U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Federal Information Security Management Act: Fiscal Year 2014 Evaluation

February 5, 2015
Report No. 529

REDACTED FOR PUBLIC RELEASE

REDACTED FOR PUBLIC RELEASE

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

February 5, 2015

TO: Jeffery Heslop, Chief Operating Officer, Office of the Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General, Office of Inspector General

SUBJECT: *Federal Information Security Management Act: Fiscal Year 2014 Evaluation*, Report No. 529

Attached is the Office of Inspector General's (OIG) final report detailing the results of the fiscal year 2014 evaluation of the U.S. Securities and Exchange Commission's (SEC) information security program and practices. Networking Institute of Technology, Inc., under a contract issued by the OIG, performed the evaluation.

On January 15, 2015, we provided you with a draft of the report for your review and comment. Based on management's response and our review of information provided by the Office of Information Technology, we deleted one recommendation (draft report Recommendation 3) that was in the draft report. As a result, the attached final report contains seven recommendations for corrective action that, if fully implemented, should strengthen the SEC's information security posture. Management fully concurred with these seven recommendations. We have included management's response as Appendix IV in the final report.

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

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

Attachment

cc: Mary Jo White, Chair
Erica Y. Williams, Deputy Chief of Staff, Office of the Chair
Luis A. Aguilar, Commissioner
Paul Gumagay, Counsel, Office of Commissioner Aguilar
Daniel M. Gallagher, Commissioner
Benjamin Brown, Counsel, Office of Commissioner Gallagher

Michael S. Piwowar, Commissioner
Jamie Klima, Counsel, Office of Commissioner Piwowar
Kara M. Stein, Commissioner
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein
Anne K. Small, General Counsel, Office of the General Counsel
Timothy Henseler, Director, Office of Legislative and Intergovernmental Affairs
John J. Nester, Director, Office of Public Affairs
Pamela C. Dyson, Director (Acting), Office of Information Technology
Barry Walters, Director, Office of Support Operations/Chief FOIA Officer
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

Executive Summary

Federal Information Security Management Act: Fiscal Year 2014 Evaluation
Report No. 529
February 5, 2015

Why We Did This Evaluation

The U.S. Securities and Exchange Commission's (SEC) information systems process and store significant amounts of sensitive, nonpublic information including information that is personally identifiable, commercially valuable, and market-sensitive. The SEC's information security program protects the agency from the risk of unauthorized disclosure, modification, use, and disruption of this sensitive, nonpublic information. Without these protections, 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 Management Act of 2002 (FISMA), the SEC Office of Inspector General (OIG) contracted the services of Networking Institute of Technology, Inc. (referred to as "we" in this report) to independently evaluate the SEC's implementation of FISMA information security requirements.

What We Recommended

To provide reasonable assurance that the SEC's information security program is effective, we urge management to take action on all outstanding recommendations from the fiscal year 2011, 2012, and 2013 FISMA evaluations. We also made seven new recommendations that address (a) outdated ATOs and controls over the ATO process; (b) developing and implementing insider threat training; (c) developing a PIV card policy; (d) ensuring the method of access is defined for external systems; and (e) conducting reviews of user accounts. In response to a draft of this report, management concurred with the recommendations. Also, based on management's response, we deleted one recommendation that was in the draft report.

What We Found

The SEC Office of Information Technology (OIT) has overall management responsibility for the SEC's information technology (IT) program, including information security. Since last year, OIT has made progress in key areas of information security, including in the agency's management of its continuous monitoring, configuration, and identity and access controls. However, we found that:

- three production systems did not always have a current authorization to operate (ATO); and
- the SEC's security awareness training did not include the required insider threat component.

These weaknesses existed, in part, because OIT management did not establish adequate controls or ensure that ATOs were up-to-date and risks were accepted, and that security awareness training included training on insider threats.

In addition, OIT has not addressed several areas of potential risk identified in prior FISMA evaluations. These include

(1) failure to implement personal identity verification (PIV) cards for logical access to the maximum extent practicable;
(2) A lack of full implementation of continuous monitoring;
(3) a lack of multi-factor authentication for external systems;
(4) outdated procedures and inconsistencies with policy; and
(5) improper review of user accounts.

Thus, these areas continue to be weaknesses in the fiscal year 2014 FISMA evaluation.

Also, while evaluating the SEC's compliance with FISMA, we identified two other matters of interest related to the agency's IT environment. Specifically, we identified that (b)(7)(E) (b)(7)(E) system security assessment may not be comprehensive or adequately address system and subsystem risks. Also, OIT did not take action to address some known vulnerabilities (recorded on plan of action and milestone documents) within established timeframes. In some cases, these items – which represent both moderate and low risk – have been open for 2 to 6 years beyond established remediation dates. Although these matters did not result in findings within this report, we encourage OIT management to consider these matters and ensure that sufficient controls exist.

For additional information, contact the Office of Inspector General at (202) 551-6061 or www.sec.gov/about/offices/inspector_general.shtml.

TABLE OF CONTENTS

ABBREVIATIONS

ALJ	Administrative Law Judges
AO	authorizing official
ATO	authorization to operate
(b)(7)(E)	(b)(7)(E)
CIO	chief information officer
DHS	U.S. Department of Homeland Security

(b)(7)(E)	
FedRAMP	Federal Risk and Management Program
FISMA	Federal Information Security Management Act of 2002
FY	fiscal year
HSPD	Homeland Security Presidential Directive
ISCM	information system continuous monitoring
IT	information technology
(b)(7)(E)	
NIST	National Institute of Standards and Technology
NIT	Networking Institute of Technology, Inc.
(b)(7)(E)	
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PII	personally identifiable information
PIV	personal identity verification
POA&M	plan of action and milestones
Rev.	Revision
SEC	U.S. Securities and Exchange Commission
SECR	SEC Regulation
SP	special publication
(b)(7)(E)	

Background and Objectives

Background

The Federal Information Security Management Act of 2002 (FISMA)[1] provides the framework for securing the Federal government's information technology (IT) and ensuring the effectiveness of security controls over information resources that support Federal operations and assets. Failure to meet FISMA information security requirements could lead to unauthorized access to information systems and the unauthorized disclosure of sensitive, nonpublic information,[2] including personally identifiable information (PII),[3] which may inhibit agencies' ability to accomplish their missions. FISMA requires agency program officials, chief information officers (CIO), privacy officers, and Inspectors General to conduct annual reviews of agency information security and privacy programs and report the results to the Office of Management and Budget (OMB) and the U.S. Department of Homeland Security (DHS).

The U.S. Securities and Exchange Commission's (SEC) Office of Inspector General (OIG) contracted the services of Networking Institute of Technology, Inc. (NIT) to independently evaluate the SEC's implementation of FISMA information security requirements; and determine the adequacy and effectiveness of the SEC's information security program's policies, procedures, and practices. The results of the evaluation supported the OIG's fiscal year (FY) 2014 Cyberscope submission to OMB and DHS.[4]

Federal Laws and Guidance. Federal information security laws establish security controls to prevent unauthorized access to information systems and to protect sensitive, nonpublic information from compromise and unauthorized disclosure. FISMA establishes government-wide requirements for Federal departments and agencies, including the SEC.

[1] 44 U.S.C. § 3541, et seq.

[2] 5 C.F.R. § 2635.703(b), *Standards of Ethical Conduct for Employees of the Executive Branch*, defines "nonpublic information" as "information that the employee gains by reason of Federal employment and that he knows or reasonably should know has not been made available to the general public. It includes information that he knows or reasonably should know . . . [i]s designated as confidential by an agency; or [h]as not actually been disseminated to the general public and is not authorized to be made available to the public on request."

[3] Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, defines PII as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

[4] Beginning FY 2010, Cyberscope is the platform CIOs, privacy officers, and Inspectors General are to use to meet FISMA reporting requirements. The SEC OIG completed its FY 2014 Cyberscope submission on November 14, 2014.

OMB has also established guidance to minimize the risk of unauthorized access to Federal agencies' information systems. Specifically, OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12- Policy for a Common Identification Standard for Federal Employees and Contractors,* includes a plan of action for agencies that will expedite the Executive Branch's full use of personal identity verification (PIV) credentials to access Federal facilities and information systems.[5] OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*, further emphasizes ensuring the confidentiality, integrity, and availability of Federal information and information systems.[6]

Finally, in furtherance of its statutory responsibilities under FISMA, the National Institute of Standards and Technology (NIST) publishes Federal guidelines specific to IT security.[7] NIST special publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013) prescribes information system security controls that are designed to: (i) protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/organizations; and (ii) satisfy a set of defined security requirements.[8] NIST organizes the security requirements into 18 security and 8 privacy families of controls.[9]

SEC Regulations, Policies, and Procedures. SEC regulations, policies, and procedures address controls over IT security. The agency's primary, overarching IT security policy is *SEC Regulation* (SECR*)* 24-04*,* SEC [Office of Information Technology] OIT CIO Policy Directive CIO PD-08-06, *SEC Information Security Program,* version *2*, March 18, 2014, and accompanying manual, *Information Security Controls Manual*, version 2, April 4, 2014. According to SECR 24-04, several individuals share responsibility for establishing and maintaining an organization-wide information security program and include the following:

---

[5] OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractors*, February 3, 2011, p. 1, paragraphs 1 and 3.

[6] OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*, November 18, 2013, p. 1, paragraph 1.

[7] NIST develops standards and guidelines, including minimum requirements, for adequate information security for all Federal agency operations and assets, excluding national security systems.

[8] NIST SP 800-53, Rev. 4, p. 1, Chapter 1, Introduction, paragraph 1.

[9] The 18 security control families are access control; awareness and training; audit and accountability; security assessment and authorization; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; system and services acquisition; system and communications protection; system and information integrity; and program management. NIST SP 800-53, Rev. 4, p. 9, Chapter 2, Security Control Structure.

The 8 privacy control families are authority and purpose; accountability, audit, and risk management; data quality and integrity; data minimization and retention; individual participation and redress; security; transparency; and use limitation. NIST SP 800-53, Rev. 4, pp. J-2 – J-3.

- the agency head ensures that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of the SEC;
- the CIO develops and maintains an agency-wide information security program;
- the chief information security officer coordinates, develops, implements, and maintains an organization-wide information security program;
- information system owners are responsible for the technical operation of systems and support; and
- information owners (business owners) have operational authority for the specified information and are responsible for establishing controls for the information's generation, collection, processing, dissemination, and disposal.[10]

Objectives

The overall objective of the evaluation was to assess the SEC's implementation of the FY 2014 FISMA OIG Reporting Metrics issued by OMB and DHS and listed below:

- Configuration Management
- Contingency Planning
- Continuous Monitoring Management
- Contractor Systems
- Identity and Access Management
- Incident Response and Reporting
- Plan of Action and Milestones (POA&M)
- Remote Access Management
- Risk Management
- Security Capital Planning
- Security Training

[10] SECR 24-04, pp. 10-13.

To assess the SEC's compliance with FISMA, we judgmentally selected and reviewed a non-statistical sample of 8 out of 61 FISMA-reportable information systems (approximately 13 percent) at the SEC's headquarters.[11] The systems selected were (b)(7)(E) system.

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

[11] We selected the information systems based on the SEC's compliance workbook (inventory of information systems), dated July 3, 2014. The inventory included 60 major information systems and 1 general support system that were FISMA-reportable. OMB Memorandum A-130, Section 6.u (Revised) defines a "major information system" as "an information 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." A FISMA-reportable system is an information system that supports the operations and assets of the agency, and FISMA requires the agency to implement an agency-wide program for information security for those systems.

Results

Improvements Are Needed in the SEC's Information Security Program

To prevent the risk of unauthorized access to information systems and compromise of sensitive, nonpublic information, the OIT established an overarching policy for information security. This policy is generally consistent with applicable Federal laws and guidance. However, based on guidance issued by the OMB, DHS, and NIST, we evaluated the OIT's information security posture and identified needed improvements in the agency's information security practices. Specifically, we found that:

- three production systems did not always have a current authorization to operate (ATO); and
- the SEC's security awareness training did not include the required insider threat component.

These weaknesses existed, in part, because OIT management did not establish adequate controls or ensure that ATOs were up-to-date and risks were accepted, and security awareness training included training on insider threats.

In addition, OIT has not addressed several areas of potential risk identified in prior FISMA evaluations. These include (1) failure to implement PIV cards for logical access to the maximum extent practicable; (2) a lack of full implementation of continuous monitoring; (3) a lack of multi-factor authentication for external systems; (4) outdated procedures and inconsistencies with policy; and (5) improper review of user accounts. Thus, these areas continue to be weaknesses in the FY 2014 FISMA evaluation.

Three Systems Remained in Operation Without Current ATOs. According to NIST[12] and SEC policy, the Authorizing Official (AO) grants an ATO and authorizes an information system to operate. Specifically, SEC policy states that an ATO is granted "to authorize operation of an information system and to explicitly accept any residual risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation".[13] The organization's AO makes the determination to authorize each system. Section 8.2 of SECR 24-04 requires that the CIO, serving as the SEC's AO,

[12] NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010, pp. 35-36, Chapter 3, Task 5-4.

[13] SECR 24-04, p. 8, Section 7.10 and p. 11, Section 8.2.

> formally assum[e] responsibility and accountability for operating information systems at an acceptable level of risk to operations, assets, and individuals.[14]

After reviewing the risks identified in each system's security assessment package and determining that these risks are at an acceptable level and would not negatively impact the agency's operations, assets, or individuals, the AO (in coordination with the business and system owners) grants an ATO. Once signed by the AO, the ATO is effective for 3 years. In accordance with SEC policy, when an ATO expires, a new security assessment should be completed and the AO should sign a new ATO.[15]

While the SEC's policy for authorizing systems to operate is consistent with NIST standards, OIT is not consistently following the policy. Specifically, the ATOs for three (b)(7)(E) systems (b)(7)(E) expired but the systems continued to operate. Without a current ATO, the AO should have removed such systems from production because OIT had not reassessed the risks to agency operations that could have occurred due to changes in system environments since the last security assessment. Instead, in one instance, the CIO relied on multiple ATO extensions as a stop-gap measure without reassessment or testing of system security controls. In two other instances, systems operated for as long as 2 years without an ATO.

Since OIT had not reassessed the security controls for the systems, new vulnerabilities could be present. As a result, the systems may have operated with unknown risks to the SEC and could have been exposed to unauthorized disclosure, modification, use, and disruption.

The three systems we reviewed without current ATOs were (1) (b)(7)(E) (b)(7)(E) Each system is discussed in detail below.

(b)(7)(E)

AO authorized the (b)(7)(E) to operate on (b)(7)(E) and the ATO expired 3 years later on (b)(7)(E) Prior to the expiration of the ATO, OIT should have completed a security assessment for the (b)(7)(E) which would have potentially identified any new risks. Then, the AO should have either (1) deemed the risks acceptable and issued a new ATO, or (2) removed the system from production until the risks were remediated and the system was approved to operate. However, OIT did not

[14] SECR 24-04, p. 11.

[15] Section 7.10 of SECR 24-04 states, "The system security assessment and authorization (SA&A) process is essential to ensuring system compliance with security controls throughout the lifecycle. The SA&A process begins during system development and continues even after authorization to operate is granted…."

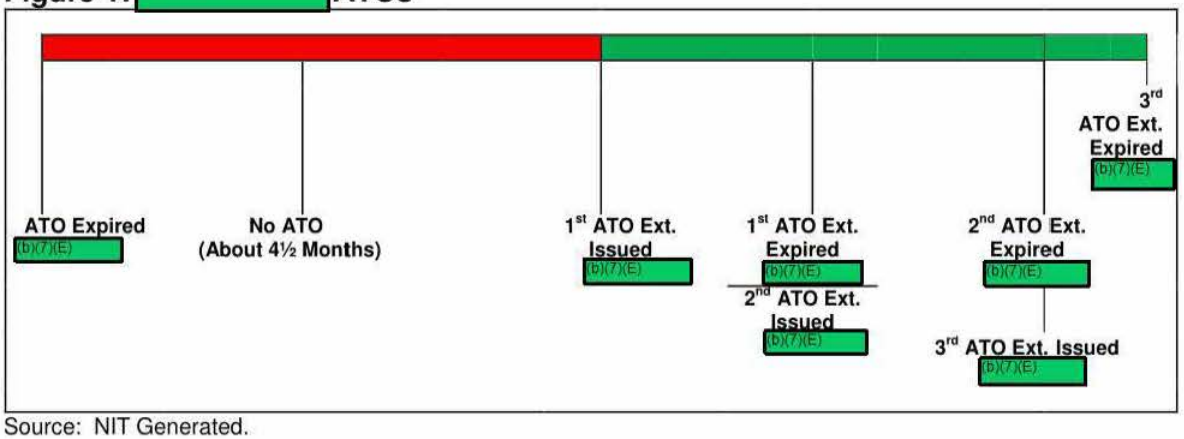
(b)(7)(E)

perform the security assessment before the ATO expired and had not completed a system risk assessment as of [redacted] Instead of conducting the security assessment and identifying potential risks posed by [redacted] OIT allowed the [redacted] to remain operational for approximately 4 and a half months without a current ATO. In addition, although OIT did not conduct a security assessment, on [redacted] the AO issued [redacted] ATO extensions for [redacted]

The first ATO extension expired 180 days from the expiration of the original ATO (or on [redacted][17] As shown in Figure 1, the AO signed the second ATO extension for [redacted] on [redacted] Then, on [redacted] the second ATO extension for [redacted] expired. On the same day, OIT officials signed and issued another ATO extension, which expired on [redacted] As reported in [redacted] OIT officials were planning to conduct a targeted system risk assessment and review known system vulnerabilities recorded on POA&M documents for [redacted] beginning in [redacted] Since [redacted] OIT completed the targeted risk assessment (consisting of conducting penetration testing and vulnerability scanning) and issued an ATO on [redacted] The ATO expires on [redacted]

Since the first [redacted] ATO expired in [redacted] the AO continued to provide ATO extensions without assessing system security controls or risks to agency operations, or ensuring that such risks were mitigated while the system remained operational. In addition, although [redacted] had one period where the system was not approved to operate and three ATO extensions without a current security assessment, the system remained in production and operational without the proper authorization. (See Figure 1.)

Figure 1: [redacted] ATOs



Source: NIT Generated.

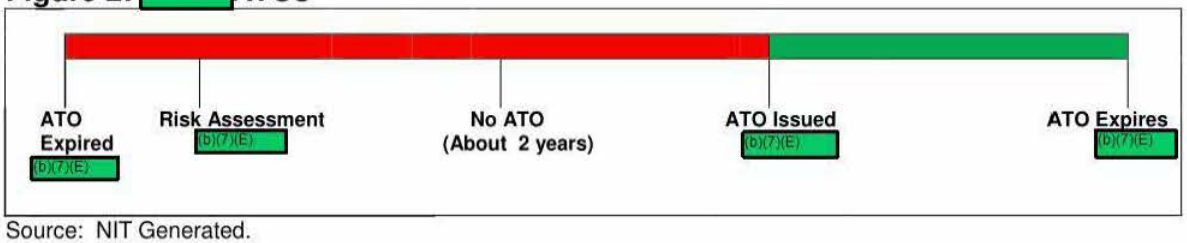
[17] The first interim ATO for [redacted] states, "Accordingly, I am issuing a 180-day extension to the previous [ATO] dated [redacted] for the information system in its existing operating environment." However, as noted, the previous ATO was dated [redacted]

OIT officials informed us that the OIT issued ATO extensions for [redacted] The AO authorized [redacted] to operate on [redacted] and the ATO expired 3 years later on [redacted] On [redacted] OIT completed a system risk assessment and identified moderate and low risk concerns. Based on the results of the system risk assessment, the AO did not sign a new ATO or an ATO extension although the system remained operational.

According to documents received from OIT, an "[ATO] meeting was held [redacted] to discuss the results [of the system risk assessment], but the decision was made not to issue an ATO until progress was made in closing the more serious findings. [Testing was performed] [redacted] and determined all five of the Moderate risk findings had been remediated. Five of the seven remaining (Low risk) findings were closed in the period between [redacted] ATO meeting and [redacted]"

In fact, the AO did not sign a new ATO [redacted] approximately 2 years after the initial ATO expired and 8 months after OIT remediated the findings from the [redacted] system risk assessment. The new ATO expires on [redacted] (See Figure 2.)

Figure 2: [redacted] ATOs

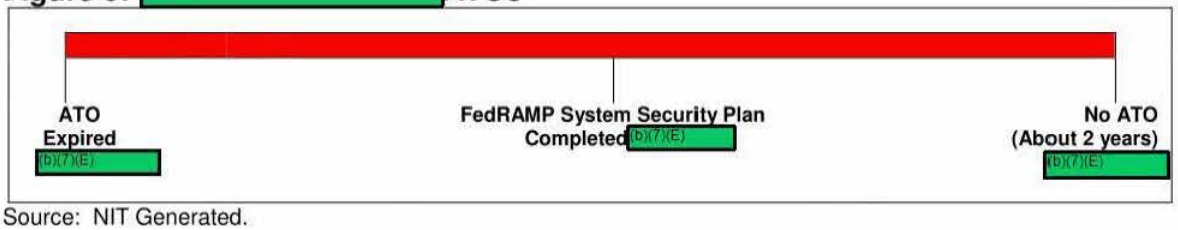


Source: NIT Generated.

OIT informed us that the AO did not sign an ATO based on the risks identified as a result of the [redacted] system risk assessment; however, due to the business impact of shutting down the system [redacted] remained operational for 2 years although the system was not authorized to operate. In addition, although OIT remediated the risks for [redacted] in [redacted] the AO did not issue a new ATO until [redacted] Because of such an extended length of time between identifying and remediating risks and issuing a new ATO, the system may have operated with unknown risks due to possible changes in the system environment.

(b)(7)(E) is an external, cloud system[18] that allows the (b)(7)(E) The AO signed the system's ATO on (b)(7)(E) and the authorization expired on (b)(7)(E) however, as of the date of our testing (b)(7)(E), the AO had not signed a new ATO although the system remained operational. According to OIT officials, they were waiting for the SEC's vendor to complete a required Federal Risk and Authorization Management Program (FedRAMP)[19] evaluation before re-authorizing (b)(7)(E) to operate. Although the vendor completed the FedRAMP system security plan on (b)(7)(E) the SEC has not conducted a system risk assessment or evaluated the risks in order to issue a new ATO. (See Figure 3.)

Figure 3: (b)(7)(E) ATOs



Source: NIT Generated.

Lack of Required Insider Threat Training. NIST SP 800-53, Rev. 4 requires that security awareness training programs for moderate information systems, which includes (b)(7)(E) of the SEC's FISMA-reportable systems,[20] address how to recognize and report potential indicators of insider threats.[21] Consistent with NIST guidance, the SEC's overarching security policy and accompanying manual require that the agency's security awareness training (conducted by OIT) include "recognizing and reporting potential indicators of insider threat."[22] However, we found that the SEC's security awareness training does not address recognizing and reporting possible precursors of insider threats. Such precursors include

- long-term job dissatisfaction;
- attempts to gain access to information not required for job performance;
- unexplained access to financial records; and

[18] Cloud systems are systems that are stored off premises and managed by a service provider in a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services) or cloud. NIST SP 800-145, *The NIST Definition of Cloud Computing,* p. 2, Section 2.

[19] FedRAMP is a government-wide program that provides a standardized approach for evaluating cloud systems, and Federal agencies and cloud service providers are required to conduct evaluations for cloud systems based on the FedRAMP-established security controls baselines.

[20] Of the SEC's 61 FISMA-reportable systems included in the agency's July 3, 2014, inventory of information systems, (b)(7)(E) are moderate systems.

[21] NIST SP 800-53, Rev. 4, p. F-38, Appendix F, AT-2(2).

[22] *SEC Information Security Control Manual*, p. 12, Section 5.2.2.

- other serious violations of organizational policies, procedures, directives, rules, or practices.[23]

Without completing insider threat training consistent with NIST requirements, SEC staff may be unaware of how to identify and report instances of potential insider threats to the agency's information resources. Therefore, the SEC may not be able to adequately protect itself or its employees from the release of sensitive, nonpublic information, including PII, or from disruptions in its information systems.

During our evaluation, we determined that the SEC's Office of Support Operations is responsible for developing an insider threat program for the agency. As reported in our November 14, 2014, submission in Cyberscope, the Office of Support Operations expected to complete a project plan for the program by January 15, 2015.[24] The Office of Support Operations plans to work with OIT to develop insider threat training content for the security awareness training taken by all SEC staff (employees and contractors). The new content will address recognizing and reporting possible precursors of insider threats.

Areas of Potential Risk Identified in Prior FISMA Evaluations. OIT has not addressed several areas of potential risk identified in prior FISMA evaluations.[25] These include (1) failure to implement PIV cards for logical access to the maximum extent practicable; (2) a lack of full implementation of continuous monitoring; (3) a lack of multi-factor authentication for external systems; (4) outdated procedures and inconsistencies with policy; and (5) improper review of user accounts. Thus, these areas, discussed further below, continue to be deficiencies in the FY 2014 FISMA evaluation.

PIV Card for Logical Access Not Implemented to Maximum Extent Practicable. HSPD-12 requires that, to the maximum extent practicable, Federal employees and contractors meet the government-wide PIV card standard to gain logical access to information systems.[26] In addition, OMB identified the HSPD-12 PIV requirements for logical access as an administration priority and recommended that Federal agencies focus their resources on implementing the requirements.[27] However, we found that most SEC staff (employees and contractors) still do not use PIV cards for logical access to information systems, as previously reported by the OIG in the FY 2011, 2012, and 2013 FISMA evaluations.

---

[23] NIST SP 800-53, Rev. 4, p. F-38, Appendix F, AT-2(2).

[24] On January 12, 2015, the Office of Support Operations informed us that, due to delays, the project plan for the insider threat program is expected to be completed by February 13, 2015.

[25] SEC OIG's *Federal Information Security Management Act: Fiscal Year 2013 Evaluation*, Report No. 522, March 31, 2014; 2012 *FISMA Executive Summary Report*, Report No. 512, March 29, 2013; and 2011 Annual FISMA Executive Summary Report, Report No. 501, February 2, 2012. SEC OIG reports can be accessed at www.sec.gov/about/offices/inspector_general.shtml.

[26] HSPD-12, paragraph 4.

[27] *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics,* pp. 1-2 and 9.

The SEC issues PIV cards to staff (b)(7)(E) (b)(7)(E) Although, its desktop and laptop computers are equipped with card readers with HSPD-12 capability, the SEC generally uses PIV cards for physical access identification purposes rather than to access the agency's information systems. We were informed that while use of the PIV card for logical access has not been fully deployed, a select group of SEC staff are participating in a pilot program and use the PIV card for logical access to information systems based on their specific roles and responsibilities. For example, the Chief Information Security Officer uses a PIV card for logical access to information systems and to sign documents electronically. While the PIV card pilot program was initiated in April 2014, it was delayed due to workstation image incompatibility issues. As reported in our November 14, 2014, submission in Cyberscope, OIT was working to address these issues and planned to implement PIV cards for logical access to information systems for both SEC's headquarters and the regional offices by December 2014.[28] As a result of not implementing the PIV card, where practicable, the SEC is not in compliance with Federal requirements and is at a higher risk for unauthorized access to its information systems.

Because we previously recommended that the SEC implement PIV cards for logical access to agency information systems, we are not making a new recommendation. However, we strongly encourage OIT to take steps to mitigate the deficiencies in this area, as identified in the OIG's FY 2011, 2012, and 2013 FISMA evaluations.

We also determined that, despite OMB requirements, the current SEC policy, SECR 24-04, and accompanying manual do not require the use of PIV cards for logical access to the SEC's information systems, where practicable. OMB Memorandum 11-11 requires the agency to "develop and issue an implementation policy, by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems."[29] Therefore, the SEC should develop and issue the required implementation policy prior to requiring staff to use PIV cards to access the agency's information systems.

Continuous Monitoring Not Fully Implemented. As previously reported in the OIG's FY 2012 and 2013 FISMA evaluations, we found that OIT has developed an information system continuous monitoring (ISCM) strategy in accordance with OMB Memorandum M-14-03, but has not fully implemented it. We evaluated whether OIT has implemented its ISCM strategy, as required by OMB for Cyberscope submission.[30] While OIT is following many of the required actions and deadlines in accordance with OMB Memorandum M-14-03, such as developing the ISCM strategy based on

[28] As of December 26, 2014, OIT had implemented the technology to support PIV card utilization at the SEC for logical access to information systems at the agency's headquarters and regional offices. However, the SEC is not requiring, where practicable, PIV cards for logical access to its information systems.

[29] OMB Memorandum M-11-11, p. 2, paragraph 1.

[30] *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, p. 9, Section 3, Identity and Access, p. 6, Metrics 1.1.3 and 1.1.6.

evaluation of risk assessments, acquiring staff and resources, providing training, and preparing to submit information to the Federal dashboard, OIT is not fully implementing its ISCM strategy. Specifically, OIT is not conducting "periodic re-assessment of security controls selected for monitoring" in accordance with its ISCM strategy,[31] OMB, and NIST guidance.[32] OMB Memorandum M-14-03 states,

> While four initial information security capability areas have been identified on which agencies must automate and automatically report to DHS for integration to the Federal dashboard, this does not eliminate the need for agencies to monitor *all* security controls documented in their security plans and implemented within agency information systems and environments of operation.[33]

Although OIT conducts penetration testing and vulnerability scanning on a continuous basis to monitor the effectiveness of critical security controls, it is not assessing security controls based on the SEC ISCM strategy. (b)(7)(E)

(b)(7)(E)

We further found that OIT has not developed procedures for continuous monitoring, in accordance with its ISCM strategy.[34] In September 2014, the SEC awarded a contract to a vendor to perform security assessment and authorization services, among other services.[35] While a portion of the contract is to develop continuous monitoring procedures and implement the SEC ISCM strategy, the procedures have not yet been developed and the ISCM strategy has not been fully implemented as of the OIG's Cyberscope submission date. Further, OIT currently assesses security controls on (b)(7)(E) but intends to conduct periodic re-assessment of its security controls on a continuous basis based on the SEC ISCM strategy.

Lack of Multi-factor Authentication for External Systems. According to the *FY 2014* [IG] *Annual FISMA Reporting Metrics*, "A single-factor authentication mechanism, such as a username and password, is insufficient to block even basic attackers."[36] (b)(7)(E)

---

[31] *SEC Information Security Continuous Monitoring Strategy*, v2.0, April 7, 2014, p. 5, last paragraph, Bullet 3.

[32] NIST SP 800-53, Rev. 4, p. F-55, Appendix F and NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems*, September 2011, p. vii, paragraph 3, and p. 5, paragraph 1, Chapter 2.

[33] OMB Memorandum M-14-03, p. 10, Section: Implement ISCM.

[34] *SEC Information Security Continuous Monitoring Strategy*, v2.0, April 7, 2014, p. 3, Section 3.

(b)(7)(E)

[36] U.S. Department of Homeland Security, Office of Cyber Security and Communications, Federal Network Resilience, *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics,* p. 9, Section 3, Identity and Access.

(b)(7)(E) however, we found that two-factor authentication was not being employed by SEC users (both privileged and non-privileged) accessing (b)(7)(E) system over the Internet, as required by NIST.[37] Additionally, (b)(7)(E) the following weaknesses:

- (b)(7)(E)
- NIST requires that moderate-impact systems accessed remotely over untrusted networks have appropriate two-factor authentication; and
- [s]ince (b)(7)(E) is accessed over the Internet, it should employ some kind of two-factor authentication."

On September 17, 2014, we tested the single-factor login/password authentication for (b)(7)(E) system and found that a non-privileged user was able to log in to (b)(7)(E) over the Internet. Subsequently, OIT worked with the vendor for the (b)(7)(E) system to restrict access, (b)(7)(E) which requires two-factor authentication. We tested access to (b)(7)(E) system on October 27, 2014, and confirmed that (b)(7)(E) This issue was previously reported by the SEC OIG in the FY 2013 FISMA evaluation.

As a result of the FY 2013 finding, OIT recently updated the SEC policy requiring that (b)(7)(E) [38] Based on our review of the agency's (b)(7)(E) system (b)(7)(E)

Outdated Procedures and Inconsistencies with Policy. As previously reported by the SEC OIG in the FY 2011, 2012, and 2013 FISMA evaluations, OIT has not updated

NIST SP 800-53, Rev. 4, states that multi-factor authentication is "[a]uthentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric)." NIST SP 800-53, Rev. 4, p. B-14, Glossary.

[37] NIST SP 800-53, Rev. 4, p. F-91, Appendix F.

[38] (b)(7)(E) (b)(7)(E)

all of its IT security procedures in accordance with NIST guidelines[40] and its own policy or procedures.[41] Specifically, as shown in Appendix III, we reviewed OIT's IT security procedures and found that the agency has not updated 41 out-of-date security procedures, and

- approximately 95 percent (39 of the 41) still remained in the OIT policy library even though they were no longer consistent with the IT security policy;
- the 41 procedures were out of date by as many as 5 to 9 years; and
- approximately 56 percent (23 of the 41) were no longer relevant and/or have been recommended for retirement or partial retirement.

For example, the SEC's *Security Configuration of Windows 2000 Server Checklist* procedure refers to an operating system that is no longer in use at the SEC. The OIG previously reported this issue and management agreed to take corrective action. However, OIT has not yet updated all of its security procedures. According to OIT officials, OIT is in the process of updating its security procedures; however, OIT has not provided draft copies of the procedures for review or an expected completion date. Based on prior FISMA evaluations, OIT reported it has limited resources available to update its IT security procedures.

As a result of not updating the IT security procedures, OIT staff has not received adequate guidance to implement security procedures identified in NIST and management's expectations for implementing security controls throughout the SEC, which could result in OIT staff not acting in accordance with NIST standards.

Improper Review of User Accounts. As previously reported by the SEC OIG in the FY 2013 FISMA evaluation, OIT management improperly reviewed user accounts for the (b)(7)(E) system. In FY 2014, OIT management did not conduct an overall review of the user account review and recertification forms for its information systems. Specifically, OIT did not properly review user accounts for the (b)(7)(E) to ensure they were properly terminated or deactivated once a user's access was no longer required, in accordance with NIST guidelines[42] and its policy.[43] (b)(7)(E) internal user accounts, we found (b)(7)(E) (or about 9 percent) were identified as users needing access (b)(7)(E) but those accounts were no longer active. Once we notified OIT officials, they reviewed (b)(7)(E) user accounts and (1) determined whether the listed accounts were required; and (2) deleted (b)(7)(E) accounts that were not required. The (b)(7)(E) accounts were instances of

[40] NIST SP 800-53, Rev. 4, p. F-7, Access Control, p. F-37, Awareness and Training, p. F-55, Security Assessment and Authorization, p. F-64, Configuration Management, and p. F-103, Incident Response.

[41] The SEC is required to update procedures to reflect the agency defined frequency of 3 years as noted in the *SEC Information Security Controls Manual*, April 4, 2014, p. 1, Section 3.1.1, Revision Schedule; or the individual policy's or procedure's defined frequency as noted in the specific policy or procedure.

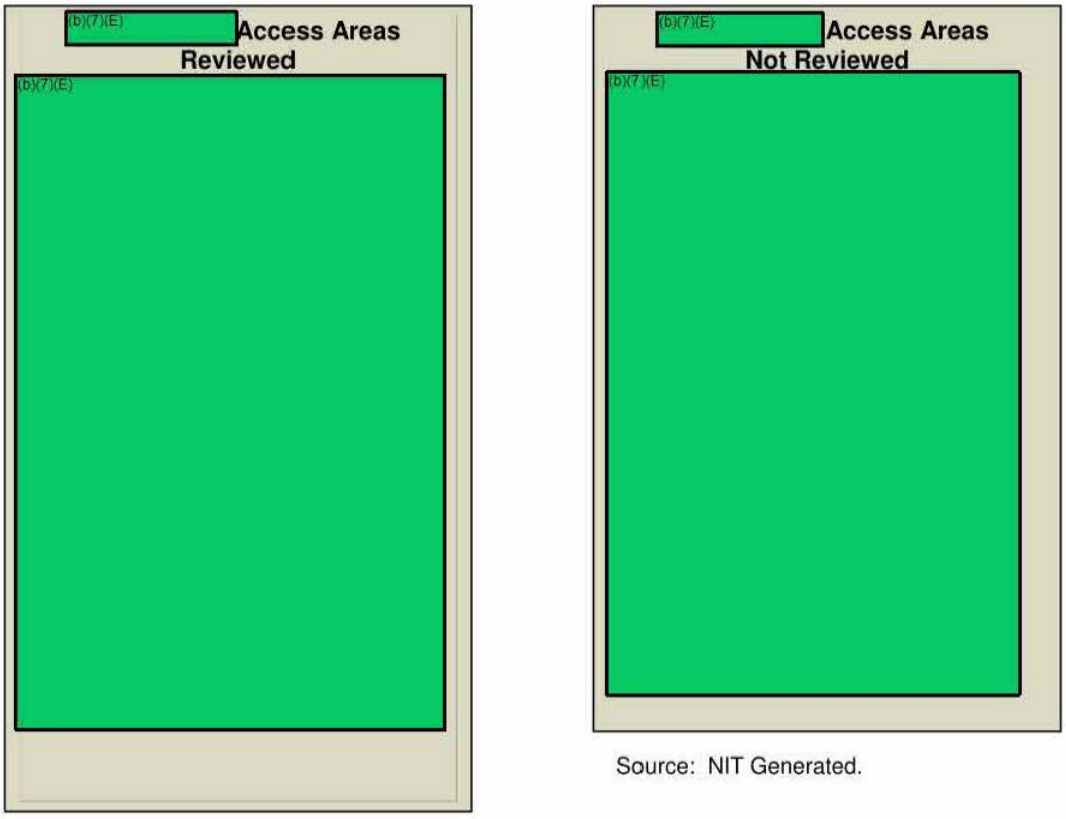
[42] NIST SP 800-53, Rev. 4, pp. F-7 – F-8.

[43] *SEC Information Security Controls Manual*, pp. 4 - 6, Sections 5.1.1 and 5.1.2.

personnel who changed their name, but did not complete the proper paperwork for the (b)(7)(E) Because of our evaluation, the paperwork process has been initiated for personnel with name changes.

We also found that system owners and business owners are required to review (b)(7)(E) user accounts for their particular access area (SEC region, office, division, etc.) and complete a user account review and recertification form. Out of (b)(7)(E) access areas, we found that (b)(7)(E) were reviewed and (b)(7)(E) were not reviewed, although 2 of the reviews were completed after we requested them.[44] (See Figure 4.)

Figure 4: (b)(7)(E) Access Areas



Source: NIT Generated.

For example, the San Francisco regional office completed the user review and recertification form 5 days after we requested it and 2 months after the user list was produced for the (b)(7)(E) Similarly, the Los Angeles regional office completed the user review and recertification form 1 day after it was requested.

As demonstrated in Figure 4 by an asterisk (*), the names of some of the SEC offices were inaccurate in (b)(7)(E) Because OIT is not updating the SEC offices within the system, the (b)(7)(E) inaccurately associates user names with offices that no longer exist. In addition, (b)(7)(E) user access review sheets signed by the

(b)(7)(E)

system/business owners do not include an accompanying list of users to ensure that the correct users have access [redacted] system/business owners are not conducting a thorough review of the user accounts and do not have adequate evidence of the user accounts they reviewed. As a result, unauthorized users may have access [redacted]

[redacted] requires a [redacted] account review. [redacted] administers it and is responsible for security administration, in terms of user accounts. We reviewed a list of [redacted] accounts, along with the user account review and recertification form dated [redacted][45] and found [redacted] accounts (or about 13 percent) were identified as users needing access to [redacted] those accounts were no longer active accounts at the SEC as of [redacted] we notified OIT officials who stated that the accounts have since been removed.

Additionally, we were unable to obtain a user account review and recertification form for [redacted] for 2014; however, we did obtain one for 2013. Finally, the user access review and recertification form and accompanying user list for [redacted] was completed on [redacted] after our second request for the information.

Because system owners and business owners are not reviewing or are incorrectly reviewing user accounts, and accounts are not being deactivated or terminated as needed, it may be possible for unauthorized users to gain access to the SEC systems.

OIT Management Did Not Establish Adequate Controls

The weaknesses that we observed existed, in part, because OIT management did not establish adequate controls or ensure that the systems in production had an up-to-date ATO and risks were accepted, and security awareness training included training on insider threats. In addition, OIT has not addressed several areas of potential risk identified in prior FISMA evaluations. For example, as previously stated and as reported in prior FISMA evaluations, while OIT has overall management responsibility for the SEC's IT program, including information security, many of the agency's IT security procedures have not been updated to support the overarching IT security policy.

The SEC's information systems process and store significant amounts of sensitive, nonpublic information including PII related to SEC employees and contractors, and commercially valuable and market-sensitive investor information. Based on guidance issued by the OMB, DHS, and NIST, we evaluated the SEC's information security posture and identified needed improvements in the agency's information security practices. If implemented, such improvements will help minimize the risk for the unauthorized disclosure, modification, use, and disruption of sensitive, nonpublic

[redacted]

information that could inhibit the SEC's ability to accomplish its mission as well as violate privacy laws and regulations that protect such information.

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

To improve the SEC's IT security program, OIT should take steps to immediately address the outstanding recommendations from the FYs 2011, 2012, and 2013 evaluations, and the SEC should implement the following new recommendations:

Recommendation 1: The Office of Information Technology should take all required steps, including performing security assessments, to determine whether systems in operation without a current authorization to operate – including the (b)(7)(E) (b)(7)(E) (b)(7)(E) should be re-authorized, and then either authorize or deactivate the systems as appropriate.

> **Management's Response.** The Office of Information Technology concurs with the recommendation. The Office of Information Technology plans to identify FISMA-reportable systems operating without a current, valid Authorization to Operate. Once identified, those systems will be assessed and then authorized with a new Authorization to Operate or deactivated as appropriate.
>
> **OIG's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the action taken.

Recommendation 2: The Office of Information Technology should develop and implement internal controls to ensure that (a) authorizations to operate do not expire, and (b) appropriate rationale is documented for issuing authorization to operate extensions.

> **Management's Response.** The Office of Information Technology concurs with the recommendation. The Office of Information Technology plans to implement an automated system for notification when an Authorization to Operate approaches its expiration date. In addition, a section will be added to the Authorization to Operate that will detail the rationale for issuing an extension.
>
> **OIG's Evaluation of Management's Response.** Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon completion and verification of the action taken.

Recommendation 3: The Office of Support Operations should coordinate with the Office of Information Technology to develop and implement the required insider threat training component of the agency's security awareness training program.

> **Management's Response.** The Office of Support Operations concurs with the recommendation and will work with the Office of Information Technology on implementation of insider threat training.

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

Recommendation 4: The Office of Information Technology should develop and implement a policy requiring, to the maximum extent practicable, the use of the personal identity verification card for logical access.

Management's Response. The Office of Information Technology concurs with the recommendation and will develop a policy and supporting procedures establishing the proper use of personal identity verification authentication for logical access, to the maximum extent practical. The ability to leverage personal identity verification cards for logical access to the SEC's network will be made available to all users.

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

Recommendation 5: The Office of Information Technology should review and update open Memorandums of Understanding, Interconnection Agreements, and/or contracts for externally-hosted systems, including (b)(7)(E) to ensure the method of remote access is defined and documented.

Management's Response. The Office of Information Technology concurs with the recommendation and will review and update Memorandums of Understanding, Interconnection Agreements, and/or contracts for externally-hosted systems to ensure the method of remote access is defined and documented.

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

Recommendation 6: The Office of Information Technology should coordinate with the business and information system owners to ensure that the (b)(7)(E) (b)(7)(E) accurately identifies the office names assigned to each active user.

Management's Response. The Office of Information Technology concurs with the recommendation and will work with the business and information system owners to validate the office names assigned to active (b)(7)(E) (b)(7)(E) users are accurate.

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

Recommendation 7: The Office of Information Technology should develop a process to annually review all system user access and recertification forms to (a) ensure the accuracy of the SEC office names, and (b) require an accompanying list of user names for each system reviewed.

Management's Response. The Office of Information Technology concurs with the recommendation. The forms used for system access and recertification will be updated to include an SEC office name where applicable. In addition, the form will include a list of users on the system being reviewed.

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

Other Matters of Interest

(b)(7)(E) Assessment May Not be Comprehensive or Adequately Address System and Subsystem Risks

We reviewed the (b)(7)(E) system as it relates to the FISMA reporting requirements.

(b)(7)(E)

(b)(7)(E)

Source: NIT Generated.

(b)(7)(E)

OIT Did Not Adhere to Established Milestone Remediation Dates for Some POA&M Items

As part of our evaluation of the OMB/DHS FY 2014 IG FISMA Reporting Metrics, we were tasked to evaluate whether OIT "establishes and adheres to milestone remediation dates" for POA&M items.[47] According to OIT, they have closed approximately 280 POA&M items in the past year.

While evaluating this metric, we determined that OIT tracks POA&M items for the SEC's systems and closed the OIG's prior recommendation concerning remediating POA&M items for systems sampled during that audit.[48] However, OIT did not close any POA&M items for (b)(7)(E) did not take action to address some POA&M items for the (b)(7)(E) within the established timeframes. For these systems, some POA&M items remained open beyond their established remediation dates. In some cases, these items have been open for 2 to 6 years beyond established remediation dates. These include POA&M items of both moderate and low risk.

Although OIT did not always adhere to POA&M remediation dates for the (b)(7)(E) (b)(7)(E) OIT staff meet weekly to review POA&M items and update the status or progress on outstanding POA&M items. OIT also told us that it uses a risk based approach when determining which POA&M items to remediate.

[47] *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics,* p. 16, Metric 7.1.4.

[48] OIG Report Number 512, *2012 FISMA Executive Summary Report*, March 29, 2013.

Appendix I. Scope and Methodology

Scope. The OIG contracted with NIT to evaluate the SEC's information security policies, practices, and procedures. The evaluation included a review of the SEC's IT security program and an assessment of how the SEC met the FY 2014 FISMA reporting requirements. In addition, the evaluation provided recommended responses for the OIG's FY 2014 Cyberscope submission to OMB and DHS.

NIT conducted the evaluation from July 2014 to January 2015. The scope of the evaluation consisted of the following 11 areas specified in DHS's FY 2014 FISMA reporting instructions:

1. configuration management;
2. contingency planning;
3. continuous monitoring management;
4. contractor systems;
5. identity and access management;
6. incident response and reporting;
7. POA&M;
8. remote access management;
9. risk management;
10. security capital planning; and
11. security training.

Appendix II lists the Federal laws and guidance and SEC regulations, policies, and procedures for information security that we reviewed.

Methodology. To assess the SEC's systems and provide the OIG with input for its Cyberscope submission, we interviewed key personnel, including personnel from OIT's Policy and Compliance Branch and Security Operations Branch, as well as from the agency's Office of Support Operations. We also examined documents and records applicable to the SEC's information security processes, including security assessment packages, related memos, security change requests, and third-party vendor contracts.

We conducted a limited-scope review of the SEC's information security posture. Specifically, to assess system security controls, we reviewed the security assessment packages for a non-statistical, judgmentally selected (b)(7)(E)

(b)(7)(E) The sample consisted of the internally- and externally-hosted systems shown in Table 2.[49]

Table 2: Sample of SEC Systems Evaluated

No.	System Name	System Description
1	(b)(7)(E)	
2		
3		
4		
5		
6		
7		
8		

Source: NIT Generated.

[49] We selected the information systems based on the SEC's compliance workbook (inventory of information systems), dated July 3, 2014.

Management Controls. Consistent with the objectives of this evaluation, we did not assess OIT's management control structure. We reviewed the SEC's controls specific to the 2014 FISMA OIG questionnaire. To understand thoroughly 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 various OIT personnel.

Prior Coverage. NIT reviewed the OIG's 2013 FISMA report, which included nine recommendations for corrective action, respectively. As of the date of this report, OIT had implemented three of those nine recommendations. We also reviewed the OIG's 2011 and 2012 FISMA reports. While OIT is working to address the outstanding recommendations, as we noted in this report, weaknesses still exist. Unrestricted SEC OIG reports can be accessed at www.sec.gov/about/offices/inspector_general.shtml.

- *Federal Information Security Management Act: Fiscal Year 2013 Evaluation*, Report No. 522, March 31, 2014.
- *2012 FISMA Executive Summary Report*, Report No. 512, March 29, 2013.
- *2011 Annual FISMA Executive Summary Report*, Report No. 501, February 2, 2012.

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

We reviewed the following during the course of our fieldwork:

Federal Laws and Guidance:

- Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011.
- E-Government Act of 2002, Pub. L. No. 107-347; 44 U.S.C. § 101.
- Standards of Ethical Conduct for the Employees of the Executive Branch, February 24, 2014, 5 C.F.R. § 2635.703 (b) (2).
- Federal Information Security Management Act of 2002, Title III, Pub. L. No. 107-347.
- OMB Circular A-130, Revised, Transmittal Memorandum No. 4, *Management of Federal Information Resources*, November 28, 2000.
- OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones,* October 17, 2001.
- OMB Memorandum, M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 6, 2003,
- OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003.
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007.
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractors*, February 3, 2011.
- OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*, November 18, 2013.
- OMB Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* November 18, 2013.

- Homeland Security Presidential Directive 12 (HSPD-12), *Policies for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

- U.S. Department of Homeland Security, Office of Cyber Security and Communications, Federal Network Resilience, *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*.

- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.

- NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

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

- NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, December 2014.

- NIST SP 800-63-2, *Electronic Authentication Guide*, August 2013.

- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011.

- NIST SP 800-145, *The NIST Definition of Cloud Computing*, September 2011.

- NIST SP 800-157, DRAFT *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, March 2014.

- Draft NIST Interagency Report 7981, *Mobile, PIV, and Authentication*, March 2014.

- Federal Information Processing Standard Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

- Federal Information Processing Standard Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

- Federal Information Processing Standard Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013.

- FedRAMP Security Controls Preface and Baseline Workbook, Revision 4, 2014.

SEC Regulations, Policies, and Procedures:

- SEC OIT CIO Policy Directive CIO PD-08-06, *SEC Information Security Program,* version *2*, March 18, 2014 and accompanying manual, *Information Security Controls Manual*, version 2, April 4, 2014.

- SEC Administrative Regulation SECR 301-01, *Operational Risk Management (ORM) and Internal Control Program (Draft)*, August 2014.

- SEC Branch Owned Document, Customer Service Branch, *LAN and Telephone Request,* October 18, 2013.

- SEC Operating Procedures OP 24-05.04.03.03 (01.0), *Security-Related Patch Management for Red Hat Linux-Based Servers, Security-Related Patch Management for Solaris-Based Servers, Security-Related Patch Management for Windows and Mac-Based Workstations, and Security-Related Patch Management for Windows-Based Servers,* June 10, 2014.

- SEC Implementing Instruction II 24-04.07.01 (A01), *SEC Incident Response Capability Handbook*, April 2014.

We also reviewed the 41 SEC IT security control procedures shown in Appendix III.

Appendix III. Outdated IT Security Control Procedures

The 41 security control procedures shown in Table 3 below were outdated as of October 2014.[50] According to SEC policy, OIT should have updated these procedures between 5 and 9 years ago.

Table 3: OIT Procedures, Date of Last Update, and Status

FISMA Control	Procedure	Procedure Number	Date Last Updated	Defined Frequency	Where Frequency Specified	No. of Years Outdated	Status: May – Aug. 2014[51]
(b)(7)(E)	(b)(7)(E)		Mar. 13, 2007	Annual	Specified in procedure	6 years	Revise
			Jan. 03, 2006	Annual	Specified in procedure	7 years	Retire, content moved
			Dec. 30, 2005	Annual	Specified in procedure	8 years	Retire, content moved
			Apr. 24, 2006	Annual	Specified in procedure	7years	Retire, content moved
			Apr. 17, 2006	Annual	Specified in procedure	7 years	Retire, content moved
			Jan. 11, 2006	Annual	Specified in procedure	7 years	Retire, content moved
			Dec. 30, 2005	Annual	Specified in procedure	8 years	Retire, content moved
			Apr. 17, 2006	Annual	Specified in procedure	7 years	Retire, content moved
			Apr. 17, 2006	Annual	Specified in procedure	7 years	Revise
			Apr. 17, 2006	Annual	Specified in procedure	7 years	Retire, content moved
			Dec. 30, 2005	Annual	Specified in procedure	8 years	Retire, content moved
			Dec.29, 2005	Annual	Specified in procedure	8 years	Revise

[50] NIT last accessed OIT's security procedures site on October 6, 2014.

[51] This status is based on the policy status roadmap provided by OIT and dated September 2, 2014.

FISMA Control	Procedure	Procedure Number	Date Last Updated	Defined Frequency	Where Frequency Specified	No. of Years Outdated	Status: May – Aug. 2014
(b)(7)(E)	(b)(7)(E)		Jan. 11, 2006.	3 years	IT Security Policy[52]	5 years	Retire, content moved
			Jan. 11, 2006	3 years	IT Security Policy	5 years	Retire, content moved
			Dec. 30, 2005	3 years	IT Security Policy	6 years	Revise
			Dec. 30, 2005	3 years	IT Security Policy	6 years	Retire, other
			Dec. 30, 2005	3 years	IT Security Policy	6 years	Retire, other
			Jan. 03, 2006	3 years	IT Security Policy	5 years	Revise
			Jan. 03, 2006	3 years	IT Security Policy	5 years	Revise
			Dec. 30, 2005	3 years	IT Security Policy	6 years	Revise
			Apr. 17, 2006	3 years	IT Security Policy	5 years	Revise
			Jan. 11, 2006	3 years	IT Security Policy	5 years	Retire, content moved
			Jan. 11, 2006	3 years	IT Security Policy	5 years	Retire, content moved
			Jan. 11, 2006	3 years	IT Security Policy	5 years	Retire, content moved
			Jan. 11, 2006	3 years	IT Security Policy	5 years	Retire, content moved
			Dec. 30, 2005	3 years	IT Security Policy	6 years	Revise
			Dec. 30, 2005	3 years	IT Security Policy	6 years	Revise

[52] IT Security Policy refers to Section 3.1.1, "Revision Schedule," of SECR 24-04, overarching IT security policy manual, version 2.0.

FISMA Control	Procedure	Procedure Number	Date Last Updated	Defined Frequency	Where Frequency Specified	No. of Years Outdated	Status: May – Aug. 2014
	(b)(7)(E)		Dec. 30, 2005	3 years	IT Security Policy	6 years	Revise
			Apr. 17, 2006	3 years	IT Security Policy	5 years	Revise
(b)(7)(E)			Mar. 17, 2006	Annual	Specified in procedure	7 years	Retire, content moved
			Mar. 17, 2006	3 years	IT Security Policy	5 years	Revise
			April 18, 2006	Annual	Specified in procedure	7 years	Retire, other
			April 18, 2006	Annual	Specified in procedure	7 years	Revise
			July 3, 2006	Annual	Specified in procedure	7 years	Retire, content moved
(b)(7)(E)			Aug. 09, 2007	Annual	Specified in procedure	6 years	Revise
			April 30, 2006	Annual	Specified in procedure	7 years	Retire, content moved
			Dec. 29, 2005	Annual	Specified in procedure	8 years	Revise
			June 29, 2005	Annual	Specified in procedure	8 years	Retire, content moved
			Aug. 20, 2002	3 years	IT Security Policy	9 years	Not listed
			Dec. 30, 2005	Annual	Specified in procedure	8 years	Revise
			Dec.12, 2005	Annual	Specified in procedure	8 years	Retire, content moved

Source: NIT Generated.

[53] This procedure was no longer in the OIT Library as of October 6, 2014.

[54] This procedure was no longer in the OIT Library as of October 6, 2014.

Appendix IV. Management Comments

MEMORANDUM

January 23, 2015

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

From: Jeffery Heslop, Chief Operating Officer JH

Subject: Management Response, *2014 FISMA Executive Summary*, Report No. 529

Thank you for the opportunity to comment on the recommendations in Report No. 529, *Draft: Federal Information Security Management Act: Fiscal Year 2014 Evaluation.* I appreciate the Office of Inspector General's insights and am providing the official response to the recommendations contained in the report.

Recommendation 1: "The Office of Information Technology should take all required steps, including performing security assessments, to determine whether systems in operation without a current authorization to operate – including (b)(7)(E) (b)(7)(E) – should be re-authorized, and then either authorize or deactivate the systems as appropriate."

Management Response: OIT concurs with the recommendation. OIT will review the entire catalog of FISMA-reportable systems to identify any operating without a current, valid ATO. Those systems will be assessed and then authorized with a new ATO or deactivated as appropriate.

Recommendation 2: "The Office of Information Technology should develop and implement internal controls to ensure that (a) authorizations to operate do not expire, and (b) appropriate rationale is documented for issuing authorization to operate extensions."

Management Response: OIT concurs with the recommendation. To help ensure future authorizations do not expire, OIT is implementing an automated system for notification when ATOs approach their expiration date. For ATO extensions, a section will be included in the body of the ATO itself detailing the rationale for issuing an extension.

Recommendation 3: "The Office of Information Technology should assess the privacy impact assessment control for all systems assessed after April 2014, and include the assessment in the related system security documents."

Management Response: OIT does not concur with the recommendation. As part of NIST 800-53 rev 4, control PL-5 *Privacy Impact Assessment* was withdrawn as a security control. It exists as a privacy control in Appendix J as control AR-2.

Control CA-2 *Security Assessments* covers the SA&A process. The supplemental guidance for CA-2 states:

> "Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans."

Privacy controls are covered under Appendix J which speaks to assessment of these controls as a separate activity from the SA&A process:

> "Organizational assessments of privacy controls can be conducted either by the SAOP/CPO alone or jointly with the other organizational risk management offices including the information security office."

Control AR-2 provides supplemental guidance calling out when PIAs are performed and updated, which is unlike the periodic assessments of the SA&A process:

> "PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks."

Finally, as for including PIAs in the System Security Plan (SSP) package, Appendix J gives leeway to the organization as to where they are maintained, stating:

> "At the discretion of the implementing organization, privacy controls may be documented in a distinct privacy plan or incorporated into other risk management documents (e.g., system security plans)."

It is the opinion of management that OIT is conducting privacy impact assessments fully in accordance with the latest NIST guidance.

OIG Note: After assessing management's response and reviewing information provided by the Office of Information Technology, we deleted draft Recommendation 3 from the final report.

Recommendation 4: "The Office of Support Operations should coordinate with the Office of Information Technology to develop and implement the required insider threat training component of the agency's security awareness training program."

Management Response: OSO concurs with the recommendation and will work with OIT on implementation of insider threat training.

Recommendation 5: "The Office of Information Technology should develop and implement a policy requiring, to the maximum extent practicable, the use of the personal identity verification card for logical access."

2

Management Response: OIT concurs with the recommendation and will develop a policy and supporting procedures establishing the proper use of PIV authentication for logical access, to the maximum extent practical considering some of the technical challenges of our increasingly mobile workforce. The ability to leverage PIV cards for logical access to SEC's network will be made available to all users.

Recommendation 6: "The Office of Information Technology should review and update open Memorandums of Understanding, Interconnection Agreements, and/or contracts for externally-hosted systems, including (b)(7)(E) to ensure the method of remote access is defined and documented."

Management Response: OIT concurs and will review the entire catalog of FISMA-reportable, externally-hosted systems to review and update MOUs, IAs and contracts and ensure the method of remote access is defined and documented.

Recommendation 7: "The Office of Information Technology should coordinate with the business and information system owners to ensure (b)(7)(E) (b)(7)(E) accurately identifies the office names assigned to each active user."

Management Response: OIT concurs with the recommendation and will work with the business and information system owners to validate the office names assigned to active (b)(7)(E) are accurate.

Recommendation 8: "The Office of Information Technology should develop a process to annually review all system user access and recertification forms to (a) ensure the accuracy of the SEC office names, and (b) require an accompanying list of user names for each system reviewed."

Management Response: OIT concurs with the recommendation. The forms used for system user access and recertification will be updated to include an SEC office name where applicable for those systems that contain that information, in addition to the list of users on the system being reviewed.

Other Matter of Interest 1 (b)(7)(E) Assessment May Not be Comprehensive or Adequately Address System and Subsystem Risks"

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

(b)(7)(E)

Other Matters of Interest 2: "OIT Did Not Adhere to Established Milestone Remediation Dates for some POA&M Items"

Management Response: OIT takes the issue of outstanding POA&Ms seriously. Quoting OMB Memorandum M14-04:

Q45. Can a POA&M process be effective even when correcting identified weaknesses is untimely?

> "Yes. The purpose of a POA&M is to identify and track remediation plans for security weaknesses. A POA&M permits agency officials and oversight authorities to identify when documented corrective actions are both timely and untimely. In either circumstance, the POA&M has served its intended purpose. Agency managers can use the POA&M process to focus resources to resolve delays."

The report calls out that "Currently OIT meets weekly to review POA&Ms and update the status or progress on outstanding POA&Ms. Summaries of POA&M status are reported to OIT's senior management in the monthly IT Risk Management meetings. Details of any POA&M are available during that meeting and individual issues are frequently discussed. OIT management uses a risk approach when determining which POA&Ms to remediate.

To further address the issue of aging POA&Ms, OIT Security is implementing an advanced Weakness Management process and is coordinating with both POA&M resolution teams and OIT management to better identify process issues as well as providing accountability.

In addition to the recommendations listed above, some prior-year recommendations were still outstanding and carried over from OIG's 2011 *FISMA Executive Summary Report*, Report No. 501, issued in February 2012 and from the OIG's 2012 *FISMA Executive Summary Report*, Report No. 512, issued on March 29, 2013.

OIT is actively working on all existing, open recommendations and is fully committed to resolving them as expeditiously and effectively as possible.

4

Appendix V. OIG's Response to Management Comments

After assessing management's response to a draft of this report and reviewing information provided by the Office of Information Technology, we deleted draft Recommendation 3 from the final report. We are pleased that SEC management concurred with the seven remaining recommendations for corrective action. Management's proposed actions are responsive to the recommendations; therefore, the recommendations are resolved and will be closed upon completion and verification of the appropriate corrective action. Full implementation of our recommendations should assist the agency in its efforts to strengthen the SEC's information security posture.

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

Web: www.reportlineweb.com/sec_oig

Email: oig@sec.gov

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 20549-2736

Comments and Suggestions

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