document the results of their findings.

Recommendation 15: Develop and implement a process to ensure that all individuals with significant security responsibilities receive required specialized training before gaining access to information systems or before performing assigned duties.

Response: OIT concurs that is important to ensure specialized security training is provided to all individuals with significant security responsibilities. Currently, users with significant security responsibilities are required to complete additional training annually. However, this training is not always completed prior to users performing assigned duties. Pursuant to Recommendation #10 from the OIG's FY16 FISMA report, the Office of

Human Resources (OHR) has invested in a technical solution to facilitate the tracking and completion of security training prior to authorizing network access and is in the process of implementing this solution. Pursuant to this recommendation, OIT will continue to work with OHR to implement this capability to ensure that personnel with significant security responsibilities complete training before performing their assigned duties. Further, OIT will adjust account management protocols to ensure training is completed prior to granting privileged access to the SEC's network or information systems.

Recommendation 16: Update the existing continuous monitoring strategy to define (a) qualitative and quantitative performance measures or data that should be collected to assess the effectiveness of the agency's continuous monitoring program; (b) procedures for reviewing and modifying all aspects of the agency's continuous monitoring strategy; and (c) the agency's ongoing authorization process.

Response: OIT concurs that is important to develop and use a continuous monitoring strategy, and that the implementation plans include derivation and use of measurements, whether qualitative or quantitative. Pursuant to this recommendation, OIT will update existing policies and procedures to define qualitative and quantitative performance measures on the continuous monitoring program. Further, OIT will create an ongoing authorization strategy that will define timeframes and a roadmap to achieve ongoing authorization.

Recommendation 17: Review and update incident response plans, policies, procedures, and strategies to (a) address all common threat and attack vectors and the characteristics of each particular situation; (b) identify and define performance metrics that will be used to measure and track the effectiveness of the agency's incident response program; (c) develop and implement a process to ensure that incident response personnel obtain data supporting the incident response metrics accurately, consistently, and in a reproducible format; (d) define incident response communication protocols and incident handlers' training requirements; and (e) remove outdated terminology and references.

Response: OIT concurs that it is important to have updated incident response policies and procedures. As you detailed in your report, the SEC has developed incident response policies and procedures. However, the existing policies and procedures did not always align with all elements listed within NIST 800-61. Pursuant to this recommendation, OIT will review and update existing incident policies and procedures to ensure they align with requirements from NIST 800-61. Also, OIT will update applicable policies and procedures to define protocols for common threat and attack vectors. OIT will also review and update the procedures that describe how performance metrics are used to measure and track the effectiveness of the agency's incident response program. Separately, OIT will review training requirements for incident handlers. OIT is currently updating the agency's Incident Management Plan to ensure that outdated terminology and references are removed.

Recommendation 18: Fully implement processes to (a) consistently document and timestamp every step in the incident response process from detection to resolution; and (b) ensure a person other than the incident ticket creator reviews incident documentation (including logs and tickets), and confirms that consistent and complete information is maintained for every step in the incident response process.

Response: OIT concurs that it is important to document actions that take place during incident response activities. OIT utilizes a centralized system that automatically reports incidents and captures logs and timestamps of analyst's input updates on incidents. However, OIT has not currently defined what key milestones should be timestamped and input into the incident response system during the incident response process. Pursuant to this recommendation, OIT will define key milestones that need to be supplied to the incident response system and will develop supporting procedures to ensure that analysts follow the process. Further, pursuant to this recommendation, OIT will revisit existing quality control processes and update the processes to ensure they are effective.

Recommendation 19: Improve its ability to review indicators of compromise by (b) (7)(E) [redacted]

Response: OIT concurs that it is important to have incident response technologies in place and implemented. OIT is continuously striving to increase the effectiveness of its information security controls including the areas of web application protection, event and incident response management, aggregation and analysis, malware detection, information management, and file integrity and endpoint security tools. (b) (7)(E) [redacted]

Recommendation 20: Perform an assessment of existing incident response reporting mechanisms, and develop a process to periodically measure and ensure the timely reporting of incidents to agency officials and external stakeholders.

Response: OIT concurs that it is important to periodically conduct assessments on incident reporting mechanisms to ensure timely reporting of incidents to agency officials and external stakeholders. (b) (7)(E) [redacted]

(b) (7)(E)

(b) (7)(E) Pursuant to this recommendation, OIT will complete a (b) (7)(E) assessment and evaluate the associated recommendations and/or corrective actions.

Major Contributors to the Report

Kelli Brown-Barnes, Audit Manager

Sara Tete Nkongo, Lead Auditor

Jacob Dull, Auditor

John Dettinger, Auditor

Mike Burger, Auditor

Sumeer Ahluwalia, 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, 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.