U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Federal Information Security Management Act: Fiscal Year 2013 Evaluation

March 31, 2014
Report No. 522

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

March 31, 2014

To: Thomas Bayer, Director, Office of Information Technology
(b)(7)(E) [redacted]

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

Subject: *Federal information Security Management Act: Fiscal Year 2013*, Report No. 522

Attached please find the Office of Inspector General's (OIG) final report detailing the results of the fiscal year 2013 evaluation of the U.S. Securities and Exchange Commission's (SEC's) information security programs and practices. Networking Insitute of Technology, Inc., under a contract issued by the OIG, performed the evaluation. The attached report contains nine recommendations for corrective action that, if fully implemented, should strengthen the SEC's information security posture.

On March 18, 2014, we provided you with a draft of the report for your review and comment. In response, management concurred with eight of the nine recommendations and noncourred with one recommendation. We have included your responses as Appendix V 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 audit. If you have questions, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects.

Attachment

cc: Mary Jo White, Chair
Erica Y. Williams, Deputy Chief of Staff, Office of the Chair
Luis A. Aguilar, Commissioner
Daniel M. Gallagher, Commissioner
Kara M. Stein, Commissioner
Michael S. Piwowar, Commissioner

Jeffery Heslop, Chief Operating Officer
Anne K. Small, General Counsel
Timothy Henseler, Director, Office of Legislative and Intergovernmental Affairs
John J. Nester, Director, Public Affairs
Pamela Dyson, Deputy Director, Office of Information Technology
Todd Scharf, Associate Director, Chief Information Security Officer
(b)(7)(E)
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

Executive Summary

Federal Information Security Management Act:
Fiscal Year 2013 Evaluation
Report No. 522
March 31, 2014

Why We Did This Evaluation

The Federal Information Security Management Act (FISMA) provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets. The Act also requires agency Inspectors General to annually assess the effectiveness of agency information security programs and practices and report the results to the Office of Management and Budget (OMB). The overall objective of the fiscal year 2013 FISMA evaluation was to assess the U.S. Securities and Exchange Commission's (SEC) systems and information security posture. The Office of Inspector General contracted the services of Networking Institute of Technology, Inc. (referred to as "we" in this report) to conduct the evaluation.

What We Recommended

To strengthen the SEC's controls over information security, the OIT should address all outstanding recommendations from prior FISMA evaluations. In addition, we made nine new recommendations for corrective action. The recommendations address procedures for conducting security assessments; requiring multi-factor authentication for remotely accessing externally-hosted systems; reviewing user accounts; and (b)(7)(E) (b)(7)(E) We also recommended training the alternate business owner for the (b)(7)(E) (b)(7)(E)

Management concurred with eight of the nine recommendations, one of which will be closed upon issuance of this report. While management noncurred with one recommendation, they took responsive actions and all open recommendations will be closed upon completion and verification of corrective action.

What We Found

To assess the SEC's system security controls and information security posture, we reviewed the security assessment packages for 7 of the SEC's 59 major information systems. Our review found several areas in which the SEC has implemented improved controls over its information security. For example, the Office of Information Technology (OIT) has made significant progress establishing (1) a risk management program; (2) an incident response and reporting program; and (3) an enterprise-wide business continuity and disaster recovery program, consistent with FISMA requirements, and OMB and National Institute of Standards and Technology guidelines. The OIT has also established a plan of action and milestones program and properly tailors its baseline control list in compliance with Federal guidance. Finally, the SEC provided, to its personnel, security awareness and role-based security training and has established an information security capital planning and investment program.

However, we found that the OIT had not taken corrective action on some issues identified during the fiscal year 2011 and 2012 FISMA evaluations. For example, while the OIT has updated many of its policies, 43 of the organization's security procedures remain out of date. In addition, until February 28, 2014, the OIT had not established a continuous monitoring strategy or plan. Finally, the agency has not implemented Homeland Security Presidential Directive 12 personal identity verification cards for logical access to information systems.

We also determined that the OIT does not:

- obtain (b)(7)(E) (b)(7)(E) have been effectively implemented;
- require multi-factor authentication for privileged users remotely accessing one of the seven SEC systems included in our review;
- review (b)(7)(E) annually; or
- update the agency's (b)(7)(E)

Finally, we found that the system owner for one of the systems we reviewed did not properly identify account types, while the alternate business owner for another system needed training on their roles and responsibilities.

The weaknesses we observed in the SEC's security controls could adversely affect the confidentiality, integrity, and availability of the agency's information and information systems. Therefore, management's attention is required.

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

TABLE OF CONTENTS

Tables

Appendices

ACRONYMS

CIO	Chief Information Officer
COO	Chief Operating Officer
(b)(7)(E) [redacted]	[redacted]
FISMA	Federal Information Security Management Act
FY	fiscal year
HSPD-12	Homeland Security Presidential Directive 12
International POD	International Program Oversight Database
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	information technology
NIST	National Institute of Standards and Technology
NIT	Networking Institute of Technology, Inc.
(b)(7)(E) [redacted]	[redacted]
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
ORM	Operational Risk Management
PIV	personal identity verification
POA&M	plan of action and milestones
SA&A	security assessment and authorization
SEC	U.S. Securities and Exchange Commission
SP	Special Publication
SSP	system security plan
VoIP	Voice over Internet Protocol
WLANs	Wireless Local Area Networks
XBRL EUT	Extensible Business Reporting Language End User Tool

Background and Objectives

Background

The Federal Information Security Management Act (FISMA) provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets.[1] The Act also requires agency program officials, Chief Information Officers (CIO), and Inspectors General to conduct annual reviews of the agency's information security programs and report the results to the Office of Management and Budget (OMB).[2] The U.S. Department of Homeland Security's *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*[3] provides instructions to heads of executive departments and agencies for meeting the fiscal year (FY) 2013 reporting requirements.

In addition, the National Institute of Standards and Technology (NIST) – a non-regulatory Federal agency within the U.S. Department of Commerce – leads the nation in utilizing existing and emerging information technology (IT). NIST has been charged under FISMA to develop cyber security standards, guidelines, and associated methods and techniques.[4]

The U.S. Securities and Exchange Commission (SEC) Office of Information Technology (OIT) supports the agency and its staff in all areas of IT. The office has overall management responsibility for the SEC's IT program including:

- application development;
- infrastructure operations and engineering;
- user support;
- IT program management;
- capital planning;
- security;

[1] 44 U.S.C. § 3451.

[2] 44 U.S.C. § 3545(a),(b).

[3] U.S. Department of Homeland Security, Office of Cyber Security and Communications, Federal Network Resilience, *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics* (August 2013).

[4] NIST Special Publication (SP) 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (February 2010), p. ii.

- enterprise architecture; and
- implementation of FISMA requirements.

The OIT's CIO is responsible for developing and maintaining an SEC-wide information security program. The Chief Information Security Officer is responsible for establishing and maintaining the SEC's security posture.

To conduct the FY 2013 FISMA evaluation, the SEC Office of Inspector General (OIG) contracted the services of Networking Institute of Technology, Inc. (NIT) (referred to as "we" in this report).

Objectives

The overall objective of the evaluation was to assess the SEC's systems and provide the OIG with input for the SEC's response to the *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*. As required by FISMA, the evaluation included a review of the SEC's information security posture based on guidance issued by the OMB, the Department of Homeland Security, and NIST. To assess the SEC's system security controls and information security posture, we reviewed the security assessment packages for a judgmentally selected sample of 7 of the SEC's 59 major information systems.[5]

Appendixes I and II include additional information on our scope and methodology and applicable Federal laws, regulations, policies, and guidance.

[5] Section 305(C)(2)(c) of FISMA states that the head of each agency shall develop and maintain an inventory of major information systems. OMB Memorandum A-130 (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."

Results

Finding 1: OIT Has Not Updated All IT Security Procedures

As previously reported by the SEC OIG, the OIT has not updated all of its IT security procedures in accordance with NIST guidelines and its own policy. Specifically, as shown in Appendix III, we identified 43 out-of-date security procedures and determined, based on OIT policy, that 95 percent of those procedures should have been updated between 4 and 7 years ago. The OIG previously reported this issue in the FY 2011 and FY 2012 FISMA evaluations, and management agreed to take corrective action. However, the OIT has not yet updated all of its security procedures.

- NIST recommends that organizations review/update their formal documented security controls procedures in accordance with the organization-defined frequency.[6] According to SEC policy, the OIT is required to update its procedures at least every 3 years and whenever there is a significant change to the system, or annually as stated in each individual procedure.[7]

- We reviewed the OIT's security procedures and determined that the organization has not updated 95 percent (or 43 out of 45) of its procedures, as required by their defined frequency. The procedures in question address FISMA controls for configuration management, incident response and reporting, security training, plan of action and milestones (POA&M), and remote access management. According to SEC policy, over half of the outdated procedures (23 of 43) should have been updated annually, while the remaining procedures (20 of 43) should have been updated every 3 years. We determined that the OIT should have updated 95 percent of the 43 procedures between 4 and 7 years ago. One procedure – (b)(7)(E) – should have been updated 8 years ago.

  Although the OIT has not updated all of its procedures, the organization has developed draft procedures for risk management and updated its identity and access management procedures. In addition, the OIT planned to review and update the remaining security procedures by March 17, 2014. While the OIT indicated that all of the procedures would be updated by March 17, 2014, to date the organization has updated only 2 of the procedures (not yet formally approved by OIT management); 3 have been scheduled for retirement, and 38 remain

[6] NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* (August 2009), p. F-38, Configuration Management; p. F-61, Incident Response; p. F-21, Awareness and Training; p. F-32, Security Assessment and Authorization; and p. F-3, Access Control.

[7] SEC Operating Directive, *IT Security Compliance Program*, OD 24-04.10 (June 9, 2011), p. 7, Section 5, #12.

outstanding. The OIT plans to consolidate 32 of the procedures into a Master Baseline Configuration Handbook.

- This finding is consistent with (1) Finding 1, "OIT's FISMA Policies and Procedures Are Outdated or Nonexistent" from the OIG's *2011 FISMA Executive Summary Report, Report No. 501*, issued on February 2, 2012;[8] and (2) Finding 9, "OIT Did Not Update Its Procedures," from the OIG's *2012 FISMA Executive Summary Report, Report No. 512*, issued on March 29, 2013.[9] In response to Report No. 501, the OIT agreed to update its security procedures; however, management has not taken appropriate corrective action. OIT staff informed us that they have not been able to take corrective action because of limited resources. Specifically, (b)(7)(E) (b)(7)(E) In addition, OIT staff stated that updating procedures is time consuming since it requires many branches of the organization to review, provide feedback, and approve each procedure.

Without current procedures, OIT staff may not receive adequate guidance to implement security controls, thus increasing the level of risk to SEC systems.

Because this finding appeared in two previous OIG reports and the related recommendation is still outstanding, we are not making a new recommendation for corrective action. Instead, the OIT should take immediate action to address the outstanding recommendation made in OIG Report No. 501 and reiterated in OIG Report No. 512.

Management's Response. The Chief Operating Officer (COO) and CIO acknowledged that some prior-year recommendations were still outstanding and carried over from the FYs 2011 and 2012 reports. The COO and CIO further stated that OIT is actively working on all existing, open recommendations and is fully committed to resolving them as expeditiously as possible. Management's complete response is reprinted in Appendix V.

OIG Evaluation of Management's Response. We are pleased that management continues to focus on the outstanding recommendations. We will continue to monitor OIT's corrective action plans to determine whether OIT's actions are responsive to the recommendations.

[8] OIG *2011 FISMA Executive Summary Report, Report No. 501*, (February 2, 2012). The report can be accessed over the Internet at http://www.sec-oig.gov/Reports/AuditsInspections/2012/501.pdf.

[9] OIG *2012 FISMA Executive Summary Report, Report No. 512*, (March 29, 2013). The report can be accessed over the Internet at http://www.sec.gov/about/offices/oig/reports/audits/2013/512.pdf.

Finding 2: OIT Developed a Continuous Monitoring Strategy That Includes Ongoing Assessments of Security Controls

On November 26, 2013, the SEC OIG reported to OMB, through the Cyberscope reporting tool, that the OIT did not have a continuous monitoring strategy or formal continuous monitoring plan. Therefore, the agency was not in compliance with NIST guidelines or its own policy. In addition, based on our review of a judgmental sample of 7 of the SEC's 59 major information systems, we found that the OIT did not conduct ongoing assessments of security controls. The OIG previously reported this issue in the FY 2012 FISMA evaluation and OIT management agreed to take corrective action. Subsequent to November 26, 2013, the OIT developed a continuous monitoring strategy, which includes a process to evaluate a subset of security controls on an ongoing, annual basis.

- NIST provides direction for developing a continuous monitoring strategy that includes configuration management, security impact analyses, assessment of selected security controls, security status reporting, and active involvement of authorizing officials.[10] Consistent with NIST, OIT policy (CIO-PD-08-06) also requires a continuous monitoring strategy.[11] In response to the OIG's *2012 FISMA Executive Summary Report, Report No. 512,* issued on March 29, 2013, OIT concurred with the recommendation to develop and implement a continuous monitoring strategy and stated that it was in the early stages of developing a continuous monitoring program. We found that, at the time of the OIG's Cyberscope submission (November 26, 2013), the OIT had not developed a continuous monitoring strategy. The OIT subsequently developed a strategy (dated February 28, 2014) and submitted it to us on March 4, 2014.

- NIST recommends that organizations, during their initial security authorization, assess all security controls employed within the information system and reassess them every 3 years during the reauthorization process. NIST also recommends that, subsequent to the initial security authorization, the organization should assess a subset of security controls on an ongoing basis through continuous monitoring.[12] We found for each of the seven judgmentally sampled systems reviewed that (1) the OIT evaluated the systems' security controls only once during the 3-year security authorization cycle; and (2) the OIT did not evaluate a subset of controls, as recommended, during the years between authorization assessments. However, the OIT's newly developed continuous monitoring strategy includes a process to evaluate a subset of controls on an ongoing, annual basis.

[10] NIST SP 800-37, Rev. 1, p. G-2, Appendix G.

[11] SEC OIT CIO Policy Directive, *SEC OIT Security Policy Framework*, CIO-PD-08-06 (August 7, 2012), p. 57, Section 10-B-04.

[12] NIST SP 800-37, Rev. 1, p. 39, Supplemental Guidance.

The OIT took corrective action to address Recommendations 1 and 2 made in OIG Report No. 512. Furthermore, the OIT's newly developed continuous monitoring strategy and ongoing assessments of security controls will be assessed as part of the OIG's FY 2014 FISMA evaluation. Therefore, we are not making a recommendation for corrective action at this time.

Management's Response. The COO and CIO acknowledged that some prior-year recommendations were still outstanding and carried over from the FYs 2011 and 2012 reports. The COO and CIO further stated that OIT is actively working on all existing, open recommendations and is fully committed to resolving them as expeditiously as possible. Management's complete response is reprinted in Appendix V.

OIG Evaluation of Management's Response. We are pleased that management continues to focus on the outstanding recommendations. We will continue to monitor OIT's corrective action plans to determine whether OIT's actions are responsive to the recommendations.

Finding 3: OIT Has Not Implemented PIV Cards for Logical Access

As previously reported by the SEC OIG, the SEC does not require personal identity verification (PIV) cards to access its information systems as required by Homeland Security Presidential Directive 12 (HSPD-12) and 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*. The OIG reported this issue in the FY 2011 and FY 2012 FISMA evaluations. While management agreed to take corrective action, the OIT has not taken sufficient steps to ensure that the SEC complies with Governmentwide requirements for use of PIV cards to access agency systems.

- HSPD-12 is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal PIV smartcard credentials, including a standardized background investigation to verify employees' and contractors' identities. HSPD-12 requires that, to the maximum extent practicable, executive departments and agencies shall require the use of the Governmentwide PIV card to gain logical access to Federally controlled information systems.[13]

- OMB Memorandum M-11-11 (dated February 3, 2011) reaffirms HSPD-12, stating, "each agency should 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." The memorandum provides guidance from the Department of Homeland Security, which requires that:

  - effective immediately, all new systems under development must be enabled to use PIV credentials, in accordance with NIST guidelines, prior to being made operational; and

  - effective the beginning of FY 2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with NIST guidelines, prior to the agency using development and technology refresh funds to complete other activities.[14]

[13] Homeland Security Presidential Directive 12 (HSPD-12), *Policies for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004, paragraph 4.

[14] 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. 3-4.

- We found that SEC employees and contractors are not required to use a PIV card to gain logical access to information systems. OIT staff indicated that the project for implementing PIV cards was put on hold so that staff could be reallocated to a higher-priority project.

- In August 2013, the OIT assigned additional resources to PIV card implementation and approved a detailed project plan. The project plan includes a pilot program that is scheduled to be deployed in April 2014 and that is estimated to be completed by August 2014. The OIT projects that full implementation of the PIV cards for logical access to SEC systems will take at least an additional 6 to 9 months after completion of the pilot program.

- This finding is consistent with (1) Finding 5, "Multi-Factor Authentication for System Access Has Not Been Linked to the PIV Card," which is in the OIG's *2011 FISMA Executive Summary Report, Report No. 501*, issued February 2, 2012; and (2) Finding 3, "OIT Has Not Implemented Multi-Factor Authentication to the SEC's Personal Identity Verification Program," which is in the OIG's *2012 FISMA Executive Summary Report, Report No. 512*, issued March 29, 2013. In response to Report No. 501, the OIT agreed to work through technical challenges and provide the SEC's user community with logical access via PIV card authentication; however, management has not taken appropriate corrective action.

Without PIV cards as a second factor authentication for users to gain logical access to SEC information systems, the SEC is at a higher risk for unauthorized access to its systems.

Because this finding appeared in previous OIG reports and the recommendation associated with it is still outstanding, we are not making a new recommendation. Instead, the OIT should take immediate action to address the outstanding recommendation made in OIG Report No. 501 and reiterated in OIG Report No. 512.

Management's Response. The COO and CIO acknowledged that some prior-year recommendations were still outstanding and carried over from the FYs 2011 and 2012 reports. The COO and CIO further stated that OIT is actively working on all existing, open recommendations and is fully committed to resolving them as expeditiously as possible. Management's complete response is reprinted in Appendix V.

OIG Evaluation of Management's Response. We are pleased that management continues to focus on the outstanding recommendations. We will continue to monitor OIT's corrective action plans to determine whether OIT's actions are responsive to the recommendations.

Finding 4: OIT Has Not Fully Evaluated Security Controls for the SEC's (b)(7)(E) System

The OIT uses a vendor-provided, externally-hosted[15] system called (b)(7)(E) as a project and portfolio management tool for tracking development, modernization, and enhancement projects. However, the organization did not comply with NIST guidelines for assessing some of the security controls for the system. Further, the OIT does not have documented procedures for evaluating externally-hosted or contractor systems.

- NIST recommends that organizations "[assess] the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to the security of the system." According to NIST, assessing many of these security controls for externally-hosted systems is the responsibility of the OIT, not a vendor.[16] In addition, according to OIT policy, the OIT is responsible for ensuring that all required security assessment documentation is developed.[17]

- We reviewed the (b)(7)(E) system's certification and accreditation package completed by the OIT in November 2011 and determined that the OIT did not evaluate several security controls as required by NIST. Such controls included access control, identification and authentication, configuration management, risk assessment, security planning, and security assessment and authorization. Because the OIT did not evaluate those security controls, the (b)(7)(E) security assessment package consisted only of a risk assessment summary report, authorization to operate memo, and recommended system security categorization report. The system security assessment package did not include required security assessment documentation, such as:

    1. a security test and evaluation report;[18]
    2. a system security plan (SSP);[19]

[15] An externally-hosted system is one that resides outside of the SEC network and is provided by a vendor external to the SEC.

[16] NIST SP 800-53, Rev. 3, p. F-32, CA-2; and pp. F-1 – F-32.

[17] CIO-PD-08-06, p. 40, Section 7-D, Audit and Control.

[18] NIST SP 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations* (June 2010) defines "security test and evaluation report" as "[t]he security document that contains the assessment criteria and the assessment results for the required security controls for each system."

[19] NIST SP 800-53A, Rev. 1, defines "SSP" as a "[f]ormal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements."

3. a risk assessment;[20] and
4. a POA&M.[21]

- NIST also recommends that an organization have formal, documented procedures to facilitate the implementation of the associated security assessment and authorization controls.[22] However, we determined that the OIT does not have formal, documented procedures that identify the specific process for conducting security assessments for externally-hosted and contractor systems (b)(7)(E)

Because the OIT did not evaluate the security controls for the externally-hosted (b)(7)(E) system, the organization did not have the required security assessment documentation and has not properly determined the vulnerabilities and the levels of risk associated with the system. In addition, the lack of written procedures for conducting security assessments for externally-hosted and contractor systems may increase the likelihood of security controls not being consistently implemented across the agency. This could increase the risk to the confidentiality, integrity, and availability of the SEC's externally-hosted systems.

Recommendation 1:

The Office of Information Technology should (a) identify all of the security controls for the (b)(7)(E) system; (b) conduct a formal evaluation of those security controls; and (c) update the (b)(7)(E) security assessment package with the required documentation.

Management's Response. The COO and CIO concurred with the recommendation. Management's complete response is reprinted in Appendix V.

OIG Evaluation of Management's Response. We are pleased that management concurred with this recommendation. We will review the corrective action plan when submitted to OIG to determine whether OIT's plan is responsive to the recommendation.

[20] NIST SP 800-53, Rev. 3, defines "risk assessment" as "[t]he process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system."

[21] NIST SP 800-53A, Rev. 1, defines "POA&M" as "[a] document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones."

[22] NIST SP 800-53, Rev. 3, p. F-32, CA-1.

Recommendation 2:

The Office of Information Technology should develop and implement formal, written procedures for conducting security assessments for externally-hosted and contractor systems.

Management's Response. The COO and CIO concurred with the recommendation and indicated that they are in the final stages of revising their formal, written procedures for conducting securities assessment. Management's complete response is reprinted in Appendix V.

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

Finding 5: OIT Does Not Require Multi-Factor Authentication for Privileged User Accounts to Remotely Access the SEC's (b)(7)(E) System

The OIT does not require multi-factor authentication for privileged user accounts[23] to remotely access the (b)(7)(E) system, even though NIST guidelines and the OIT's own policy require it. In addition, the OIT did not properly evaluate the (b)(7)(E) system to determine whether adequate remote access controls requiring multi-factor authentication were present.

- According to NIST, remote access is "[a]ccess to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet)."[24] NIST SP 800-53, Rev. 3, 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)."[25] NIST further requires that "[t]he information system uses multifactor authentication for network access to privileged accounts."[26]

- In addition, CIO-PD-08-06 states, "SEC information systems use multi-factor authentication for network access to privileged accounts."[27] However, we found that multi-factor authentication is not required for remote access to the (b)(7)(E) system for privileged user accounts. Specifically (b)(7)(E) privileged user accounts are able to connect directly to the system via the Internet using only single-factor authentication, namely, a valid user ID and password.

We found that the OIT did not properly evaluate the remote access security controls for the (b)(7)(E) system to ensure that multi-factor authentication for privileged user accounts was required. As a result, privileged users are able to access the (b)(7)(E) system using single-factor authentication, which does not provide the required level of security and may increase the SEC's risk for unauthorized access to the (b)(7)(E) system.

[23] NIST SP 800-53, Rev. 3, Glossary, p. B-9, defines "privileged account" as an information system account with authorizations of a privileged user. A "privileged user" is defined as a user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

[24] NIST SP 800-53, Rev. 3, p. B-10, Glossary.

[25] NIST SP 800-53, Rev. 3, p. B-8, Glossary.

[26] NIST SP 800-53, Rev. 3, p. F-55, IA-2(1).

[27] CIO-PD-08-06, p. 60, Section 11-B-01, Identification and Authentication (Organizational Users).

Recommendation 3:

The Office of Information Technology should (a) require privileged (b)(7)(E) users to use multi-factor authentication for remote access to the (b)(7)(E) system via the Internet, and (b) ensure multi-factor authentication is required for remote access to all other externally-hosted systems using privileged user accounts.

Management's Response. The COO and CIO nonconcurred with the recommendation. Management indicated that multi-factor authentication is addressed in Finding 3 above. In addition, management indicated that (b)(7)(E) is (b)(7)(E) are covered. Also, management stated they have updated their security policies (b)(7)(E) Management's complete response is reprinted in Appendix V.

OIG Evaluation of Management's Response. Our recommendation for OIT to use multi-factor authentication for remote access to (b)(7)(E) via the internet and ensure multi-factor authentication for remote access to all other externally-hosted systems using a privileged accounts is intended to ensure that OIT's business practices are consistent with OIT's policy. While we agree that the requirement for two-factor authentication is governed by NIST 800-53, Rev. 3, we determined that OIT's policy required SEC information systems, including (b)(7)(E) and other externally-hosted systems, to use multi-factor authentication for network access to privileged accounts. Our test results found that privileged users were able to access (b)(7)(E) without the need for two-factor authentication. As stated in the COO and OIT's response to our draft report, management has updated OIT's policy (b)(7)(E) (b)(7)(E) Management's actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the actions taken.

Finding 6: (b)(7)(E) (b)(7)(E)

The OIT does not comply with NIST guidelines and its own policy (b)(7)(E) (b)(7)(E)

- NIST recommends that organizations (b)(7)(E) (b)(7)(E)

(b)(7)(E)

Recommendation 4:

The Office of Information Technology should (b)(7)(E) (b)(7)(E)

Management's Response. The COO and CIO concurred with the recommendation. Management's complete response is reprinted in Appendix V.

OIG Evaluation of Management's Response. We are pleased that management concurred with this recommendation. We will review the corrective action plan when submitted to OIG to determine whether OIT's plan is responsive to the recommendation.

(b)(7)(E)

Recommendation 5:

The Office of Information Technology should implement (b)(7)(E) (b)(7)(E)

Management's Response. The COO and CIO concurred with the recommendation. Management has begun a project to implement (b)(7)(E) (b)(7)(E) Management's complete response is reprinted in Appendix V.

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

Finding 7: (b)(7)(E) System User Accounts Were Incorrectly Identified

(b)(7)(E)

(b)(7)(E) However, the system owner did not properly identify account types for the system in accordance with NIST guidelines and OIT policy.

- NIST recommends that organizations manage information system accounts, including identifying account types (i.e., individual, group, system, application, anonymous, and temporary).[32] In addition, OIT policy[33] requires the OIT to identify account types. We reviewed a list of approximately (b)(7)(E) user accounts and found that (b)(7)(E) were incorrectly identified as user accounts. According to OIT (b)(7)(E) non-user accounts were active directory groups[34] (b)(7)(E) (b)(7)(E) accounts.

(b)(7)(E)

Recommendation 6:

(b)(7)(E)

Management's Response. (b)(7)(E) concurred with the recommendation. (b)(7)(E) (b)(7)(E)

[32] NIST SP 800-53, Rev. 3, p. F-3, AC-2.

[33] CIO-PD-08-06, pp. 28-29, Section 5-B-01.

[34] An active directory group is a collection of objects including users, services, computers and other groups that can be managed as a single unit.

(b)(7)(E) Management's complete response is reprinted in Appendix V.

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

Finding 8: OIT Does Not (b)(7)(E) (b)(7)(E)

The OIT does not comply with NIST guidelines and its own policy for maintaining a (b)(7)(E)

- (b)(7)(E)
- (b)(7)(E)

(b)(7)(E)

- (b)(7)(E)

(b)(7)(E)

Recommendation 7:

The Office of Information Technology should (b)(7)(E) (b)(7)(E)

Management's Response. The COO and CIO concurred with the recommendation. Management indicated they have begun (b)(7)(E) (b)(7)(E) (b)(7)(E) Management's complete response is reprinted in Appendix V.

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

[40] (b)(7)(E)

[41]

Recommendation 8:

The Office of Information Technology should (b)(7)(E) [redacted] (b)(7)(E) [redacted]

Management's Response. The COO and CIO concurred with the recommendation. Management's complete response is reprinted in Appendix V.

OIG Evaluation of Management's Response. We are pleased that management concurred with this recommendation. We will review the corrective action plan when submitted to OIG to determine whether OIT's plan is responsive to the recommendation.

Finding 9: Alternate Business Owner for the SEC's (b)(7)(E) Requires Training

(b)(7)(E) (b)(7)(E) The system has about 60 users and is described in the SEC enterprise disaster recovery plan as a primary, mission critical system. We determined that, during the business owner's extended, unscheduled leave, (b)(7)(E) had not formally designated an alternate business owner for the (b)(7)(E) Further, the information system owner was not actively involved in all aspects of the ongoing management of the system.

- **Business Owner Roles and Responsibilities.** The OIT requires that system business owners be chosen from the division or office that uses the system. Business owners should be familiar with a system's business uses and should be able to authorize access to information within the system. Specifically, business owners are responsible for the following actions:
  - approving, authorizing, and documenting system account actions;
  - periodically reviewing audit reports;
  - reviewing system accounts semiannually;
  - participating in system authorization meetings;
  - reviewing SSPs and the POA&M;
  - working with the OIT to complete the business impact analysis and privacy analysis worksheet; and
  - ensuring the business office participates in annual contingency plan tests and exercises.[42]

  We found that the business owner of the (b)(7)(E) has been on (b)(7)(E) does not know when the business owner is expected to return During the business owner's absence, (b)(7)(E) had not formally assigned an alternate or secondary business owner. During the initial phase of the business owner's absence, a Deputy Director acted in lieu of the business owner. (b)(7)(E) staff were deployed to participate in the SEC-wide disaster recovery exercises, and OIT resources were located for preparing certain reports. According to (b)(7)(E) staff, (b)(7)(E) was unable to immediately assign an alternate business system owner because it lacked the resources to do so. However, on March 12, 2014, (b)(7)(E)

[42] SEC Memorandum, *Revision of System Owner Responsibilities* (June 11, 2013), from the Chief Information Security Officer and certification agent.

formally designated an alternate business owner and plans to provide necessary training for that individual. While assigning an alternate business owner provides needed oversight and support for the (b)(7)(E) should provide training to the alternate business owner to reduce the security-related risks to the system.

- **Information System Owner Roles and Responsibilities.** The OIT also requires that all systems have an OIT-assigned information system owner who is responsible for the overall security state of the system and who provides adequate oversight and support for the security assessment and authorization (SA&A)[43] and continuous monitoring processes. Specifically, information system owners are responsible for the following actions:

  - participating in SA&A activities, including remediating POA&M;
  - reviewing the SSP and contingency plan;
  - maintaining standard operating procedures;
  - participating in continuous monitoring and contingency plan testing and exercises; and
  - reviewing accounts and audit reports.[44]

  Although the (b)(7)(E) system owner was assigned in November 2012 and performed some of the above responsibilities, such as remediating items documented in the POA&M report quarterly, he was not actively involved in all aspects of the ongoing management of the system. For example, we found that he was not reviewing the SSP and contingency plan, participating in contingency plan testing and exercises, or reviewing accounts and audit reports.

  Subsequent to the OIG's Cyberscope submission, the OIT began contacting information system owners to remind them of their roles and responsibilities and the resources available to help them properly execute their responsibilities. (b)(7)(E) has also conducted some of the information system owner responsibilities for the (b)(7)(E) such as disaster recovery (contingency plan) exercises. Finally, the OIT briefed the (b)(7)(E) owner on the technical and administrative aspects of the system. Therefore, we are not making a recommendation pertaining to the information system owner.

[43] "SA&A" is also known as certification and accreditation.

[44] SEC Memorandum, *Revision of System Owner Responsibilities*, pp. 1-2.

Recommendation 9:

The (b)(7)(E) should train the alternate business owner for the (b)(7)(E) on their roles and responsibilities relating to the system.

Management's Response. The Director of the (b)(7)(E) concurred with the recommendation. The Director selected a new alternate business owner for the (b)(7)(E) who is conversant with the application's purposes, uses, and features. The alternate business owner was provided training and a reference guide, as well as signed an acknowledgement of his awareness of his new role and receipt of the guide.

OIG Evaluation of Management's Response. We have verified management's corrective action taken in response to the recommendation. The recommendation is resolved and will be closed upon issuance of this report.

Appendix I. Scope and Methodology

Scope. NIT conducted this review from June 2013 to March 2014. The scope of the review consisted of the following 11 areas specified in OMB's FY 2013 FISMA reporting instructions:

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

Methodology. The overall objective of the 2013 FISMA evaluation was to assess the SEC's systems and provide the OIG with input for the SEC's response to *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics.* To meet this objective, and as further described below, we reviewed and evaluated the SEC's implementation of information security requirements, conducted interviews of SEC personnel, performed process walkthroughs, and reviewed relevant documents. We provided the OIG with the results of our evaluation, and we recommended responses for submission to the OMB. Using NIT's evaluation and recommendations, the OIG submitted to the OMB, on November 26, 2013, its responses to the 2013 FISMA questionnaire through OMB's Cyberscope reporting tool.

We based our review of the SEC's information security program on guidance issued by the OMB, the Department of Homeland Security, and NIST. We completed the data collection instruments required for 2013 FISMA reporting, performed the necessary evaluation procedures to answer questions published by the OMB and the Department of Homeland Security in its reporting guidance, and compiled this report for the SEC OIG.

To complete the OIG's portion of the annual FISMA questionnaire and to address the evaluation objectives, we interviewed key OIT personnel such as information system owners, OIT staff, and other stakeholders. We also examined governing policies, procedures, processes, and other related documentation and 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 judgmentally selected sample of 7 of the SEC's 59 major information systems. The sample consisted of the internally-hosted and externally-hosted systems shown in Table 1 below.

Table 1: Sample of the SEC Systems Evaluated

No.	System Name	System Description
1	(b)(7)(E)	
2	(b)(7)(E)	(b)(7)(E)
3	Office of the Chief Accountant	An internal system used by the Office of the Chief Accountant to track issues such as consultation or opinions on complex accounting matters.
4	Tracking Reporting Examination National Documentation System	The Office of Compliance Inspections and Examinations' internal national examination document system.
5	Extensible Business Reporting Language End User Tool (XBRL EUT)	An internal system for analyzing financial data, primarily used by the Division of Risk, Strategy, and Financial Innovation, Office of Interactive Disclosure. The SEC retired the system on October 25, 2013.
6	(b)(7)(E)	(b)(7)(E)
7	Federal Shared Services Provider	An externally-hosted system that owns, operates, and maintains the core financial management and procurement systems for the SEC.

Source: NIT generated

We based our judgmental sample on a limited scope review of both internally-hosted systems and externally-hosted systems found in the SEC's inventory compliance workbook.

In addition, we conducted a walkthrough of the OIT's processes related to our evaluation. We performed the walkthroughs with SEC officials to discuss and confirm our findings.

Finally, to determine the OIT's compliance with FISMA and OMB and NIST guidelines, we reviewed the OIT's security assessment packages, POA&Ms, SSPs, risk assessments, security test and evaluation reports, certification and accreditation memoranda, and applicable policies and procedures.

Overall, we based our analysis on information from interviews, support documentation, artifacts, governing guidance, and our expertise.

Management Controls. Consistent with the objectives of this review, we did not assess the OIT's management control structure. We reviewed the SEC's controls specific to the 2013 FISMA OIG questionnaire. To understand thoroughly the OIT's management controls pertaining to its policies, procedures, and methods of operation, we relied on information requested from and supplied by the OIT staff and information from interviews with various OIT personnel.

Use of Computer-Generated Data. We did not assess the reliability of the OIT's computer-generated data because it did not pertain to our objectives. Further, we did not perform any tests on the general or application controls over the OIT's automated systems because such tests were not within the scope of our work. The information retrieved from these systems as well as the requested documentation provided to us was sufficient, reliable, and adequate for meeting our stated objectives.

Prior Coverage. NIT reviewed the OIG's 2011 and 2012 FISMA reports,[45] which included 13 and 11 recommendations for corrective action, respectively. The OIT has implemented 20 of those 24 recommendations. While the OIT is working to address the four outstanding recommendations, as we note in this report, weaknesses still exist.

[45] *OIG 2011 FISMA Executive Summary Report, Report No. 501,* (February 2, 2012). The report can be accessed over the Internet at http://www.sec-oig.gov/Reports/AuditsInspections/2012/501.pdf.

OIG 2012 FISMA Executive Summary Report, *Report No. 512,* (March 29, 2013). The report can be accessed over the Internet at http://www.sec.gov/about/offices/oig/reports/audits/2013/512.pdf.

Appendix II. Applicable Federal Laws, Regulations, Policies, and Guidance

We reviewed the following during the course of our fieldwork:

Federal Laws and Guidance

- 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-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.
- 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 2013 Inspector General Federal Information Security Management Act Reporting Metrics.*
- NIST Special Publications (SP)
  - SP 800-16, *Information Security Technology Training Requirements: A Role- and Performance-Based Model*, April 1998.
  - SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2012.
  - SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.
  - SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.

  - SP 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security*, June 2009.

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

  - SP 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, June 2010.

  - SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, January 2005.

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

- 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 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006.

SEC Policies and Procedures

- SEC OIT CIO Policy Directive CIO-PD-08-06, *SEC OIT Security Policy Framework*, August 7, 2012.

- SEC Administrative Regulation SECR 301-01, *Operational Risk Management (ORM) and Internal Control Program (Draft)*, August 2013.

- SEC Branch Owned Document, Customer Service Branch, *LAN and Telephone Request,* May 28, 2013.

- We also reviewed the 43 SEC security control procedures shown in Appendix III.

Appendix III. OIT Procedures for Security Control and Date of Last Update

As stated in Finding 1, the 43 security control procedures shown in Table 2 below were outdated as of December 2013.[46] According to SEC policy, OIT should have updated 95 percent of the 43 procedures between 4 and 7 years ago.

Table 2: Outdated Security Control Procedures

FISMA Controls	No.	Name of Procedure	Procedure Number	Date Last Updated	Defined Frequency	Where Frequency Specified	Number of Years Outdated
(b)(7)(E) [redacted]	1	(b)(7)(E) [redacted]	[redacted]	Mar. 13, 2007	Annual	Specified in procedure	5 years
	2	[redacted]	[redacted]	Jan. 3, 2006	Annual	Specified in procedure	6 years
	3	[redacted]	[redacted]	Dec. 30, 2005	Annual	Specified in procedure	7 years
	4	[redacted]	[redacted]	Apr. 24, 2006	Annual	Specified in procedure	6 years
	5	[redacted]	[redacted]	Apr. 17, 2006	Annual	Specified in procedure	6 years
	6	[redacted]	[redacted]	Jan. 11, 2006	Annual	Specified in procedure	6 years
	7	[redacted]	[redacted]	Dec. 30, 2005	Annual	Specified in procedure	7 years
	8	[redacted]	[redacted]	Apr. 17, 2006	Annual	Specified in procedure	6 years
	9	[redacted]	[redacted]	Apr. 17, 2006	Annual	Specified in procedure	6 years
	10	[redacted]	[redacted]	Apr. 17, 2006	Annual	Specified in procedure	6 years
	11	[redacted]	[redacted]	Dec. 30, 2005	Annual	Specified in procedure	7 years

[46] NIT last accessed the OIT's security procedures site on December 22, 2013.

FISMA Controls	No.	Name of Procedure	Procedure Number	Date Last Updated	Defined Frequency	Where Frequency Specified	Number of Years Outdated
(b)(7)(E) [redacted] (Continued)	12	(b)(7)(E) [redacted]	[redacted]	Dec. 28, 2005	Annual	Specified in procedure	7 years
	13	[redacted]	[redacted]	Dec. 29, 2005	Annual	Specified in procedure	7 years
	14	[redacted]	[redacted]	Jan. 11, 2006	3 years	IT Security Compliance Program Policy	4 years
	15	[redacted]	[redacted]	Jan. 11, 2006	3 years	IT Security Compliance Program Policy	4 years
	16	[redacted]	[redacted]	Dec. 30, 2005	3 years	IT Security Compliance Program Policy	5 years
	17	[redacted]	[redacted]	Dec. 30, 2005	3 years	IT Security Compliance Program Policy	5 years
	18	[redacted]	[redacted]	Dec. 30, 2005	3 years	IT Security Compliance Program Policy	5 years
	19	[redacted]	[redacted]	Jan. 3, 2006	3 years	IT Security Compliance Program Policy	4 years
	20	[redacted]	[redacted]	Jan. 3, 2006	3 years	IT Security Compliance Program Policy	4 years
	21	[redacted]	[redacted]	Dec. 30, 2005	3 years	IT Security Compliance Program Policy	5 years
	22	[redacted]	[redacted]	Apr. 17, 2006	3 years	IT Security Compliance Program Policy	4 years
	23	[redacted]	[redacted]	Jan. 11, 2006	3 years	IT Security Compliance Program Policy	4 years
	24	[redacted]	[redacted]	Jan. 11, 2006	3 years	IT Security Compliance Program Policy	4 years
	25	[redacted]	[redacted]	Jan. 11, 2006	3 years	IT Security Compliance Program Policy	4 years

FISMA Controls	No.	Name of Procedure	Procedure Number	Date Last Updated	Defined Frequency	Where Frequency Specified	Number of Years Outdated
(b)(7)(E) (Continued)	26	(b)(7)(E)		Jan. 11, 2006	3 years	IT Security Compliance Program Policy	4 years
	27			Dec. 30, 2005	3 years	IT Security Compliance Program Policy	5 years
	28			Dec. 30, 2005	3 years	IT Security Compliance Program Policy	5 years
	29			Dec. 30, 2005	3 years	IT Security Compliance Program Policy	5 years
	30			Apr. 17, 2006	3 years	IT Security Compliance Program Policy	4 years
	31			Mar. 17, 2006	Annual	Specified in procedure	6 years
	32			Mar. 17, 2006	3 years	IT Security Compliance Program Policy	4 years
	33			Apr. 18, 2006	Annual	Specified in procedure	6 years
	34			Apr. 18, 2006	Annual	Specified in procedure	6 years
	35			July 3, 2006	Annual	Specified in procedure	6 years
(b)(7)(E)	36			Aug. 9, 2007	Annual	Specified in procedure	5 years
	37			Mar. 6, 2007	3 years	IT Security Compliance Program Policy	3 years

FISMA Controls	No.	Name of Procedure	Procedure Number	Date Last Updated	Defined Frequency	Where Frequency Specified	Number of Years Outdated
(b)(7)(E) [redacted]	38	(b)(7)(E) [redacted]	[redacted]	May 30, 2006	Annual	Specified in procedure	6 years
	39	[redacted]	[redacted]	Dec. 29, 2005	Annual	Specified in procedure	7 years
	40	[redacted]	[redacted]	June 29, 2005	Annual	Specified in procedure	7 years
	41	[redacted]	[redacted]	Aug. 20, 2002	3 years	IT Security Compliance Program Policy	8 years
	42	[redacted]	[redacted]	Dec. 30, 2005	Annual	Specified in procedure	7 years
	43	[redacted]	[redacted]	Dec.12, 2005	Annual	Specified in procedure	7 years

Source: NIT generated.

Appendix IV. SEC's Major Information Systems

According to the SEC's inventory compliance workbook (dated July 5, 2013), the agency's 59 major information systems are those shown in Table 3 below. The (b)(7)(E) [redacted]

Table 3: SEC's Major Information Systems

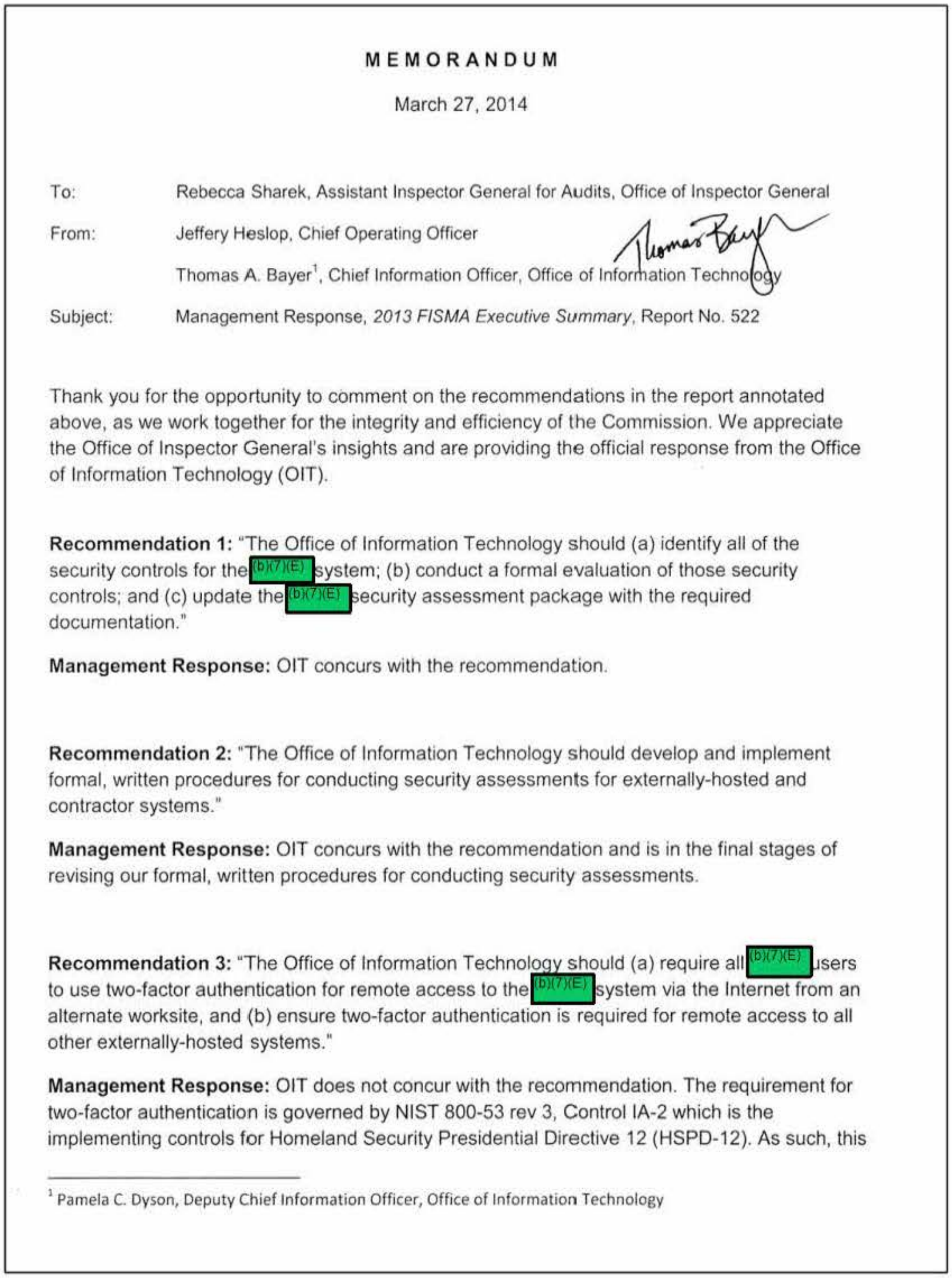
No.	Name of System
1	(b)(7)(E) [redacted]
2	[redacted]
3	[redacted]
4	[redacted]
5	[redacted]
6	[redacted]
7	[redacted]
8	[redacted]
9	[redacted]
10	[redacted]
11	[redacted]
12	[redacted]
13	[redacted]
14	[redacted]
15	[redacted]
16	[redacted]
17	[redacted]
18	[redacted]
19	[redacted]
20	[redacted]
21	[redacted]
22	[redacted]
23	[redacted]
24	[redacted]
25	[redacted]
26	[redacted]
27	[redacted]
28	[redacted]
29	[redacted]
30	[redacted]
31	[redacted]
32	[redacted]

No.	Name of System
33	(b)(7)(E) [redacted]
34	[redacted]
35	[redacted]
36	[redacted]
37	[redacted]
38	[redacted]
39	[redacted]
40	[redacted]
41	[redacted]
42	[redacted]
43	[redacted]
44	[redacted]
45	[redacted]
46	[redacted]
47	[redacted]
48	[redacted]
49	[redacted]
50	[redacted]
51	[redacted]
52	[redacted]
53	[redacted]
54	[redacted]
55	[redacted]
56	[redacted]
57	[redacted]
58	[redacted]
59	[redacted]

Source: NIT generated.

[47] The SEC retired the XBRL EUT system on October 25, 2013.

Appendix V. Management Comments



MEMORANDUM

March 27, 2014

To: Rebecca Sharek, Assistant Inspector General for Audits, Office of Inspector General

From: Jeffery Heslop, Chief Operating Officer

Thomas Bayer

Thomas A. Bayer[1], Chief Information Officer, Office of Information Technology

Subject: Management Response, *2013 FISMA Executive Summary*, Report No. 522

Thank you for the opportunity to comment on the recommendations in the report annotated above, as we work together for the integrity and efficiency of the Commission. We appreciate the Office of Inspector General's insights and are providing the official response from the Office of Information Technology (OIT).

Recommendation 1: "The Office of Information Technology should (a) identify all of the security controls for the (b)(7)(E) system; (b) conduct a formal evaluation of those security controls; and (c) update the (b)(7)(E) security assessment package with the required documentation."

Management Response: OIT concurs with the recommendation.

Recommendation 2: "The Office of Information Technology should develop and implement formal, written procedures for conducting security assessments for externally-hosted and contractor systems."

Management Response: OIT concurs with the recommendation and is in the final stages of revising our formal, written procedures for conducting security assessments.

Recommendation 3: "The Office of Information Technology should (a) require all (b)(7)(E) users to use two-factor authentication for remote access to the (b)(7)(E) system via the Internet from an alternate worksite, and (b) ensure two-factor authentication is required for remote access to all other externally-hosted systems."

Management Response: OIT does not concur with the recommendation. The requirement for two-factor authentication is governed by NIST 800-53 rev 3, Control IA-2 which is the implementing controls for Homeland Security Presidential Directive 12 (HSPD-12). As such, this

[1] Pamela C. Dyson, Deputy Chief Information Officer, Office of Information Technology

Finding and Recommendation are duplicates of Finding 3 *OIT Has Not Implemented PIV Cards for Logical Access*. In addition (b)(7)(E) (b)(7)(E) covered. We respectfully request this Recommendation be closed upon issuance in accordance with our revised policies.

Recommendation 4: "The Office of Information Technology should (b)(7)(E) (b)(7)(E)

Management Response: OIT concurs with the recommendation.

Recommendation 5: "The Office of Information Technology should implement (b)(7)(E) (b)(7)(E)

Management Response: OIT concurs with the recommendation and has begun an explicit project to implement (b)(7)(E)

Recommendation 6: (b)(7)(E) (b)(7)(E)

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

Recommendation 7: "The Office of Information Technology should conduct a comprehensive (b)(7)(E)

Management Response: OIT concurs with the recommendation and has begun a review of its (b)(7)(E)

Recommendation 8: "The Office of Information Technology should conduct (b)(7)(E) (b)(7)(E)

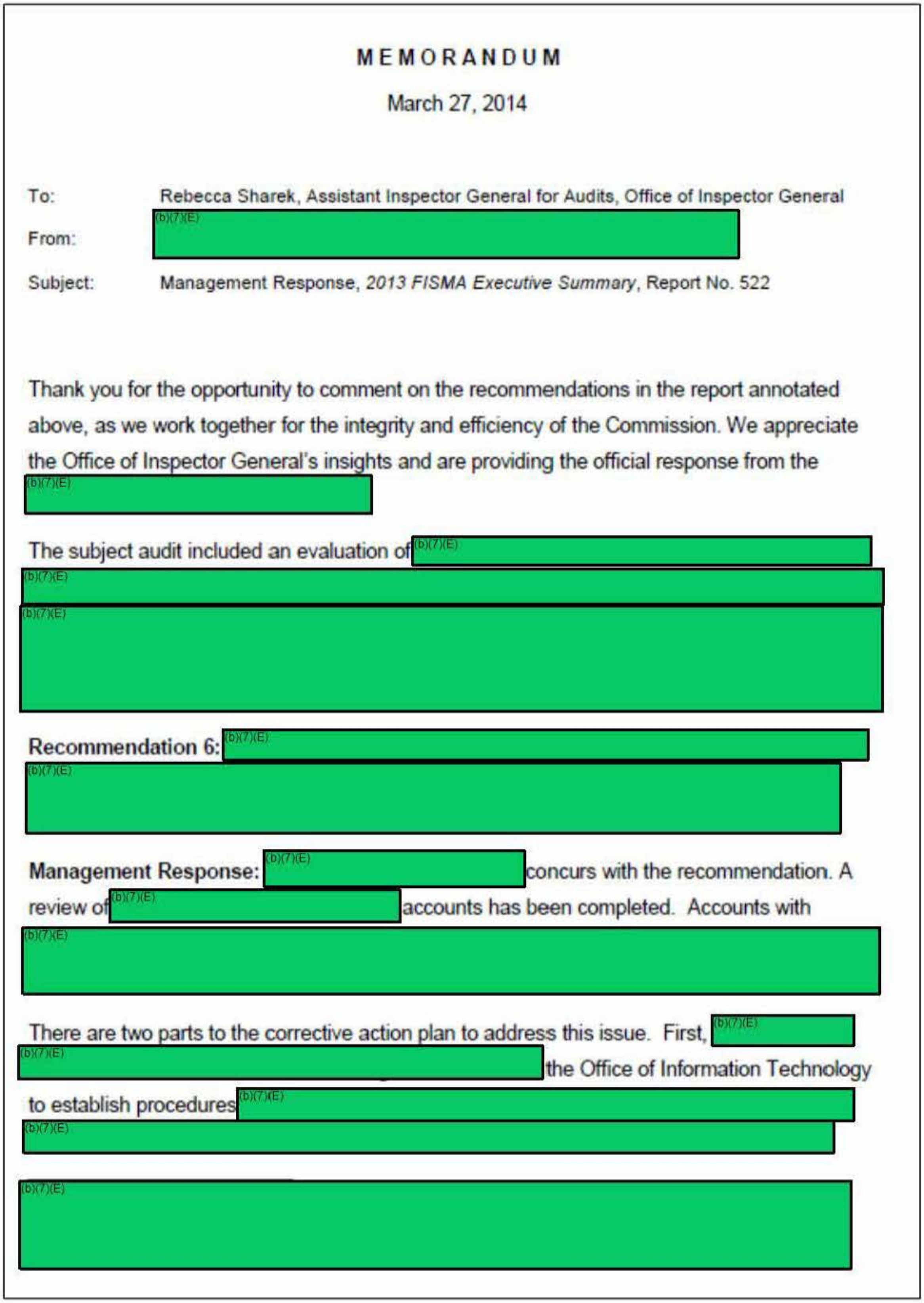
Management Response: OIT concurs with the recommendation.

Recommendation 9: "The (b)(7)(E) should train the alternate business owner for the (b)(7)(E) system on their roles and responsibilities relating to the system."

Management Response: (b)(7)(E) will respond separately.

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.



MEMORANDUM

March 27, 2014

To: Rebecca Sharek, Assistant Inspector General for Audits, Office of Inspector General

From: (b)(7)(E)

Subject: Management Response, *2013 FISMA Executive Summary*, Report No. 522

Thank you for the opportunity to comment on the recommendations in the report annotated above, as we work together for the integrity and efficiency of the Commission. We appreciate the Office of Inspector General's insights and are providing the official response from the (b)(7)(E)

The subject audit included an evaluation of (b)(7)(E) (b)(7)(E) (b)(7)(E)

Recommendation 6: (b)(7)(E) (b)(7)(E)

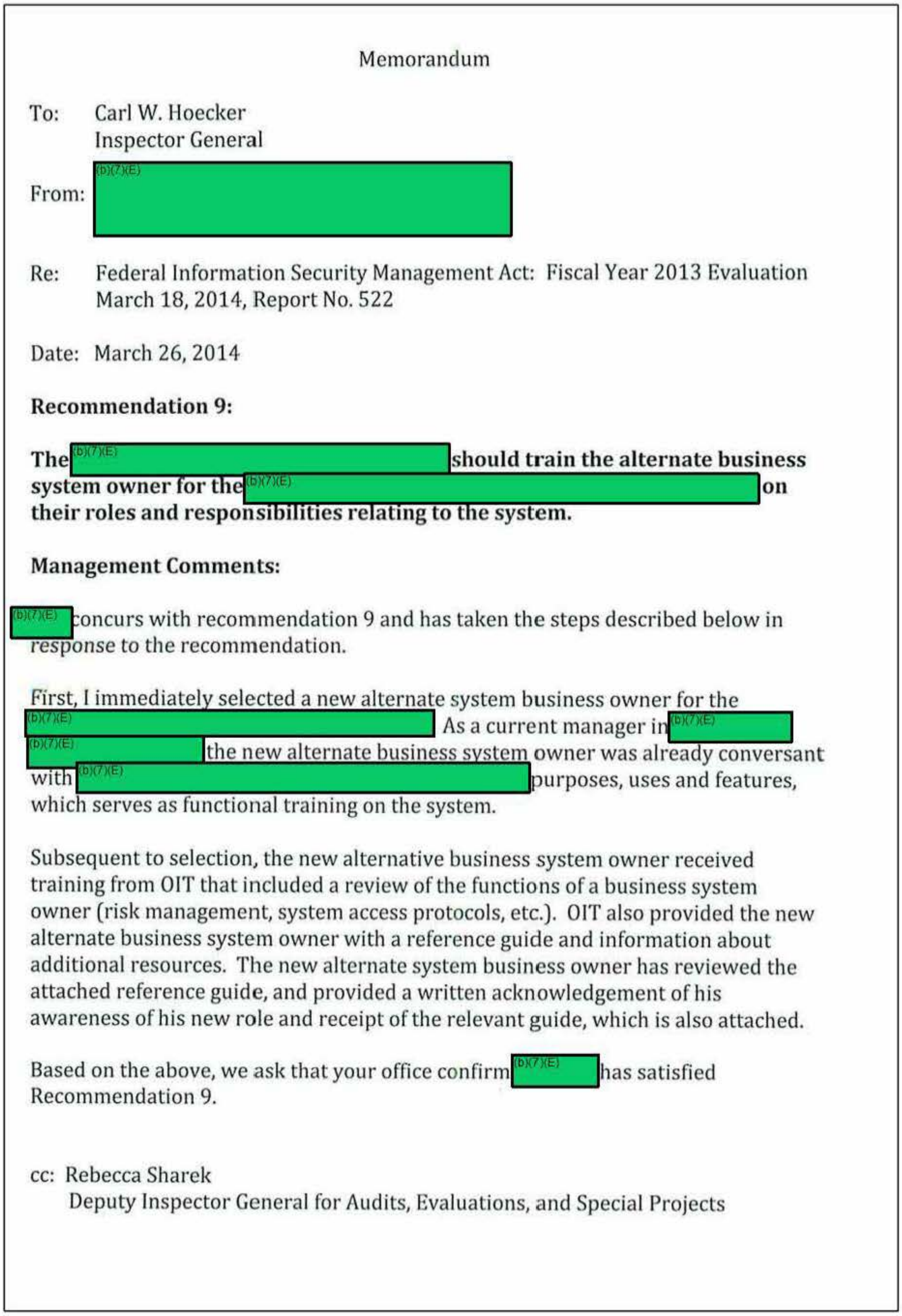
Management Response: (b)(7)(E) concurs with the recommendation. A review of (b)(7)(E) accounts has been completed. Accounts with (b)(7)(E)

There are two parts to the corrective action plan to address this issue. First, (b)(7)(E) (b)(7)(E) the Office of Information Technology to establish procedures (b)(7)(E) (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

[redacted]



Memorandum

To: Carl W. Hoecker
Inspector General

From: (b)(7)(E)

Re: Federal Information Security Management Act: Fiscal Year 2013 Evaluation
March 18, 2014, Report No. 522

Date: March 26, 2014

Recommendation 9:

The (b)(7)(E) should train the alternate business system owner for the (b)(7)(E) on their roles and responsibilities relating to the system.

Management Comments:

(b)(7)(E) concurs with recommendation 9 and has taken the steps described below in response to the recommendation.

First, I immediately selected a new alternate system business owner for the (b)(7)(E) As a current manager in (b)(7)(E) (b)(7)(E) the new alternate business system owner was already conversant with (b)(7)(E) purposes, uses and features, which serves as functional training on the system.

Subsequent to selection, the new alternative business system owner received training from OIT that included a review of the functions of a business system owner (risk management, system access protocols, etc.). OIT also provided the new alternate business system owner with a reference guide and information about additional resources. The new alternate system business owner has reviewed the attached reference guide, and provided a written acknowledgement of his awareness of his new role and receipt of the relevant guide, which is also attached.

Based on the above, we ask that your office confirm (b)(7)(E) has satisfied Recommendation 9.

cc: Rebecca Sharek
Deputy Inspector General for Audits, Evaluations, and Special Projects

Appendix VI. OIG Response to Management Comments

The OIG is pleased that OIT, (b)(7)(E) [redacted] concurred with eight of the nine recommendations for corrective action. We are also encouraged that management has indicated that it has taken or planned certain actions to address many of the recommendations in this report, as well as the outstanding recommendations from the FYs 2011 and 2012 FISMA evaluations. We have verified the corrective actions (b)(7)(E) [redacted] has taken in response to our recommendation and will close the recommendation upon issuance of this report. In addition, we will review management's corrective action plan when it is submitted to determine whether the plan is responsive to each of the report recommendations. We believe that fully implementing our recommendations should strengthen the SEC's information security posture.

While OIT noncurred with Recommendation 3 of this report, we have determined the actions taken by OIT to address the recommendation are responsive and the recommendation will be closed upon completion and verification of the actions.

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

Web:	www.reportlineweb.com/sec_oig
E-mail:	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 executive summary 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) 551-6083. 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.