U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

2012 FISMA Executive Summary Report

March 29, 2013
Report No. 512

REDACTED PUBLIC VERSION

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

March 29, 2013

To: Jeff Heslop, Chief Operating Officer, Office of the Chief Operating Officer
Thomas A. Bayer, Director/Chief Information Officer, Office of Information Technology

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

Subject: *2012 FISMA Executive Summary Report*, Report No. 512

This memorandum transmits the U.S. Securities and Exchange Commission (SEC), Office of Inspector General's (OIG) final report detailing the results of our *2012 FISMA Executive Summary Report*. The review was conducted as part of our continuous effort to assess management of the Commission's programs and operations and as a part of our annual audit plan.

The report contains 11 recommendations which if fully implemented should strengthen the SEC's controls over information security. The Office of the Chief Operating Officer and the Office of Information Technology concurred with all the recommendations that were addressed to their respective offices. Your written response to the draft report is included in Appendix VII.

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

REDACTED PUBLIC VERSION

Should you have any questions regarding this report, please do not hesitate to contact me. We appreciate the courtesy and cooperation that you and your staff extended to our office.

Attachment

cc: Elisse B. Walter, Chairman
Erica Y. Williams, Deputy Chief of Staff, Office of the Chairman
Luis A. Aguilar, Commissioner
Troy A. Paredes, Commissioner
Daniel Gallagher, Commissioner
Pamela C. Dyson, Deputy Director/Deputy Chief Information Officer, Office of Information Technology
Todd K. Scharf, Associate Director, Chief Information Security Officer, Office of Information Technology

REDACTED PUBLIC VERSION

2012 FISMA Executive Summary Report

Executive Summary

The U.S. Securities and Exchange Commission (SEC or Commission) Office of Inspector General (OIG) contracted the services of Networking Institute of Technology, Inc. (NIT) to conduct the fiscal year 2012 Federal Information Security Management Act (FISMA) assessment and a review of the SEC's security requirements.

FISMA was enacted, in 2002 as *Title III of the E-Government Act of 2002,* to recognize the importance of information security to the economic and national security interests of the United States.[1] The law emphasizes the need for organizations to develop, document, and implement organization-wide programs providing security for the information systems supporting the organization's operations and assets, as well as information systems provided or managed by other agencies, contractors, or other sources. FISMA provides the framework for securing the federal government's information technology (IT) and requires agency program officials, chief information officers (CIO), privacy officers, and inspectors general to conduct annual reviews of the agency's information security and privacy programs and report the results to Office of Management and Budget (OMB). For fiscal year 2012, FISM 12-02 provides instructions to heads of executive departments and agencies for meeting the fiscal year 2012 reporting requirements. It also requires inspectors general to independently evaluate and report how their department's or agency's CIO, senior agency official for privacy, and program officials implemented information security requirements.

The Office of Information Technology (OIT) supports the SEC and its staff in all areas of IT. The office has overall management responsibility for the Commission's IT program including application development, infrastructure operations and engineering, user support, IT program management, capital planning, security, enterprise architecture, and implementing the SEC's FISMA requirements. OIT's CIO is responsible for developing and maintaining a Commission-wide information security program. The office also includes a Chief Information Security Officer (CISO) who, among other things, is responsible for establishing and maintaining the SEC's security posture.

Objectives. The overall objective of the 2012 FISMA assessment was to assess the SEC's systems and provide OIG with input to the SEC's response to the

[1] Title III, Publication L, No. 107-347 (December 17, 2002).

REDACTED PUBLIC VERSION

OMB. The assessment included a review of the SEC's information security posture, as required annually by FISMA. The 2012 FISMA assessment included the following mandated security requirements:

- continuous monitoring management
- configuration management
- identity and access management
- incident response and reporting
- risk management
- security training
- plan of action and milestones
- remote access management
- contingency planning
- contractor systems
- security capital planning

In addition to the mandated security requirements, NIT independently evaluated and reported on how the Commission has implemented the following security requirements:

- systems inventory and the quality of the inventory
- enterprise security architecture
- data and boundary protection
- network security protocols

The evaluation criteria for the requirements listed above is based on the National Institute of Standards and Technology (NIST) standards and industry best practices. There were no findings related to these requirements.

Results. Our review found that OIT did not fully conduct and document continuous monitoring in accordance with certain NIST requirements. Continuous monitoring is the process where organizations develop a strategy and implement a program for the continuous monitoring of security control effectiveness. It includes the potential need to change or supplement a control set, taking into account any proposed/actual changes to the information system or its operational environment. OIT conducts penetration testing and vulnerability scanning on a continuous basis and provided NIT with its penetration test reports. However, we found that penetration testing is not sufficient to meet the continuous monitoring strategy requirements per NIST Special Publication (SP) 800-137. We also found that OIT did not test some areas between the three-year certification and accreditation (C&A) assessment cycle, or on a continuous basis for critical security controls. As a result, OIT's continuous monitoring program needs improvement.

Further, we found that OIT configuration management program is generally in compliance with governing FISMA requirements and NIST guidelines. However, OIT has not defined baseline configurations and it has not conducted configuration compliance scanning for [redacted]. OIT implemented configuration baselines for all [redacted] and it scans all [redacted] for baseline configuration compliance and documents and it approves all deviations from the baseline. Also, OIT did not implement configuration baselines for [redacted]. OIT began establishing baselines and implemented compliance scanning for [redacted] in August of 2012 and asserts it is scheduled to be completed with the process by the end of March 2013. However, OIT has not fully implemented baseline configurations and compliance scanning [redacted].

Additionally, OIT has not approved a formal project plan to implement personal identity verification (PIV) and it has not implemented a technical solution to link PIV badges to multi-factor authentication. As a result, the SEC is not compliant with the Federal Information Processing Standards Publication (FIPS) 201-1, which could expose the Commission to unauthorized access to its information systems.

Our assessment of the SEC's risk management strategy found that it does not address the requirements needed for a comprehensive governance structure and organizational overall security risk management. Further, it does not address risk from a mission and business process perspective, as described in the risk management framework (RMF) identified in NIST SP 800-37, Rev. 1.2.[3] As a result of not updating the risk management strategy to address NIST guidelines, the SEC could be exposed to higher risk levels.

Our review also found that Designated Authorizing Officials are not fully involving the Information System Owners (ISO) in system security categorization as directed by NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Lifecycle Approach, Task 1-1*. Not involving the ISO in the categorization process runs the risk of them not understanding the overall context of the system and the subsequent security controls needed to properly safeguard agency information. Our review of the documentation for the systems in our sample universe found that the systems in our sample had FIPS 199 system security categorizations.

Based on our review we determined that OIT did not tailor its baseline security controls for specific systems that require such controls. We further found OIT did

[2] NIST SP 800-37, Rev. 1, p. 2, Section 1.2, Purpose and Applicability.
[3] NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (February 2010) p. 2, Section 1.2, Purpose and Applicability.

REDACTED PUBLIC VERSION

not tailor baseline security controls for the nine information systems in our sample universe. Also, the system security plan for the systems in our sample universe did not include OIT's decision to not tailor during the security control selection process, nor its rationale for the decision. While OIT has not tailored baseline security controls, it has identified and selected a generic set of baseline security controls that are based on the security categorization of the system. OIT also did not develop formal procedures or instructions regarding tailoring it baseline security controls in accordance with NIST SP 800-53, Rev. 3 guidelines.

The security awareness training program could be improved by including role-based training for IT staff in information security. Moreover, IT security awareness training program does not specify who is required to take role-based training and there is no enforcement mechanism to ensure IT staff have taken the correct role-based training, based on duties and responsibilities. The IT security awareness training program should include role-based training for staff having information security duties.

Though OIT establishes milestone remediation dates for plan of action and milestones (POA&M) it did not adhere to specific milestone remediation dates identified when closing POA&Ms. As a result, POA&Ms are open for an extended period of time, which puts the Commission at risk if the weakness is not remediated in a timely manner.

Although OIT has now updated many of its policies, the office did not update the existing procedures for the 18 control families to ensure compliance with the new policy. OIT has not developed procedures for risk management, continuous monitoring management, and information security oversight over systems operated by SEC contractors and other entities. Though OIT has made progress in correcting policy deficiencies the lack of procedures could result in OIT improperly implementing informal procedures that is not consistent with management's expectations and current policy.

We further found OIT could improve its process for documenting the interfaces between the contractor/external systems and SEC-operated systems in its system inventory. The absence of interface data related to systems within the system inventory may lead to confusion when making risk-based decisions for external systems.

OIT did not disable the network accounts for all users who no longer require access or who no longer work at the SEC. As a result, some users still had access to the SEC's network, which put the Commission at a higher risk for malicious acts.

Finally, OIT had repeat findings and six repeat recommendations from a prior issued OIG report that have not been fully addressed and were found to still exist as deficiencies during this review.

Summary of Recommendations. The report contains 11 recommendations that were developed to strengthen the SEC's controls over information security. Our most significant recommendations were having OIT to revise its security assessment procedures, annually assess a subset of its manager system's security controls, and develop and implement a continuous monitoring strategy in accordance with applicable NIST requirements.

We further recommended OIT continue its implementation of its risk strategy to ensure risk is addressed at the organization, mission and business, and information system levels of the risk management framework. The Office of Risk Management should work with OIT to provide training to management throughout the Commission regarding their roles and responsibilities related to operating in a three-tiered risk management framework.

In addition, OIT should develop procedures to obtain documented approval, by adding a signature block to the security categorization form, from the system owner and the authorizing official in step one of the risk management framework.

To improve its POA&M tracking, we recommended OIT review all POA&Ms and update its tracking system to include future remediation dates and ensure POA&Ms are closed or mitigated to an acceptable level.

Finally, OIT should review all user accounts and disable accounts that are no longer needed and perform periodic reviews of user accounts and develop internal controls to ensure periodic reviews of user accounts are performed on accounts that are terminated.

Management's Response to the Report's Recommendations. OIG provided SEC management with the formal draft report on March 18, 2013. SEC management concurred with all recommendations in this report. OIG considers the report recommendations resolved. However, the recommendations will remain open until documentation is provided to OIG that supports each recommendation has been fully implemented. SEC management's response to each recommendation and OIG's analysis of their responses are presented after each recommendation in the body of this report.

The full version of this report includes information that the SEC considers to be sensitive and proprietary. To create this public version of the report, OIG redacted (blacked out) potentially sensitive, proprietary information from the report.

TABLE OF CONTENTS

Tables

Appendices

Figures

REDACTED PUBLIC VERSION

Background and Objectives

Background

The U.S. Securities and Exchange Commission (SEC or Commission) Office of Inspector General (OIG) contracted the services of Networking Institute of Technology, Inc. (NIT) to conduct the fiscal year 2012 Federal Information Security Management Act (FISMA) assessment and a review of the SEC's security requirements.

FISMA provides a framework for ensuring the effectiveness of information security controls over federal operations and assets and it serves as a mechanism for oversight of federal information security programs.[4] Agency information security programs must provide for among other things, periodic risk assessments, policies and procedures based on the risk assessments, periodic testing and evaluation of the effectiveness of policies and procedures, security planning, security awareness training, and continuity of operations. FISMA also requires federal agencies have an annual independent evaluation of their information security program and practices performed. The evaluation is conducted by the agency's inspector general or by an independent external auditor.[5]

FISMA also provides the framework for securing the Federal government's information technology (IT). FISMA emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide information security for the systems supporting its operations and assets. All agencies must implement FISMA requirements and report annually to the Office of Management and Budget (OMB).

The Department of Homeland Security Memorandum FISM 12-02 provided instructions to heads of executive departments and agencies for meeting the fiscal year 2012 reporting requirements. It also required inspectors general to independently evaluate and report how their department or agency's chief information officer (CIO), senior agency official for privacy, and program officials implemented information security requirements.

The Office of Information Technology (OIT) supports the SEC and its staff in all areas of IT. The office has overall management responsibility for the Commission's

[4] Title III, Pub. L, No. 107-347 (December 17, 2002).
[5] Ibid, § 3545(a), (b).

IT program including application development, infrastructure operations and engineering, user support, IT program management, capital planning, security, enterprise architecture, as well as the SEC's FISMA requirements. OIT's CIO is responsible for developing and maintaining a Commission-wide information security program. The office also includes a Chief Information Security Officer (CISO) who, among other things, is responsible for establishing and maintaining the SEC's security posture.

Objectives

The overall objective of the FISMA assessment was to assess the SEC's systems and provide the OIG with input to the SEC's response to the OMB. The assessment included a review of the SEC's information security posture, as required annually by FISMA. The FISMA assessment addressed the following mandated security requirements:

- continuous monitoring management
- configuration management
- identity and access management
- incident response and reporting
- risk management
- security training
- plan of action and milestones
- remote access management
- contingency planning
- contractor systems
- security capital planning

In addition to the mandated security requirements, NIT independently evaluated and reported on how the Commission has implemented the following security requirements:

- systems inventory and the quality of the inventory
- enterprise security architecture
- data and boundary protection
- network security protocols

The evaluation criteria for the objectives described above was based on National Institute of Standards and Technology (NIST) standards and industry best practices.

Findings and Recommendations

Finding 1: OIT's Continuous Monitoring Program Needs Improvement

> OIT did not fully conduct and document continuous monitoring for security controls in accordance with NIST guidelines and does not have a formal continuous monitoring program or strategy. As a result, the SEC could implement an insufficient security program and is not operating within acceptable risk tolerance levels.

OIT has not fully conducted and documented continuous monitoring for security controls. While OIT assessed all security controls on a three-year Certification and Accreditation (C&A) assessment cycle and a subset of controls were inherently tested in between the three-year C&A cycle, some critical security controls (i.e., access control, physical access control devices) have not been reviewed in some cases, up to three years. In addition, OIT's continuous monitoring strategy is not fully documented.

OIT's Continuous Monitoring

Continuous monitoring is the process where organizations develop a strategy and implement a program for the continuous monitoring of security control effectiveness. It includes the potential need to change or supplement a control set, taking into account any proposed/actual changes to the information system or its operational environment.[6] OIT's SEC's Operating Procedure (OP) 24-04-10-03, *IT Security Assessment Procedure,* issued April 28, 2006, mandates testing all common, system-specific and hybrid security controls at least every three years during the authorization period. This procedure does not address reviewing a subset of controls on a more frequent basis.

NIST Special Publication (SP) 800-37, Revision (Rev.) 1 requires organization identify critical security controls for ongoing monitoring and select a subset of security controls for monitoring during the off years of a full C&A assessment cycle.[7] The C&A process consists of a comprehensive assessment of the management, operational, and technical security controls in an information system. It is made in support of security accreditation to determine the extent to which the controls are implemented correctly, operating as intended, and are

[6] NIST SP 800-37, Rev. 1, p. G-1, Appendix G, Continuous Monitoring.
[7] Ibid.

producing the desired outcome with respect to meeting the security requirements for the system. Based on the results of the assessment, a senior agency official authorizes an information system to operate and explicitly accepts the risk to agency operations.[8]

Further, according to NIST SP 800-137 and NIST SP 800-37, Rev. 1, organizations should review a subset of their security controls to include management, operational, and technical security control families, and security controls that should be evaluated on a rotating basis. Further, critical security controls should be evaluated more frequent monitoring.

We judgmentally selected 9 of 59 information systems to test the security controls. We also conducted a limited-review of the SEC's information security posture. Our sample universe consisted of the following systems:

Consistent with the requirements in OP 24-04-10-03, our testing found that all the security controls for the systems in our sample universe were assessed once in OIT's three-year C&A assessment cycle. Moreover, we found that access control, identification and authentication, audit mechanisms, security configuration settings, physical access control devices, information system backup operations, incident response capability, and contingency planning were not tested in between the three-year C&A assessment cycle, or on a continuous basis for critical security controls. We found that this practice does not meet the requirements of a continuous monitoring strategy or plan according to NIST SP 800-137, NIST SP 800-37, Rev. 1, and NIST SP 800-53A, Rev. 1.

Although OIT conducts penetration testing and vulnerability scanning on a continuous basis to monitor the effectiveness critical security controls, penetration testing and vulnerability scanning do not review all critical security controls such as physical access control. While penetration testing and vulnerability scanning identifies system specific controls, it is not sufficient to meet the continuous monitoring strategy requirements per NIST SP 800-137. According to NIST SP 800-137, "Organization-wide monitoring cannot be

[8] NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems* (February 2006), pp. 31-32, Appendix B, Glossary.

REDACTED PUBLIC VERSION

efficiently achieved through manual processes alone or through automated processes alone."[9]

Continuous Monitoring Strategy

In August 2012, OIT issued Policy Directive CIO-PD-08 (CIO-PD-08). The CIO-PD-08 references continuous monitoring as follows:

> OIT establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:
>
> - A configuration management process for the information system and its constituent components;
> - A determination of the security impact of changes to the information system and environment of operation;
> - Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and
> - Reporting the security state of the information system to appropriate SEC officials based on an assessment of risk pertaining to the current threat environment. [10]

This policy references OIT's continuous monitoring strategy. However, OIT has not developed a formal continuous monitoring strategy or documented its continuous monitoring program per NIST SP 800-137 and NIST SP 800-37, Rev. 1. NIT was informed that OIT has a continuous monitoring strategy that is in the early stages of development, but it has not been formalized.

NIST SP 800-137 provides guidance for the development of a continuous monitoring program. We found that OIT's continuous monitoring strategy has not been developed or implemented and OIT has not taken steps to address the guidance identified in NIST SP 800-37, Rev. 1, which was released in February 2010 and defines the criteria for a continuous monitoring strategy.

For benchmarking purposes, we contacted the National Credit Union Administration (NCUA), Federal Deposit Insurance Corporation (FDIC), and the U.S. Commodity Futures Trading Commission (CFTC) regarding their FISMA related practices and procedure to comply with governing guidance such as NIST.

[9] NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (September 2011), p. vii.
[10] Policy Directive, Office of Information Technology, CIO Policy Directive, *SEC OIT Security Policy Framework*, Policy Number CIO-PD-08 (August 7, 2012), p. 57.

When asked about their compliance with NIST SP 800-137, and learned that each year NCUA, FDIC, and CFTC assesses a subset of controls or critical controls as part of their continuous monitoring process. NCUA and FDIC informed us they have established continuous monitoring programs. While, the CFTC indicated it is in the process of developing a continuous monitoring program.

Conclusion

As a result of not fully implementing continuous monitoring and assessing a subset of its critical security controls at least annually, OIT may not be operating within acceptable risk tolerance levels because they evaluate security controls every three years, rather than on a continuous or rotating basis. This could impact OIT's security program and result in the office being unable to fully produce evidence that is needed to determine the full security status of its information systems. Also, without a documented continuous monitoring strategy, OIT may not have adequate visibility into organizational assets, sufficient awareness of treats and vulnerabilities, or effectively deploy security controls.

Recommendation 1:

The Office of Information Technology should revise its information technology security assessment procedures to ensure they are consistent with its current practices and include verbiage to implement continuous monitoring and requirements for on-going assessment of a subset of critical security controls.

Management Comments. OIT concurred with this recommendation. See Appendix VII for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Recommendation 2:

The Office of Information Technology should develop and implement a continuous monitoring strategy in accordance with NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* and NIST Publication 800-37, Revision 1, *Guide for Applying Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*

Management Comments. OIT concurred with this recommendation. See Appendix VII for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Finding 2: OIT Has Not Fully Implemented Baseline Configurations and Compliance Scanning for [redacted]

OIT did not define baseline configurations and has not conducted configuration compliance scanning for [redacted]. Improperly configured devices could lead to potential weaknesses in OIT's systems.

NIT found that OIT's configuration management program is generally in compliance with governing FISMA requirements and NIST guidelines. However, OIT has not defined baseline configurations and it has not conducted configuration compliance scanning for [redacted].

We confirmed OIT has implemented configuration baselines for all [redacted]. OIT scans all [redacted] for baseline configuration compliance and documents and it approves all deviations from the baseline.[11] Further, we found all [redacted] have baseline configurations defined, using Center for Internet Security (CIS) standards. However, there are no allowable exceptions defined and approved for [redacted]

Although OIT has implemented the configuration baselines for [redacted], they have not fully implemented configuration baselines and configuration compliance scanning for [redacted]. OIT also did not implement configuration baselines for [redacted] because for the past year the office has focused on implementing baselines standards and compliance scanning for [redacted]. OIT began establishing baselines and implemented compliance scanning for [redacted] in August of 2012 and is scheduled to be completed with the process by the end of March 2013.

[11] [redacted].

REDACTED PUBLIC VERSION

OIT asserted that due to the lack of resources, it has not documented configuration baselines and conducted compliance scans for [redacted]. Our review also found that although OIT works toward a 100 percent goal, it does not maintain a documented list of exceptions to the baseline configuration of [redacted]. However, we confirmed that OIT documents and approves deviations from the baseline for [redacted].

As a result of not having updated configuration baselines for [redacted] and approved deviations for [redacted], OIT could inconsistently apply configurations to these devices, which could lead to potential weaknesses in its environment and present increased security related risks to the SEC's systems. Additionally, by not conducting compliance scans of [redacted], configuration settings may be altered without the administrator's knowledge of the network, devices may not meet minimum configuration requirements. Thus, it may be impossible to determine if the device configurations are aligned with approved baseline configurations. Further, OIT's current [redacted] may not comply with current FISMA and NIST best practices.

NIST Requirements. NIST SP 800-53, Rev. 3 guidelines specifies that organizations should develop, document, and maintain under configuration control…a current baseline configuration of the information system.[12] Our review found that OIT has not defined baseline configurations and while they conduct compliance scanning for [redacted], OIT has not conducted configuration compliance scanning for [redacted]. Although not required, OIT uses a tool to monitor configurations of the SEC's [redacted] for unauthorized changes.

With respect to configuration management NIST SP 800-53, Rev. 3 recommends that organizations:

a) Establish and document mandatory configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;
b) Implement configuration settings;
c) Identify, document, and approve exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
d) Monitor and control changes to configuration settings in

[12]NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* (August 2009), p. F-38.

REDACTED PUBLIC VERSION

accordance with the organization's policies and procedures.[13]

Repeat Recommendation from Prior OIG Report

We determined that the remedy for this finding would result in a repeat recommendation that was previously made in OIG's *2011 FISMA Executive Summary Report*, Report No. 501, issued in February 2012. Specifically, the report's Finding 4 "OIT Has Not Conducted Configuration Compliance Scans and Needs a Defined Process to Address Compliance Scan Results in a Timely Manner," found that OIT's baseline configurations were outdated and inconsistent with NIST guidance and OIT did not conduct configuration compliance scans.[14] OIT concurred with the following recommendation in the report:

> ***Recommendation 9:*** The Office of Information Technology should review and document its current standard baseline configuration, including identification of approved deviations and exceptions to the standard.

To date this recommendation is still open and OIT has not fully implemented it. We determined that because OIT is making progress in addressing this recommendation, a new recommendation will not be made in this report pertaining to conducting configuration compliance scans for [redacted] However, we encourage OIT to fully mitigate the deficiencies identified in the prior issued OIG report and in this finding and fully implement the recommendation in a timely manner.

Finding 3: OIT Has Not Implemented Multi-Factor Authentication to the SEC's PIV Program

> OIT has not approved a formal project plan to implement personal identity verification (PIV) and it has not implemented a technical solution to link PIV badges to multi-factor authentication. As a result, the SEC is not compliant with the Federal Information Processing Standards Publication 201-1, *Personal Identity Verification (PIV) of*

[13] NIST SP 800-53, Rev. 3, p. F-42.
[14] OIG, *2011 FISMA Executive Summary,* Report No. 501 (Feb. 2, 2012).

Federal Employees and Contractors.[15] This noncompliance could expose the Commission to unauthorized access to its information systems.

Our review found that OIT has not approved a formal project plan to implement PIV and it has not implemented a technical solution to link PIV badges to multi-factor authentication. Multi-factor authentication for system access is the process for establishing confidence of authenticity by using two or more factors to achieve authentication. The Commission is required to have a minimum two of three factors for multi-factor authentication. The multi-factor authentication three factors are a:

(1) Password or a personal identification number (PIN).
(2) PIV card.[16]
(3) Physical security token, or a biometric[17] feature such as a fingerprint or retina scan.

Homeland Security Presidential Directive-12 (HSPD-12) established control objectives for the secure and reliable identification of Federal employees and contractors. The HSPD-12 requirements, issued by President Bush in August 27, 2004, state,

> Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent

[15] Federal Information Processing Standards Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors* (FIPS 201-1), was issued by NIST on February 25, 2005, and revised in March 2006.
[16] A PIV card is defined as "[a] physical artifact (e.g., identity card, 'smart card') issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable)." Federal Information Processing Standards Publication (FIPS Pub.) 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, p. 73, Appendix F.
[17] Biometric is defined as "[a] measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an Applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics." FIPS Pub. 201-1, p. 70.

REDACTED PUBLIC VERSION

> with ongoing government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.[18]

In addition, FIPS 201-1 guidance for implementing multi-factor authentication stating,

> PIV Cards must be personalized with identity information for the individual to whom the card is issued, in order to perform identity verification both by humans and automated systems. Humans can use the physical card for visual comparisons, whereas automated systems can use the electronically stored data on the card to conduct automated identity verification.

Repeat Finding and Recommendation from Prior OIG Report

This finding is consistent with Finding 5, "Multi-Factor Authentication for System Access Has Not Been Linked to the SEC's Personal Identity Verification Program" found in OIG's *2011 FISMA Executive Summary Report*, Report No. 501, issued February 2, 2012. The finding concluded that OIT had not implemented a technical solution for linking the PIV cards to multi-factor authentication. OIT concurred with the recommendation in Report No. 501 as follows:

> ***Recommendation 13****:* The Office of Information Technology should complete its implementation of the technical solution for linking multi-factor authentication to PIV cards for system authentication and require use of the PIV cards as a second factor authentication factor by December 2012.

To date this recommendation is still open and OIT has not fully implemented it. OIT staff informed us they are working to address the recommendation. Based on our assessment, these deficiencies have not been timely mitigated and OIT still has not developed an effective technical solution to fully implement PIV cards at the SEC, as a second authentication factor for accessing the Commission's information systems. OIT's proposed technical solution to implement PIV for logical access was delayed because it did not meet the PIV program's requirements in FIPS 201-1.

In addition, OIT has not approved a formal project plan with timelines, resource allocation, and management has not approved the implementation of PIVs for logical access to SEC's systems. OIT informed us they have an informal outline

[18] *HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors,* paragraph 4.

of tasks that will be conducted. OIT delayed the project plan that was established to implement PIV for logical access because the proposed technical solution did not meet the PIV program requirements in FIPS 201-1.

As a result, the SEC is not complying with the requirements that federal employees and contractors use PIV cards to gain physical access to federally controlled facilities and logical access to federally controlled information systems. Not fully implementing a multi-factor authentication could expose the Commission to unauthorized access to its information systems.

Conclusion

This is a repeat finding that would result in a repeat recommendation from OIG's *2011 FISMA Executive Summary Report*, Report No. 501, February 2, 2012. Therefore, a new recommendation will not be made pertaining to the technical solution for linking PIV cards to a multi-factor authentication. However, we strongly encourage OIT to take steps to mitigate the deficiencies identified in OIG Report No. 501, Finding 5, recommendation 13 and this finding. OIT should fully implement this recommendation in a timely manner.

Finding 4: The SEC's Risk Management Strategy Does Not Address a Comprehensive Governance Structure or the SEC's Overall Security Risks

> The SEC's risk management strategy does not address the requirements needed for a comprehensive governance structure and organizational overall security risk management. Further, it does not address risk from a mission and business process perspective, as described in the risk management framework (RMF) identified in NIST SP 800-37, Rev. 1.[19] As a result of not updating the risk management strategy to address NIST guidelines, OIT is more likely to be exposed to higher level risks.

OIG's FISMA 2012 review found OIT's current risk management strategy still exists, but only within the context of one tier/level within the NIST RMF. The other two tiers, mission and business process level and organization level have not been fully implemented.

NIST SP 800-37, Rev. 1 was released in February 2010 and it changed the

[19] NIST SP 800-37, Rev. 1, p. 2, Section 1.2, Purpose and Applicability.

traditional C&A process into a six-step RMF. RMF's focus is a three-tiered approach to risk management that addresses risk-related concerns in organization level, the mission and business processes level, and at the information system levels.[20]

OIG's *2011 FISMA Executive Summary Report*, Report No. 501, issued in February 2012 concluded SEC risk management policy did not adhere to the requirements for a comprehensive governance structure and organization-wide risk management strategy. Hence, OIT's risk management policy did not address risk from a mission and business process perspective as described in NIST's SP 800-37, Rev. 1, released February 2010.[21]

Currently, OIT only addresses risk at the information system level. The Office of Risk Management, located in the Office of the Chief Operating Officer (OCOO), is responsible for implementing RMF at the mission and business process level and the organization level. OCOO has a newly hired risk executive who has oversight of this function. As a whole, the Commission has not fully developed a comprehensive governance structure and risk management strategy, which is necessary for facilitating organization-wide security risks at all RMF levels: organization level, the mission and business process level, and the information system level.

Although, OCOO's Office of Risk Management has not fully implemented a risk management strategy that is fully aligned with NIST SP 800-37, Rev. 1, it is making progress. Further, while a comprehensive risk management strategy has not been fully implemented, currently OIT is working on a project to develop and implement a comprehensive risk management strategy at the information system level that is scheduled to be completed by January 2014.

Additionally, we found the SEC has not updated work procedures to address the new requirement to develop a comprehensive risk management strategy. However, in compliance with NIST guidance OIT conducted risk assessments at the information system level prior to the release of NIST SP 800-37, Rev. 1.

Conclusion

As a result of not updating its risk assessment strategy to address the RMF's identified in NIST SP 800-37, Rev. 1, the Commission has not developed a comprehensive strategy to manage risk at the organization, the mission and business, and information system levels. Thus, the Commission could risk not being able to effectively identify risk and properly allocate resources to address

[20] Ibid, p. 5, Figure 2-1.
[21] Ibid.

weakness and vulnerabilities that could affect the SEC's information systems, business processes, or organization effectiveness.

Recommendation 3:

The Office of Information Technology should continue to implement the existing project for the development and implementation of a comprehensive risk management strategy in accordance with NIST Special Publication 800-37, Revision 1, *Guide for Applying Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* addressing risk at the organization level, the mission and business process level and the information system level.

Management Comments. OIT concurred with this recommendation. See Appendix VII for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Recommendation 4:

The Office of the Chief Operating Officer should ensure the Office of Risk Management coordinates with the Office of Information Technology to provide training to management throughout the Commission and educate staff on their roles and responsibilities related to operating in a three-tiered risk management framework.

Management Comments. OCOO concurred with this recommendation. See Appendix VII for management's full comments.

OIG Analysis. We are pleased that OCOO concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Finding 5: OIT Did Not Categorize the SEC's Information Systems in Accordance with NIST's Risk Management Framework

> Designated Authorizing Officials are not fully involving the Information System Owners (ISO) in system security categorization as directed by NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Lifecycle Approach, Task 1-1. Not involving the ISO in the categorization process runs the risk of them not understanding the overall context of the system and the subsequent security controls needed to properly safeguard agency information.

Our review of the security test and evaluation (ST&E) documentation for the systems in our sample universe found all nine systems had FIPS 199 system security categorizations either in the ST&E documentation or the risk assessment report. The ST&E is the security document containing the assessment criteria and the assessment results for the required security controls for each system. For the systems reviewed in our sample universe, one did not have a ST&E. Although OIT does not conduct ST&Es for contractor systems, they examine the ST&Es the contractor completes.[22]

The results of the system security categorization influences the selection the appropriate security controls for information systems, which were included in the ST&E and where applicable, the minimum assurance requirements for the system.[23] However, we found the FIPS 199 system security categorizations for the nine systems in our sample were not approved by the system owners in step one of RMF, as required by NIST SP 800-37, Rev. 1.[24] Instead, the approvals were done as part of the system security plan (SSP) review in step five of the RMF.[25] We found OIT's policy and procedures does not address the requirement for system owners to conduct system security categorization in step one of RMF. Figure 1 shown below, illustrates OIT's system security categorization approval takes place in step one versus step five of the RMF.[26]

[22] NIST SP 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations* (June 2010), p. ix, Preface.
[23] NIST SP 800-37, Rev. 1, p. 21, section 3.1 Task 1-1.
[24] Ibid.
[25] SSP - A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. NIST SP 800-18, Rev. 1, p. 39.
[26] NIST SP 800-37, Rev. 1, p. 8, Section 2.1. Figure 2-2.

Figure 1: Risk Management Framework Process Overview

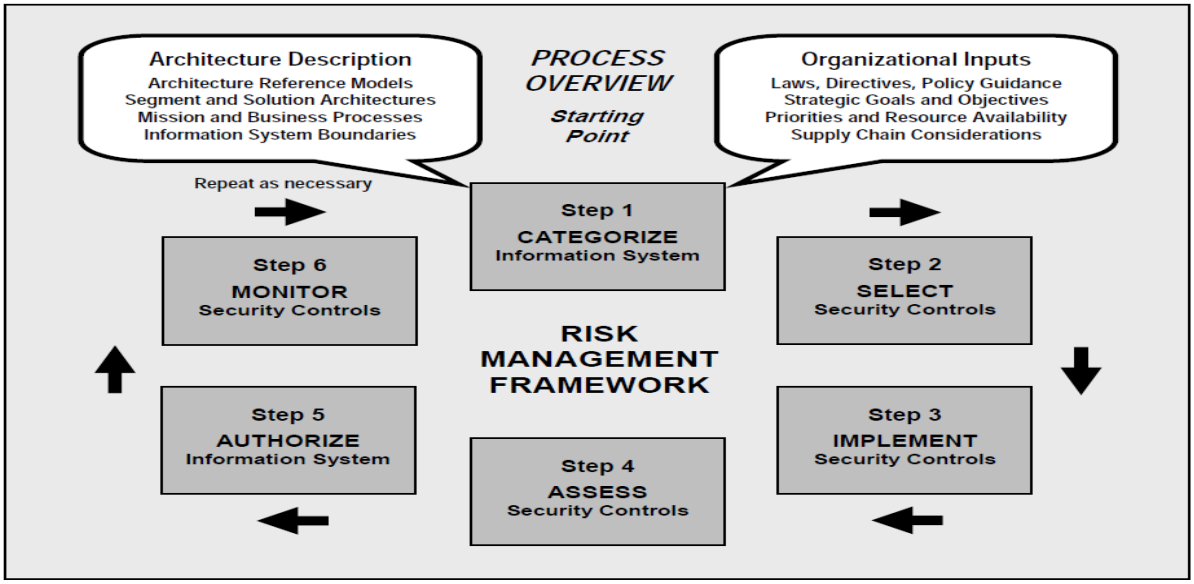


FIGURE 2-2: RISK MANAGEMENT FRAMEWORK

Source: NIST SP 800-37, Rev. 1

NIST Requirements. NIST SP 800-37, Rev. 1, Step 1, System Development Life Cycle (SDLC), states the system security categorization is to be completed in either the system development life cycle phase: initiation phase or step one of the RMF.[27] Further, NIST SP 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, states all steps in the RMF should be completed and approved before conducting a security assessment. [28]

Benchmark Results with Other Federal Agencies. Based on our benchmarking with the NCUA, FDIC, and CFTC, we learned that each agency signs and approves formal system security categorizations before selecting and assessing their respective security controls.

Conclusion

As a result of not obtaining an approved signature in step one of RMF, there is no assurance system security categorization was done prior to the security assessments being conducted. We were unable to confirm if the system categorization was completed and whether NIST and management needs were met. Without formal approval prior to conducting security assessments, the SEC runs the risk of assessing the system using the incorrect security controls based on an incorrect system security categorization.

[27] NIST SP 800-37, Rev. 1, p. 21, Section 3.1. Task 1-1.
[28] NIST SP 800-53A, Rev. 1, p. 13, Section 3.1.

Recommendation 5:

The Office of Information Technology should develop procedures to ensure Federal Information Processing Standard 199 system security categorization and to properly document the involvement of the information system owner (ISO) and the authorizing official, respectively, in step on of the risk management framework.

Management Comments. OIT concurred with this recommendation. See Appendix VII for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Recommendation 6:

The Office of Information Technology should revise its Federal Information Processing Standard 199 system security categorization form to include signature blocks for the system owner and authorizing official.

Management Comments. OIT concurred with this recommendation. See Appendix VII for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Finding 6: OIT Has Not Tailored Baseline Security Controls for Specific Systems

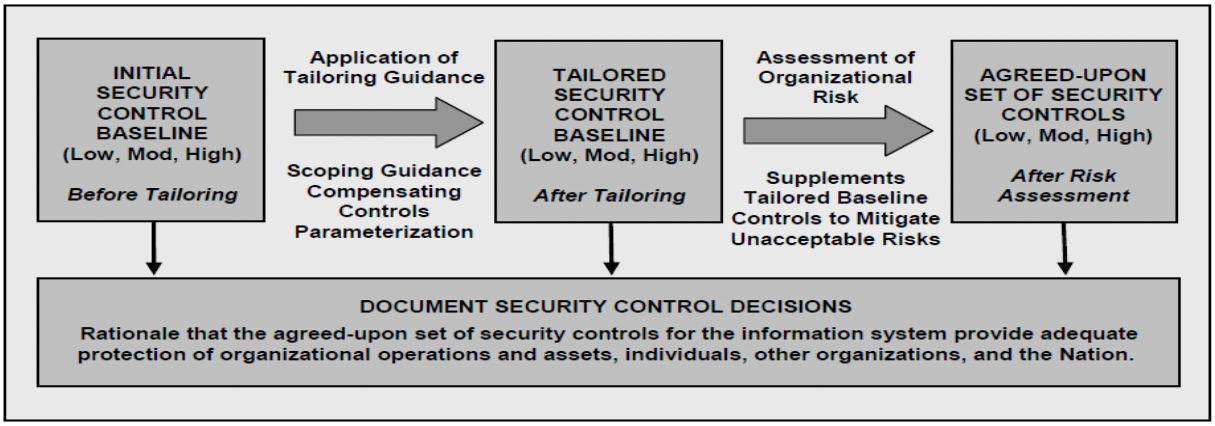
OIT has not tailored baseline security controls for specific systems. Not having a tailored control list could result in the OIT understating or overstating the security requirements for its system and critical controls for certain systems may not be identified.

Based on our review we found that OIT has not tailored its baseline security controls for specific systems that require such controls. We further found OIT did not tailor baseline security controls for the nine systems in our sample universe.

In addition, the SSPs for the systems in our sample universe did not include OIT's decision to not tailor during the security control selection process, nor its rationale for the decision. While OIT has not tailored baseline security controls, it has identified and selected a generic set of baseline security controls based on the security categorization of the system. Finally, we found OIT has not developed formal procedures or instructions for tailoring the baseline security controls in accordance with NIST SP 800-53, Rev. 3 guidelines.

Figure 2, below summarizes the security control selection process that include tailoring initial security control baselines and additional modifications that may be needed to the baseline, based on an organizational assessment of risk.[29]

Figure 2: Security Control Selection Process



Source: NIST SP 800-53, Rev. 3

Baseline Security Controls Guidance. NIST SP 800-37, Rev. 1 provides guidelines to organizations to tailor the baseline security controls by applying scoping, parameterization, and compensating control guidance. Further, NIST SP 800-37 guides organizations to supplement the tailored baseline security controls, if necessary, with additional controls and/or control enhancements to address unique organizational needs based on a risk assessment (either formal or informal) and local conditions including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances. Also, NIST SP 800-37 guides organizations to specify minimum assurance requirements, as appropriate. Further, the publication guides organizations document in the security plan, the decisions (e.g., tailoring, supplementation, etc.) taken during the security control selection process, providing a sound rationale for those decisions.[30]

[29] Ibid, p. 25, Figure 3.2.
[30] NIST SP 800-37, Rev. 1, p. 25, Section 3.2, Task 2-2, Supplemental Guidance.

REDACTED PUBLIC VERSION

NIST SP 800-37, Rev. 1, defines tailoring as the process by which a security control baseline is modified based on the application of scoping guidance; the specification of compensating security controls, if needed; and the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.[31]

OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management*, question 13 indicates agencies expectations are to use the baseline as a starting point and tailor the controls based on NIST SP 800-53, Rev. 3, eliminating or adding controls as necessary.
Per this guidance, OIT is required to tailor baseline security controls, document tailored controls in the SSP or other security documentation, and provide sound rationale for tailoring the security selection.

Feedback we received from NCUA, FDIC, and CFTC representatives found these agencies tailor their baseline security controls, and develop tailored control lists based on NIST SP 800-53, Rev. 3 guidelines, prior to conducting assessments. Also, our interview with a NIST RMF subject matter expert found that tailoring baseline security controls is a required activity in carrying out step two of RMF, security control selection and specification.

Repeat Recommendations from Prior OIG Report

This finding is consistent with Finding 3 "OIT Has Not Formally Defined a Tailored Set of Baseline Security Controls and Has Not Tailored Control Sets for Specific Systems," found in OIG's *2011 FISMA Executive Summary Report*, Report No. 501, issued February 2, 2012. The finding concluded that OIT had not developed formal procedures and instructions for tailoring its baseline security controls in accordance with the NIST SP 800-53, Rev. 3 guidelines.[32] In addition, the report found that OIT had not developed a tailored set of baseline security controls for each applicable system requiring such controls, or as defined in the SSP or other security documents. The report consisted of the three recommendations that follow, which OIT fully concurred to implement.

> ***Recommendation 5***: The Office of Information Technology should develop and implement formal policy addressing tailoring baseline security control sets.
>
> ***Recommendation 6***: The Office of Information Technology should determine whether it should perform the tailoring process at the organization level for all information systems (either as the required tailored baseline or as the starting point for system-specific

[31] Ibid, p. B-10, Appendix B, Glossary.
[32] NIST 800-53, Rev 3.

tailoring), at the individual information system level, or using a combination of organization-level and system-specific approaches.

Recommendation 7: The Office of Information Technology should tailor a baseline security controls set (with rationale) for applicable systems in accordance with the guidance provided by National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems and Organizations*.

These recommendations are still open and OIT has not implemented them. Based on our review, the issues identified in OIG Report No. 501 and discussed in this finding still exist. To fully resolve this finding, OIT must address these recommendations.

NIT's Review of OIT's Applying NIST Guidelines. Though NIST SP 800-37, Rev. 1 and NIST SP 800-53, Rev. 3 recommends tailoring security baseline control sets, OIT elected to use a generic a baseline security control set because they determined it properly addressed NIST's guidance. We were informed OIT did not tailor baseline security controls because determined tailoring is not required, and using only the generic baseline security control set (based on the system's security categorization) to further tailoring is not required.

Our review of C&A packages, SSPs, and other security documents for the nine systems in our sample universe found no indication baseline security control set was tailored in accordance with the guidance provided in NIST SP 800-37, Rev. 1 and NIST SP 800-53, Rev. 3. Further, we did not find a consensus amongst OIT management to ascertain whether OIT should perform the tailoring process (1) at the organization level for all information systems, (2) at the information system level, (3) or using a combination of both. We determined OIT's interpretation of NIST guidance does not ensure its baseline security control sets are properly tailored.

Conclusion

OIT uses a generic control set based on security categorization, which could result in under/overstating the security requirements for its systems. As a result, critical controls may not be identified for certain systems.

We identified three repeat recommendations in this finding, so no new recommendations will be made pertaining to tailoring baseline security controls. OIT should take immediate steps to mitigate the deficiencies identified in OIG

Report No. 501, for recommendations 5, 6, 7 and this finding and fully implement these recommendations in a timely manner.

Finding 7: IT Security Awareness Training Program Could be Improved by Including Role-Based Training for Staff with IT Duties and Responsibilities

> IT security awareness training program does not specify who is required to take role-based training and there is no enforcement mechanism to ensure Commission staff have taken the correct role-based training, based on duties and responsibilities. The IT security awareness training program should include role-based training for staff having IT responsibilities.

The SEC's United States (U.S.) SEC Learning Management Server application is used to administer security awareness training, identifies several IT positions, but it does not include all IT positions that have access to SEC sensitive data or materials. It also does not have a mechanism users with IT responsibilities can use to complete role-based training. The application allows employees and contractors to choose the roles that are best suited for their duties and responsibilities. In addition, the application does not prevent users from circumventing appropriate role-based training. Hence, the user does not have to select a role from the list that is provided.

OIT provides annual privacy and cyber security awareness training to all SEC employees and contractors, which requires them to access the SEC's information systems. This training includes role-based training for IT specialist, IT program manager, database administrator, network administrator, programmer, and system administrators. In 2012, the SEC reached 100 percent participation and compliance in completing the Annual Privacy and Cyber Security Awareness Training.[33] We found the IT security awareness training program does not specify who is required to take role-based training and there is no enforcement mechanism to ensure its staff have taken the correct role-based training, based on duties and responsibilities.

OIT's Implementing Instruction (II) 24-04-03-01, *IT Security Awareness Training* states, "[role-based] training is required of employees holding certain IT positions, specifically those having access to, or knowledge of SEC sensitive

[33] *The Insider*, intranet site for the SEC (August 2012).

REDACTED PUBLIC VERSION

data or materials." [34] Although, OIT has policy requiring role-based training for employees in certain IT positions, such as information security, the policy does not specifically identify the positions.

OIT's security awareness training does not include role-based training for persons with duties and responsibilities related to information security, in accordance with NIST SP 800-16.[35] An example of the roles that are linked to SEC employees responsibilities include:

- authorizing official
- information owner
- chief information officer
- chief information security officer
- information systems security officer
- risk executive
- privacy act official

Role-based training in the security awareness training course is limited to select technical IT roles (i.e. system administrator) and it does not include other positions where the staff in the position would have access to sensitive data or materials.

NIST SP 800-53, Rev. 3 provides guidance for role-based security training and determines its content based on roles and responsibilities. Specifically, Awareness and training 3 (AT-3) Security Training states,

> The organization provides role-based security related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.
>
> *Supplemental Guidance*: The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the information systems to which personnel have authorized access… [36]

II 24-04-03-01, *IT Security Awareness Training* does not define the frequency of role-based refresher training or the process for tracking role-based training.[37] The instruction states, "[t]he OIT Security Group tracks progress in and

[34] II 24-04-03-01, *IT Security Awareness Training*, (Dec. 29, 2005), p. 4, Section 5b(1).
[35] NIST SP 800-16, *Information Technology Security Training Requirements* (April 1998), p. 47, Exhibit 4.3.
[36] NIST SP 800-53, Rev. 3, p. F-22, Security Awareness and Training.
[37] II, *IT Security Awareness Training*, Policy Number 24-04-03-01 (Dec. 29, 2005), p. 4, Section 5b(1).

completion of required training courses." After conducting interviews and reviewing documentation, we found OIT does not track progress and completion of role-based training in accordance with its policy.[38]

Conclusion

We determined OIT has not clearly determined what IT staff need role-based training or information security related training for risk management. Additionally, OIT management has not defined the course or level of training that is needed for certain specific roles that are found in the U.S. SEC Learning Management Server. By not providing proper direction to IT staff with information security roles to complete role-based training, the employees may not get training that is best suited for their specific duties and responsibilities. This could result in them not receiving training needed to aid in understanding their role in implementing information security at the SEC. Thus, this could potentially lead to IT staff not fully complying with applicable NIST guidelines.

Recommendation 7:

The Office of Information Technology should review and update the existing information technology security awareness training program to:

- Include specific role-based training based on the duties and responsibilities for staff with information security roles.
- Track the progress and completion of IT staff's role-based training.

Management Comments. OIT concurred with this recommendation. See Appendix VII for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

[38] Ibid.

Finding 8: OIT Did Not Adhere to the Milestone Remediation Dates Identified to Close POA&Ms Having Lower Priority Risks

Though OIT establishes milestone remediation dates for plan of action and milestones (POA&M), it did not adhere to specific milestone remediation dates identified when closing POA&Ms having lower priority risks. As a result, POA&Ms are open for an extended period of time, which puts the Commission at risk if the weakness is not remediated in a timely manner.

Our review found that OIT does not adhere to specific milestone remediation dates for closing POA&Ms having lower priority risk. We evaluated two sets of POA&M documents as follows: (1) A GSS POA&M report, dated August 6, 2012, that identified GSS open and closed POA&Ms from June 2011 to June 2012;[39] and (2) A listing of application POA&Ms that was created in [redacted][40] and covered eight major applications from June 2011 to June 2012.

Our review of POA&Ms documents found a significant number that were not remediated and exceeded the projected remediation date. OIT asserts these were all lower priority risk POA&Ms. Specifically, 99 of the 177 POA&Ms we reviewed were open. Of the 99 that were open, only one had not exceeded the projected remediation date. The remaining 98 POA&Ms had exceeded the remediation date by as much as five years. Table 1, shown below illustrates the inability to close POA&M's and remediate them by the proposed date.

Table 1: Open POA&Ms

Information Systems	Open POA&Ms	Number of POA&Ms Past Projected Remediation Date	Number of POA&Ms Not Exceeding Projected Remediation Date
Major Applications	64	63	1
General Support System	34	34	0
Total	**99**	**98**	**1**

Source: NIT Generated

[39] Team Track is an automated application used by OIT to track the GSS POA&Ms.
[40] [redacted]

REDACTED PUBLIC VERSION

Of the 99 total open POA&Ms for the SEC's information systems, 63 of 64 for major applications exceeded the projected remediation dates. We further found one POA&M was 5 years past the remediation date, one was 4 years past the remediation date, one was 3 years past the remediation date, 39 were 2 years past the remediation date, and 21 were one year past the remediation date. Our review of the 34 open POA&Ms for GSS found they all exceeded the projected remediation date. Our review of the POA&Ms that was not remediated is detailed in Appendix VI.

Based on the nine systems in our sample we found four had POA&Ms that exceeded the proposed remediation dates. Table 2 below, identifies the four systems having proposed remediation dates that exceeded more than a year.

Table 2: Sample POA&Ms

System Acronym	POA&M ID	POA&M Title	Remediation Start Date	Projected Remediation Date	Status as of 10/9/2012
[redacted]	[redacted]	[redacted]	09/1/2010	02/28/2011	Open
[redacted]	[redacted]	[redacted]	04/14/2010	09/30/2010	Open
[redacted]	[redacted]	[redacted]	12/22/2008	08/31/2009	Open
[redacted]	[redacted]	[redacted]	12/15/2011	Last Updated 01/03/2012+	Open

Source: NIT Generated

While we found that OIT has not achieved the proposed remediation dates, OIT meets weekly and more frequently if needed to review POA&Ms and update the status or progress on outstanding POA&Ms. OIT indicated POA&Ms are not always remediated by the proposed dates for several reasons, including but not limited to lack of resources and changing priorities. OIT informed us that it uses a risk approach when determining which POA&Ms may be delayed or do not achieve their proposed remediation dates.

Even though OIT addressed some POA&Ms by their proposed remediation dates based on risk, by not addressing POA&M in a timely manner could lead to increased risk to the Commission information systems if the POA&M is not remediated in a timely manner. For example, we found a POA&M open for two years, which could potentially create a risk to the SEC for the [redacted]

REDACTED PUBLIC VERSION

[redacted]

NIST SP 800-53, Rev. 3, security assessment and authorization CA-5, plan of action and milestones, states an organization should develop "a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and…"[42]

Recommendation 8:

The Office of Information Technology should review all plan of action and milestones (POA&M) and update its POA&M's tracking system to include future remediation dates and ensure POA&Ms are closed or mitigated to an acceptable level.

Management Comments. OIT concurred with this recommendation. See Appendix VII for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Finding 9: OIT Did Not Update its Procedures

OIT issued a new policy handbook, but did not update its procedures to ensure compliance with the new policy handbook. As a result, OIT staff could inconsistently apply informal and undocumented policies within the IT environment.

OIG's *2011 FISMA Executive Summary Report,* Report No. 501, issued February 2012, found OIT's documented FISMA policies and procedures were outdated. In August 2012, OIT issued Policy Directive CIO-PD-08 (CIO-PD-08).[43] CIO-PD-

[41] List of Application POA&Ms document created in [redacted] for the eight major applications, within the June 2011 to June 2012 time frame.
[42] NIST SP 800-53, Rev. 3, p. F-35, Security Assessment and Authorization, CA-5.
[43] Policy Directive, Office of Information Technology, CIO Policy Directive, *SEC OIT Security Policy Framework*, Policy Number CIO-PD-08 (August 7, 2012).

08 supplements existing SEC policies. In issuing CIO-PD-08, OIT is in the process of rescinding previously issued policies that cover many of the areas covered in the handbook. Below, Table 3 shows the list of Securities and Exchange Commission Regulation (SECR) OIT provided us, that we found OIT is in the process of rescinding.

Table 3: Listing of IT Related SECRs

SECR	Title
24.04	Information Technology Security Program
24-04.01	Security Policy, Program Management, and Organizational Security
24-04.02	IT Security Asset Management and FISMA Inventory Management Program
24-04.03	IT Security Human Resources Program
24-04.04	IT Security Operations and Communications Security Management Program
24-04.05	IT Security Physical and Environment Protection Plan
24-04.06	IT Security Access Management Plan
24-04.07	Information Security Incident Management
24-04.08	IT Security Activities for Information System Acquisition, Development, and Maintenance
24-04.09	IT Security Business Continuity Management Program
24-04.10	IT Security Certification and Accreditation

Source: NIT Generated.

Although OIT has now updated many of its policies, the office did not update the existing procedures for the 18 control families to ensure compliance with the new policy. In addition, OIT has not developed procedures for risk management, continuous monitoring management and information security oversight over systems operated by SEC contractors and other entities, although this was identified in OIG's *2011 FISMA Executive Summary* report as non-existent.[44] Though OIT has made progress in correcting policy deficiencies the lack of procedures could result in OIT improperly implementing informal procedures that is not consistent with management's expectations and current policy.

According to NIST SP 800-53, Rev. 3, an organization should develop, disseminate, and review/update, as frequently as the organization policy specifies, the following:

[44] The Commission is required to update procedures to reflect the agency defined frequency of three years as noted in the OIT's IT Security Compliance Program Policy, the individual policy's or procedure's defined frequency as noted in the specific policy or procedure, and current NIST guidelines.

a) A formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

b) Formal, documented procedures to facilitate the implementation of the policy and associated controls.[45]

Repeat Finding and Recommendation from Prior OIG Report

This finding is consistent with Finding 1, "OIT's FISMA Policies and Procedures Are Outdated or Nonexistent" found in OIG's *2011 FISMA Executive Summary Report*, Report No. 501, issued February 2, 2012. The finding concluded that OIT's FISMA policies and procedures were outdated and the office lacked documented procedures for risk management, continuous monitoring management, and information security oversight over systems. OIT concurred with the recommendation in Report No. 501 as follows:

> ***Recommendation 1***: The Office of Information Technology (OIT) should develop and implement a detailed plan to review and update OIT security policies and procedures and to create OIT security policies and procedures for areas that lack formal policy and procedures.

This recommendation is still open and OIT has not fully implemented it. Based on our review, the issues identified in OIG Report No. 501 and discussed in this finding still exist. To fully resolve this finding, OIT must address this recommendation.

Conclusion

We determined OIT should ensure it conducts procedure reviews and updates in accordance with organization-defined timeframes. OIT has procedures that need updating. As such, OIT staff may not properly apply OIT's policies within IT's environment and may not receive proper guidance on implementing OIT policy, current NIST guidance and OIT management's expectations for implementing controls throughout the Commission.

[45] NIST SP 800-53, Rev. 3, p. F-92, Risk Assessment (RA-1), p. F-38, Configuration Management (CM-1), p. F-61, Incident Response (IR-1), p. F-21, Awareness and Training (AT-1), p. F-32, Security Assessment and Authorization (CA-1), p. F-2, Access Control (AC-1), p. F-47, Contingency Planning (CP-1), p. F-54, Identification and Authentication (IA-1). Each of the control families defines policy and procedures in level one of the control.

This finding contains a repeat finding, so a new recommendation will be made pertaining to outdated policies and procedures. OIT should take immediate steps to mitigate the deficiencies identified in OIG Report No. 501, for recommendation 1 and this finding and fully implement the recommendation in a timely manner.

Finding 10: OIT Did Not Document its Interface Between Contractor and SEC-Operated Systems

> OIT did not document the interfaces between the contractor/external systems and SEC-operated systems in its system inventory. The absence of interface data related to systems within the system inventory may lead to confusion when making risk-based decisions for external systems.

We reviewed four inventory compliance workbook updates for the reporting system inventories as of January 27, 2012; March 16, 2012; May 11, 2012; and June 29, 2012.[46] Our review determined that interfaces between the contractor, external systems and organization-operated systems were not identified in the system inventory. We determined there should be a separate column identifying contractor interfaces within the inventory compliance workbook, but none exists. We concluded that OIT does not identify interfaces between contractor, external systems and organization-operated systems within the inventory compliance workbook. OIT's C&A coordinator acknowledged he was unaware of FISMA's requirement to identify system interfaces in the system inventory, inventory compliance workbook.

FISMA, Section 3505 Requirements. FISMA, Section 3505, requires the head of the agency to develop an inventory of major information systems including "…an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency." [47] [48] In addition, NIST SP 800-53, Rev. 3 states "[t]he organization develops and maintains an inventory of its information systems".[49]

[46] An inventory compliance workbook contains an inventory of the information systems within an agency.
[47] OMB, Memorandum A-130 Revised (OMB A-130), section 6(u), Definitions, "The term "major information system" means 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."
[48] Title III, Pub. L, No. 107-347, section 3505(c)(2).
[49] NIST 800-53, Rev. 3, p. G-3, Program Management (PM)-5.

Conclusion

Without a proper and accurate inventory compliance workbook containing all major information systems, including interfaces between SEC and all sources (internal and external), OIT cannot effectively protect the Commission's network in the event an external system is compromised. In addition, the absence of interface data related to systems within the inventory compliance workbook can lead to confusion when making risk based decisions for external systems.

Recommendation 9:

The Office of Information Technology should identify and update the systems inventory list to include interface data for external systems.

Management Comments. OIT concurred with this recommendation. See Appendix VII for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Finding 11: OIT Did Not Terminate/Deactivate Accounts for all SEC Employees/Contractors' Access to Local Area Network Access Who No Longer Worked at the SEC

OIT did not disable the network accounts for all users (SEC employees/contractors) who no longer require access or who no longer work at the SEC. As a result, some users still had access to the SEC's network, which put the Commission at a higher risk for malicious acts.

We determined OIT did not terminate or disable user accounts for users (SEC employees/contractors) who no longer required access or who no longer worked at the SEC. This occurred due to oversight or timing issues. By not disabling these accounts, unauthorized employees/contractors can have access to the SEC's network and putting the SEC at a higher risk for malicious acts. Our review of user accounts from August 1, 2012 to October 31, 2012, for 74 SEC employees and 132 SEC contractors who no longer work at the SEC found OIT

did not terminate or deactivate one SEC employee user account and nine contractor user accounts. Our review of user accounts consisted of only network access.

SEC policy requires OIT disable user accounts immediately.[50] The directive states, "When personnel are terminated from the SEC, access to SEC information and information systems will be disabled immediately following established procedures for various contingencies. SEC, upon termination of individual employment: Terminates information system access and…"[51] Further, NIST SP 800-53, Rev. 3, requires agencies disable user accounts after they separate from the agency, within the agency's defined frequency. Consistent with NIST 800-53, Rev. 3, the *SEC OIT Security Policy Framework* directive states, "...SEC manages information system accounts, including: Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; …Reviewing accounts at least annually.[52] NIST SP 800-53, Rev. 3 also requires agencies disable user accounts after they separation within the organization-defined time period of inactivity.[53]

Recommendation 10:

The Office of Information Technology should conduct a full review of all user accounts to determine if any were used after an employee or contractor either no longer required access to SEC's systems or was no longer employed by the SEC, and ensure the accounts are disabled.

Management Comments. OIT concurred with this recommendation. See Appendix VII for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

[50] Policy Directive, Office of Information Technology, CIO Policy Directive, *SEC OIT Security Policy Framework*, Policy Number CIO-PD-08 (August 7, 2012), pp. 12-13.
[51] Ibid.
[52] Policy Directive, Office of Information Technology, CIO Policy Directive, *SEC OIT Security Policy Framework*, Policy Number CIO-PD-08 (August 7, 2012), pp. 28-29.
[53] NIST SP 800-53, Rev. 3, p. F-56, IA-4, Letter e.

Recommendation 11:

The Office of Information Technology should strengthen its internal controls to ensure user accounts are properly terminated or disabled for employees or contractors who either no longer require user access or are not employed with the SEC.

Management Comments. OIT concurred with this recommendation. See Appendix VII for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation. OIG considers this recommendation resolved. However, this recommendation will remain open until documentation is provided to OIG that supports it has been fully implemented.

Abbreviations

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
C&A	Certification and Accreditation
CFTC	U.S. Commodity Futures Trading Commission
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
[redacted]	[redacted]
DAA	designated approving authority
DHS	Department of Homeland Security
DNSSEC	Domain Name Security Extension
[redacted]	[redacted]
FDIC	Federal Deposit Insurance Corporation
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GSS	General Support System
HSPD-12	Homeland Security Presidential Directive-12
[redacted]	[redacted]
II	Implementing Instruction
IPv6	Internet Protocol Version 6
IPSec	Internet Protocol Security
[redacted]	[redacted]
ISO	Information System Owners System owners and designated authorizing System owners and designated authorizing officials are not approving
IT	Information Technology
[redacted]	[redacted]
NCUA	National Credit Union Administration

NIST	National Institute of Standards and Technology
NIT	Networking Institute of Technology, Inc.
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OP	Operating Procedure
PIN	Personal Identification Number
PIV	Personal Identity Verification
PM	Program Management
POA&M	Plan of Action and Milestones
Rev.	Revision
RMF	Risk Management Framework
SEC or Commission	Securities and Exchange Commission
SECR	Securities and Exchange Commission Regulation
SDLC	System Development Life Cycle
SP	Special Publication
SSP	System Security Plan
ST&E	Security Test and Evaluation
TIC	Trusted Internet Connections
TLS	Transport Layer Security
U.S.	United States
WAP	Wireless Access Points

Scope and Methodology

The full version of this report includes information that the SEC considers to be sensitive and proprietary. To create this public version of the report, OIG redacted (blacked out) potentially sensitive, proprietary information from the report.

Scope. NIT conducted this review from June 2012 to December 2012. The scope of the review consisted of the following areas specified in OMB's fiscal year 2012 FISMA reporting instructions:

- continuous monitoring management
- configuration management
- identity and access management
- incident response and reporting
- risk management
- security training
- plan of action and milestones
- remote access management
- contingency planning
- contractor systems
- security capital planning

In addition to the security mandated requirements, NIT independently evaluated and reported on how the Commission has implemented the following security requirements:

- systems inventory and the quality of the inventory
- enterprise security architecture
- data and boundary protection
- network security protocols

The evaluation criteria for the requirements listed above was based on NIST standards and industry best practices. Appendix V shows the specific evaluation criteria used for evaluating the security requirements.

Methodology. The overall objective of the 2012 FISMA assessment was to assess the SEC's systems and provide the OIG with input to the Commission's response to Department of Homeland Security (DHS) Memorandum FISM 12-02 and *FY 2012 Inspector General Federal Information Security Management Act*

Reporting Metrics.[54] To meet this objective, we reviewed and evaluated the SEC's implementation of information security requirements and provided the OIG the results of its assessment and its recommended responses for submission to OMB through Cyberscope (OMB's online FISMA reporting system) and for compiling this report. Based on interviews conducted, documentation we reviewed, and support documentation provided by Commission staff, NIT developed its responses to the FISMA questionnaire. Using NIT's assessment and recommendations, the OIG submitted its responses to the 2012 FISMA questionnaire through Cyberscope to OMB.

We conducted a review of the SEC's information security program based on guidance issued by OMB, DHS, and NIST and completed the data collection instruments required for 2012 FISMA reporting, performed the necessary evaluation procedures to answer questions published by OMB and DHS in its reporting guidance, and compiled this executive summary report for the SEC OIG.

To complete OIG's portion of the annual FISMA questionnaire, we interviewed key OIT personnel such as the information system owners, OIT staff, and stakeholders. We further examined governing policies, procedures, and other related documentation to address the evaluation objectives.

Also, we contacted representatives from NCUA, FDIC, and CFTC regarding their FISMA related practices and procedure to comply with governing guidance such as NIST. We benchmarked the SEC's reviewed controls against those at the NCUA, FDIC, and the CFTC. Our review of policies and procedures also included discussions with SEC officials to discuss and confirm our findings.

Additionally, we reviewed OIT's C&A packages, including POA&Ms, SSPs, risk assessments, ST&Es, C&A memoranda, and applicable policies and procedures, to determine OIT's compliance with OMB, FISMA, and NIST guidelines. Finally, we reviewed documentation related to the scope of the fiscal year 2012 annual FISMA assessment. Overall, our analysis was based 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 OIT's management control structure or its internal controls. We reviewed existing controls at the Commission considered specific to the 2012 FISMA OIG questionnaire. To thoroughly understand OIT's management controls pertaining to its policies and procedures and methods of operation we relied on information

[54] U.S. Department of Homeland Security, National Cyber Security Division, Federal Network Security, *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, March 6, 2012.

requested from and supplied by OIT staff members and information from interviews with various OIT personnel.

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

Prior OIG Reports. NIT reviewed the *2011 FISMA Executive Summary,* which has thirteen recommendations.[55] OIT has implemented and closed two of these recommendations, but 11 remain open. While NIT found OIT is working on addressing the open recommendations, as noted in this report, weaknesses still exist. In addition, we reviewed the GAO 2012 Financial Audit and concurred OIT does not adequately ensure network accounts are terminated or deactivated once access is no longer required, in multiple instances.[56]

Judgmental Sampling. As required by FISMA, we conducted a limited-scope review of the Commission's information security posture. The review consisted of a review of the security assessment packages for a judgmental sample of 9 of 59 SEC systems to review its security controls, that were agreed upon between the OIT and NIT. The sample universe of information systems selected for the FY 2012 FISMA consisted of the GSS, [redacted] We based the judgmental sample on a limited-scope review of both internal and external systems found in the SEC's system inventory.

[55] OIG, *2011 FISMA Executive Summary,* Report No. 501 (Feb. 2, 2012).
[56] *Fiscal Year 2012 Agency Financial Report*, pp. 51-52, A more detailed report will be published in April 2013 report entitled "Management Report: Improvements Needed in SEC's Internal Controls and Accounting Procedures".

REDACTED PUBLIC VERSION

Criteria and Guidance

Federal Information Security Management Act of 2002, **Title III, Pub. L. No. 107-347**. Requires Federal agencies to develop, document, and implement an agency-wide program providing security for the information and information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

DHS Memorandum FISM 12-02, FY 2012 *Reporting Instructions for the Federal Information Security Management Act and Privacy Management Act*. Provides instructions to agencies for meeting fiscal year 2012 reporting requirements under FISMA.

U.S. Department of Homeland Security, National Cyber Security Division, Federal Network Security, *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*. Provides general instructions under each control area for the OIG questions for Cyberscope reporting.

NIST Special Publication 800-16, *Information Security Training Requirements*. Provides guidance for security training and implementation.

NIST Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*. Provides guidance for improving protection of information system resources.

NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*. Provides guidance related to the steps in the risk management framework addressing security control section.

NIST Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations* (companion guideline to NIST Special Publication 800-53). Covers the security control assessment and continuous monitoring steps in the risk management framework and provides guidance on the security assessment process.

NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. Provides guidance for applying the risk management framework to Federal information systems.

NIST Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations. Assist agencies in the development of a continuous monitoring strategy and the implementation of a continuous monitoring program.

NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations.

Homeland Security Presidential Directive-12 (HSPD-12*),* Policies for a Common Identification Standard for Federal Employees and Contractors. Provides guidance and details for implementing a common identification standard throughout Federal agencies.

Federal Information Processing Standard Publication 199 (FIPS 199), Standards for Security Categorization of Federal Information and Information Systems. Provides guidance on the proper categorization of an information system based on the security level of the information contained in the system.

Federal Information Processing Standard Publication 200 (FIPS 200), Minimum Security Requirements for Federal Information and Information Systems. Outlines the minimum security requirements for the security of Federal information system.

Federal Information Processing Standard Publication 201-1 (FIPS 201-1), Personal Identity Verification (PIV) of Federal Employees and Contractors. Outlines the HSPD-12 requirements.

List of Recommendations

Recommendation 1:

The Office of Information Technology should revise its information technology security assessment procedures to ensure they are consistent with its current practices and include verbiage to implement continuous monitoring and requirements for on-going assessment of a subset of critical security controls.

Recommendation 2:

The Office of Information Technology should develop and implement a continuous monitoring strategy in accordance with NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* and NIST Special Publication 800-37, Revision 1, *Guide for Applying Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*

Recommendation 3:

The Office of Information Technology should continue to implement the existing project for the development and implementation of a comprehensive risk management strategy in accordance with NIST Special Publication 800-37, Revision 1, *Guide for Applying Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* addressing risk at the organization level, the mission and business process level and the information system level.

Recommendation 4:

The Office of the Chief Operating Officer should ensure the Office of Risk Management coordinates with the Office of Information Technology to provide training to management throughout the Commission and educate staff on their roles and responsibilities related to operating in a three-tiered risk management framework.

Recommendation 5:

The Office of Information Technology should develop procedures to ensure Federal Information Processing Standard 199 system security categorization and to properly document the involvement of the information system owner (ISO) and

the authorizing official, respectively, in step on of the risk management framework.

Recommendation 6:

The Office of Information Technology should revise its Federal Information Processing Standard 199 system security categorization form to include signature blocks for the system owner and authorizing official.

Recommendation 7:

The Office of Information Technology should review and update the existing information technology security awareness training program to:

- Include specific role-based training based on the duties and responsibilities for staff with information security roles.
- Track the progress and completion of IT staff's role-based training.

Recommendation 8:

The Office of Information Technology should review all plan of action and milestones (POA&M) and update its POA&M's tracking system to include future remediation dates and ensure POA&Ms are closed or mitigated to an acceptable level.

Recommendation 9:

The Office of Information Technology should identify and update the systems inventory list to include interface data for external systems.

Recommendation 10:

The Office of Information Technology should conduct a full review of all user accounts to determine if any were used after an employee or contractor either no longer required access to SEC's systems or was no longer employed by the SEC, and ensure the accounts are disabled.

Recommendation 11:

The Office of Information Technology should strengthen its internal controls to ensure user accounts are properly terminated or disabled for employees or contractors who either no longer require user access or are not employed with the SEC.

Review of Additional Information Security Requirements

In addition to the Cyberscope requirements, we independently evaluated how the SEC implemented the following security requirements:

- systems inventory and the quality of the inventory
- enterprise security architecture
- data and boundary protection
- network security protocols

The evaluation criteria we used was based on NIST standards and industry best practices. Our evaluation criteria was selected based on the *Fiscal Year 2012 CIO FISMA Reporting Metrics,*[57] NIST SP 800-53, Rev. 3,[58] NIST SP 800-37, Rev. 1,[59] and NIST SP 800-39.[60]

Systems Inventory and the Quality of the Inventory

Background. System inventory is a basic tool used to identify, track, and monitor information systems requiring security assessments. For each system requiring a FIPS 199 analysis, a corresponding entry should exist in the system inventory list. In addition, the system inventory list should identify if the system is a GSS, major application system, cloud computing system, or externally hosted system. An important part of this process is to ensure systems are properly inventoried in accordance with the FIPS 199 system categorization.

Results. We determined the SEC has a comprehensive system inventory process and OIT issued the policy handbook, Policy Directive CIO-PD-08, SEC *OIT Security Policy Framework*, in August 2012, which addresses system inventory. However, many of the procedures are outdated and should be revised.

We found OIT tracks and maintains systems within the system inventory (compliance workbook). Systems requiring C&As are tracked on a tab in the systems inventory, "Accredited Systems."

[57] US Department Homeland Security, National Cyber Security Division, Federal Network Security (February 14, 2012). *FY 2012, Chief Information Officer, Federal Information Security Management Act, Reporting Metrics.*
[58] NIST SP 800-53, Rev. 3.
[59] NIST SP 800-37, Rev. 1.
[60] NIST SP 800-39.

We determined OIT added systems to the system inventory (compliance workbook) during the planning phase and that were removed during the retirement phase of the SDLC. Hence, OIT has a formal retirement process to remove systems from the inventory. At various points during the SDLC, items impacting the system inventory list can change, such as system categorizations, new systems, and contractor systems not in compliance with required baseline security controls, which would modify the inventory list.

An important part of this system inventory process is to ensure systems are properly inventoried in accordance with the system categorization. We found OIT reviews information categorization if a system is going through re-authorization as part of the C&A cycle or when the system goes through a major change such as personally identifiable information.

Below, Table 4 illustrates the evaluation objectives NIT used to evaluate systems inventory, the quality of inventory, and the results of our evaluation by objectives.

Table 4: Evaluation Objectives for Systems Inventory and the Quality of the Inventory

Evaluation Objectives	Results
Documented policies and procedures for systems inventory	The Office of Information Technology has policies and procedures that address systems inventory and quality of the inventory. However, the procedures are outdated and should be revised.
For each of the FIPS 199 systems categorized impact levels (H = High, M = Moderate, L = Low), What is the total number of Organization information systems by Organization component (i.e. Bureau or Sub-Department Operating Element)? How does the SEC track systems that require C&As? (Reference: CIO FISMA Metrics Section 1-2)	The Commission has one GSS and 86 major systems, and the total number of information systems is categorized by organizational component. . The Office of Information Technology tracks systems within the system inventory (compliance workbook).
For each of the FIPS 199 system categorized impact levels, what is the total number of Organization operational, and information systems using cloud services by Organization component (i.e. Bureau or Sub-Department Operating Element)? (Reference: CIO FISMA Metrics, Section 1-2)	There are two systems across the categorized impact levels that are using cloud services by the Commission. Those two systems are [redacted] Both are moderate impact systems and both are in production status at the Commission.
At what portion of the SDLC are systems added to and or removed from the system inventory list? (Reference: NIST SP 800-37, Task 1-3)	The Office of Information Technology adds information systems to the system inventory (compliance workbook)during the planning phase of the SDLC.
Are there “trip-wires” in place within the SDLC or continuous monitoring program to add, modify, or remove the system in	At various points during the SDLC, items that impact the system inventory list can

REDACTED PUBLIC VERSION

Evaluation Objectives	Results
the inventory list? (Reference: NIST SP 800-37, Task 1-3)	change, which modify the inventory.
How often the information categorization of the system is reviewed, updated, changed, etc.? Who is involved in that process? What are the circumstances that determine a change to system inventory? (Reference: NIST SP 800-37, Task 1-1)	Information categorization is only reviewed if the system is going through a re-authorization via a regular cycle or major change. The individuals involved in the process are the C&A manager, the system owner, and the systems engineer.
Is there a formal retirement process in place at the organization to remove systems from the systems inventory? (Reference: NIST SP 800-37, Task 6-7)	There is a formal retirement process in place at the Commission to remove systems from the inventory.

Source: NIT Generated

Conclusion. The SEC controls are adequate for systems inventory and the quality of the inventory. There were no findings related to systems inventory.

Enterprise Security Architecture

Background. "The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This also embeds into the enterprise architecture, an integral security architecture consistent with organizational risk management and information security strategies. Security requirements and control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures."[61]

NIST SP 800-53 provides the following guidance pertaining to enterprise security architecture:

> **Control—Program Management**: PM-7 Enterprise Architecture [62]

Results. NIT determined the SEC has an established enterprise security architecture program. OIT issued the handbook, Policy Directive CIO-PD-08, *SEC OIT Security Policy Framework*, in August 2012, which addresses

[61] NIST SP 800-53, Rev. 3, p. G-4
[62] Ibid.

enterprise security architecture. However, our review found the documented enterprise security architecture procedures are outdated based on the SEC's defined three-year frequency found in the OIT's IT Security Compliance Program Policy. Also, our determination was based on OIT's procedures that define frequency as noted in the specific procedure.

NIT determined the SEC's enterprise architecture strategic plan aligns with the Federal approach related to enterprise architecture. OIT identifies strategic elements supporting the enterprise architecture at the SEC. We also determined that the OIT's security and privacy efforts are integrated into the enterprise architecture plan.

Shown below is Table 5, which contains the evaluation objectives we used to evaluate enterprise security architecture and the results by evaluation objective.

Table 5: Evaluation Objectives for Enterprise Security Architecture

Evaluation Objectives	Results
Does the agency enterprise architecture (EA) policy and procedures address security and privacy requirements?(Reference: NIST SP 800-53, Rev. 3, PM-7)	The Office of Information Technology has policies and procedures that address enterprise security architecture. However, the procedures are outdated and should be revised.
Is the existing organization's enterprise architecture plan in line with the Federal enterprise architecture plan? (Reference: NIST SP 800-53, Rev. 3, PM-7, NIST 800-39, Section 2.4.2)	The Commission's enterprise architecture strategic plan is in line with the Federal approach to enterprise architecture.
Does the agency address security and privacy requirements in the context of the mission and business processes as part of the enterprise architecture? (Reference: NIST SP 800-53, Rev. 3, PM-7, NIST 800-39, Section 2.4.2)	The Commission's enterprise architecture strategy plan addresses security and privacy as part of the enterprise architecture.
Does the agency enterprise architecture include an embedded information security architecture that describes the integration of security and privacy requirements for providing traceability from the highest-level strategic goals and objectives of organizations, through specific mission/business protection needs, to specific information security solutions provided by people, processes, and technologies?(Reference: NIST SP 800-53, Rev. 3, PM-7, NIST 800-39, Section 2.4.2)	The Office of Information Technology has a plan identifying the various elements that support enterprise architecture at the Commission.

Source: NIT Generated

Conclusion. The controls the SEC uses are adequate for enterprise security architecture. We had no findings in this area.

Data and Boundary Protection

Background. Data and boundary protection is the means used to assess the security of Federal data in various environments (i.e., mobile devices and email). The organization's information systems need to monitor and control communications at the external boundary of the system and at key internal boundaries within the system; and connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the organization security architecture.

Mobile devices and unencrypted e-mail are a primary source of loss for sensitive data and are also an easy way to carry malware back into the intranet environment. The use of encryption of data at rest or in motion is vital to protect data's confidentiality, integrity and/or availability. NIST SP 800-53, Rev. 3 provides the following guidance pertaining to data and boundary protection:

> **Control—System and Communications Protection:** SC-7 Boundary Protection [63]

Results. NIT determined the SEC has data and boundary protection protocols in place to protect data at rest and data in transit. We further found the collection of physical and logical security controls is sufficient to protect data at rest at the Commission. Data in transit is protected using various encryption methods such as Transport Layer Security (TLS), Internet Protocol Security (IPsec), and Secure Sockets Layer (SSL), which are cryptographic protocols providing communication security over the Internet.

Further, Trusted Internet Connection (TIC) 1.0 capabilities were implemented and certified, in accordance with FISMA requirements. However, TIC 2.0 capabilities have not been implemented and there is no current requirement to implement TIC 2.0.

OIT uses [redacted] a product scanning email messages for spoofed email, to scan inbound e-mail messages and to ensure mail identified as "spoofed" is not forwarded. [64] The SEC's email systems properly implements sender verification (anti-spoofing) technologies when sending messages. OIT does not allow attachments with an executable file extension (i.e. .exe) into its mail system. Additionally, users cannot run .exe files at the SEC.

[63] NIST SP 800-53, Rev. 3, pp. F-108 – F-111.
[64] Spoofed email is email which the sender address and other parts of the email header are altered to appear as though the email originated from a different source.

NIT found OIT conducts scheduled scans for unauthorized wireless access points (WAP) connected to the SEC network at least two times per month.

Table 6 consists of the evaluation objectives NIT used to evaluate data and boundary protection, as well as the results listed by evaluation objective.

Table 6: Evaluation Objectives for Data and Boundary Protection

Evaluation Objectives	Results
How does the SEC protect data at rest? (Reference: NIST SP 800-53, Rev. 3, SC-28)	The collection of security technology that makes up the enterprise protects the data at rest.
How does the SEC protect data in transit? (Reference: NIST SP 800-53, Rev. 3, IA-2 (8))	Data in transit is protected by SSL v3 and TLS encrypted tunnels.
Does the SEC use encryption technology to protect email when sending messages to government agencies or the public? (Reference: CIO FISMA Metrics, Section 6.1)	Data in transit is protected using various encryption methods such as TLS, IPsec, and SSL, which are cryptographic protocols providing communication security over the Internet.
How does the SEC manage its PKI Certificate Authority? (Reference: CIO FISMA Metrics, Section 6.2)	PKI support is managed by a Federal or commercial shared service provider.
Which TIC 1.0 Capabilities have been implemented by SEC? (Reference: CIO FISMA Metrics, Section 7.1)	TIC 1.0 capabilities have been implemented and certified at the Commission, in accordance with FISMA requirements.
Has the SEC implemented any of the TIC 2.0 Capabilities? If so which ones? (Reference: CIO FISMA Metrics, Section 7.1)	The TIC 2.0 capabilities have not been implemented; however, as of this report, there is no current requirement to implement TIC 2.0.
Is there a formal Project Plan developed to implement TIC 2.0 Capabilities? (Reference: CIO FISMA Metrics, Section 7.1)	The TIC 2.0 capabilities have not been implemented; however, as of this report, there is no current requirement to implement TIC 2.0.
Has the SEC deployed Einstein, Einstein 2? Einstein 3? (Reference: CIO FISMA Metrics, Section 7.2)	Einstein 3 is deployed at the Commission.
What is the percentage of external network traffic to/from the SEC that passes through the TIC/MTIPS? (Reference: CIO FISMA Metrics, Section 7.3)	The percentage of external traffic to/from the TIC/MTIPS is 100%.
What types of external network traffic to/from the SEC that does not pass through the TIC? (Reference: CIO FISMA Metrics, Section 7.3)	Not applicable. See previous response above.
How many email systems are used by the SEC? What are they? (Reference: CIO FISMA Metrics, Section 7.7)	There is only one email system used by the Commission, and that is Exchange 2010.
What type of (anti-spoofing) technologies are implemented by SEC e mail systems? (Reference: CIO FISMA Metrics, Section 7.6)	The Commission uses Ironport, a product that scans email messages for spoofed email, to scan inbound e-mail messages and to ensure mail identified as “spoofed” is not forwarded.
What is the percentage of SEC email systems that	The percentage of email systems

Evaluation Objectives	Results
implement sender verification (anti-spoofing) technologies when sending messages? (Reference: CIO FISMA Metrics, Section 7.6)	that implement sender verification (anti-spoofing) is 100%.
How does the SEC email system implement sender verification (anti-spoofing) technologies? (Reference: CIO FISMA Metrics, Section 7.6)	All of the Commission's email systems implement sender verification (anti-spoofing) technologies when sending messages.
Does the SEC have the capability to check incoming email traffic where the link/attachment is executed/opened in a sandbox/virtual environment in-line to ascertain whether or not it is malicious, and quarantined as appropriate, before it can be opened by the recipient? (Reference: CIO FISMA Metrics, Section 7.7)	The Commission does not allow attachments with an executable file extension (i.e. .exe) into the mail system. Additionally, users cannot run .exe files at the Commission.
Does the SEC conduct scheduled scans for unauthorized wireless access points (WAP) connected to an SEC network? What tool is used? How frequently? (Reference: CIO FISMA Metrics, Section 7.8)	The Office of Information Technology conducts scheduled scans for unauthorized wireless access points (WAP) connected to the SEC network.
What is the percentage of hardware assets which are in facilities where WAP scans are conducted? (Reference: CIO FISMA Metrics, Section 7.8)	One hundred percent of the hardware assets are included in those scans.
What network boundary devices are assessed by an automated capability to ensure that they continue to be adequately free of vulnerabilities and are adequately configured as intended, such as to adequately protect security? (Reference: CIO FISMA Metrics, Section 7.12)	The Office of Information Technology conducts scheduled scans for unauthorized WAP connected to the SEC network at least two times per month.

Source: NIT Generated

Conclusion. The controls in place at the Commission are adequate for data and boundary protection, and there were no findings related to data and boundary protection.

Network Security Protocols

Background. Network security protocols should be in place at the organization establishing usage restrictions and implementation guidance for Internet access. The need for security and privacy has led to several security protocols and standards. Domain Name System Security Extension (DNSSEC) is used at the Federal level.

Results. NIT found the OIT uses DNSSEC to prevent the pirating of government domain names. We determined OIT is capable of using Internet Protocol Version 6 (IPv6); however, there are no requirements for the office to implement IPv6. OIT is capable and ready to upgrade to IPv6 by fiscal year 2014, and is using the Department of Homeland Security (DHS) tool to inspect for DNSSEC and IPv6

compliance. Finally, OIT has taken steps to ensure DNSSEC certificates do not expire.

Table 7, shown below, contains the evaluation objectives NIT used to evaluate network security protocols and our results are listed by the evaluation's objective.

Table 7: Evaluation Objectives for Network Security Protocols

Evaluation Objectives	Results
Does the SEC use the Domain Name System Security Extension (DNSSEC) at the Federal level to prevent the pirating of government domain names? (Reference: CIO FISMA Metrics, Section 11.1a)	The Commission uses DNSSEC to prevent the pirating of government domain names.
Has the SEC upgraded public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) to operationally use native IPv6 by the end of FY 2012? (Reference: CIO FISMA Metrics, Section 11.1)	The Commission is capable of using [redacted] however, as of this report, there is no current requirement to implement [redacted]
Is there a plan in place to upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014?(Reference: CIO FISMA Metrics, Section 11.2)	The Commission is capable and ready to upgrade to IPv6 by fiscal year 2014.
Does the SEC use any of the tools offered by DHS/NPPD/NCSD/FNS to enable organizations to inspect for DNSSEC and IPv6 compliance? If so which tools? (Reference: CIO FISMA Metrics, Section 11 (FY 2012 target))	The Commission is using a DHS tool inspecting for DNSSEC and IPv6 compliance.
What steps are taken by SEC to ensure that DNSSEC certificates do not expire if not updated by the owning Organization? (Reference: CIO FISMA Metrics, Section 11 (FY 2012 target))	The Commission has steps to ensure the DNSSEC certificates do not expire.

Source: NIT Generated

Conclusion. The controls in place at the Commission are adequate for network security protocols, and there were no findings.

POA&Ms and Remediation Dates

Table 8: POA&Ms and Remediation Dates

System Name	POA&M Document Reviewed	No. of POA&Ms	No. of Open POA&Ms	Up-to-Date		Comments	No. of Years Past Projected Remediation Date
				Y	N		
[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]

REDACTED PUBLIC VERSION

System Name	POA&M Document Reviewed	No. of POA&Ms	No. of Open POA&Ms	Up-to-Date		Comments	No. of Years Past Projected Remediation Date
				Y	N		

Source: NIT Generated

MEMORANDUM

March 26, 2013

To: Jacqueline Wilson, Assistant Inspector General for Audits, Office of Inspector General

From: Jeffery Heslop, Chief Operating Officer 3/26/13
Pamela C Dyson for:
Thomas A. Bayer[1], Chief Information Officer, Office of Information Technology

Subject: Management Response, *2012 FISMA Executive Summary*, Report No. 512

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 revise its information technology security assessment procedures are consistent with its current practices and include verbiage to implement continuous monitoring and requirements for on-going assessment of a subset of critical security controls."

Management Response: OIT concurs with the recommendation. OIT Security is currently updating its policies and procedures to include verbiage to directly address the continuous monitoring program.

Recommendation 2: "The Office of Information Technology should develop and implement a continuous monitoring strategy in accordance with NIST publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* and NIST Publication 800-37, Revision 1, *Guide for Applying Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*."

Management Response: OIT concurs with the recommendation.

Recommendation 3: "The Office of Information Technology should continue to implement the existing project for the development and implementation of a comprehensive risk management strategy in accordance with NIST Special Publication 800-37, revision 1, *Guide for Applying Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*,

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

REDACTED PUBLIC VERSION

addressing risk at the organization level, the mission and business process level and the information system level."

Management Response: OIT concurs with the recommendation and is in the final stages of the existing project.

Recommendation 4: "The Office of the Chief Operating Officer should ensure the Office of Risk Management coordinates with the Office of Information Technology to provide training to management throughout the Commission and educate staff on their roles and responsibilities related to operating in a three-tiered risk management framework."

Management Response: OCOO concurs with the recommendation. OCOO Operational Risk Management is currently coordinating with the Office of Information Technology to update policies and will coordinate to provide training to management throughout the Commission and educate staff on their roles and responsibilities related to operating in a three-tiered risk management framework.

Recommendation 5: "The Office of Information Technology should develop procedures to ensure FIPS 199 system security categorization requirements and to properly document the involvement of the information system owner (ISO) and the authorizing official, respectively, in step one of the risk management framework."

Management Response: OIT concurs with the recommendation and will take steps to ensure the participation of the ISO in the categorization process, as well as documenting their involvement.

Recommendation 6: "The Office of Information Technology should revise its FIPS 199 system security categorization form to include signature blocks for the system owner and authorizing official."

Management Response: OIT concurs with the recommendation.

Recommendation 7: "The Office of Information Technology should review and update the existing information technology security awareness training program to:

- Include specific role-based training based on the duties and responsibilities for staff with information security roles.
- Track the progress and completion of IT staff's role-based training."

Management Response: OIT concurs with the recommendation.

Recommendation 8: "The Office of Information Technology should review all plan of action and milestones (POA&M) and update its POA&M's tracking system to include future remediation dates and ensure POA&Ms are closed or mitigated to an acceptable level."

Management Response: OIT concurs with the recommendation.

Recommendation 9: "The Office of Information Technology should identify and update the systems inventory list to include interface data for external systems."

Management Response: OIT concurs with the recommendation and will ensure interface data for external systems is recorded explicitly in the systems inventory.

Recommendation 10: "The Office of Information technology should conduct a full review of all user system accounts and disable or delete those that no longer require access."

Management Response: OIT concurs with the recommendation.

Recommendation 11: "The Office of Information Technology should strengthen its internal controls to ensure user accounts are properly terminated or disabled for employees or contractors who either no longer require user access or are not employed with the SEC."

Management Response: OIT concurs with the recommendation.

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.

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

Audit Requests and Ideas

The Office of Inspector General welcomes your input. If you would like to request an audit in the future or have an audit idea, please contact us at:

U.S. Securities and Exchange Commission
Office of Inspector General
Attn: Assistant Inspector General, Audits (Audit Request/Idea)
100 F Street, N.E.
Washington D.C. 20549-2736

Tel. #: 202-551-6061
Fax #: 202-772-9265
Email: oig@sec.gov

Hotline

To report fraud, waste, abuse, and mismanagement at SEC, contact the Office of Inspector General at:

Phone: 877.442.0854

Web-Based Hotline Complaint Form:
www.reportlineweb.com/sec_oig