U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

2011 Annual FISMA Executive Summary Report

February 2, 2012
Report No. 501

Assessment and Review Conducted by Networking Institute of Technology, Inc.

REDACTED PUBLIC VERSION

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

February 2, 2012

To: Thomas Bayer, Chief Information Officer, Office of Information Technology

From: Jacqueline Wilson FOR Noelle Maloney, Acting Inspector General, Office of Inspector General (OIG)

Subject: *2011 Annual FISMA Executive Summary Report*, Report 501

This memorandum transmits the U.S. Securities and Exchange Commission, OIG's final report detailing the results on our 2011 Federal Information Security Management Act of 2002 review.

The final report contains 13 recommendations which, if fully implemented, should strengthen the SEC's controls over information security. The Office of Information Technology (OIT) concurred with all of the report recommendations. OIT's written response to the report is included in the appendices.

Within the next 45 days, please provide the OIG with a written corrective action plan that is designed to address the report's agreed-upon 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 each recommendation.

Should you have any questions regarding this report, please do not hesitate to contact me or Jacqueline Wilson, Assistant Inspector General for Audits, at ext. 1-6326. We appreciate the courtesy and cooperation that you and your staff extended to our staff and contractors during this review.

Attachment

cc: James R. Burns, Deputy Chief of Staff, Office of the Chairman
Luis A. Aguilar, Commissioner
Troy A. Paredes, Commissioner
Elisse B. Walter, Commissioner
Daniel Gallagher, Commissioner
Jeff Heslop, Chief Operating Officer, Office of Chief of Operations
Todd Scharf, Chief Information Security Officer, Office of Information Technology

2011 Annual FISMA Executive Summary Report

Executive Summary

In June 2011, the U.S. Securities and Exchange Commission (SEC or Commission) Office of Inspector General (OIG) contracted with Networking Institute of Technology, Inc. (NIT) to assist with the completion and coordination of the OIG's response to Office of Management and Budget (OMB) Memorandum M-11-33*, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management Act* (OMB M-11-33).[1] This memorandum provides instructions for meeting the fiscal year 2011 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA).[2]

NIT began work on this project in June 2011. NIT's task included reviewing and evaluating the major components for FISMA 2011 in order to provide its recommended responses to OMB through Cyberscope (OMB's online FISMA reporting system). Further, NIT's task was to compile an Executive Summary Report that communicates the Inspector General's response to the fiscal year 2011 FISMA submission. NIT's review process included interviewing key SEC Office of Information Technology (OIT) personnel, and examining policies, procedures and other related documentation. Based on NIT's evaluation and recommendations, the OIG submitted its responses to the fiscal year 2011 FISMA submission. In addition, during the course of the review, NIT identified the following areas requiring improvement: OIT policies and procedures are outdated or nonexistent; OIT risk assessment policy does not address risk from a mission and business process perspective or the SEC's overall organizational risk strategy; a tailored set of baseline security controls has not been formally defined and control sets have not been tailored for the specific systems; OIT has not conducted configuration compliance scans and has no defined process for remediating compliance scan results in a timely manner; and multi-factor authentication for system access has not been linked to the Commission's Personal Identity Verification (PIV) Program.

Background. FISMA was enacted in 2002 as *Title III of the E-Government Act of 2002*. The purpose of this law is to recognize the importance of information security to the economic and national security interests of the United States. The law emphasizes the need for organizations to develop, document, and implement

[1] OMB, Memorandum M-11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Privacy Management Act (Sept. 14, 2011), http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf.
[2] Title III, Pub. L. No. 107-347, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.

organization-wide programs that provide security for the information systems that support the organization's operations and assets, as well as information systems that are provided or managed by other agencies, contractors, or other sources. FISMA provides the framework for securing the federal government's information technology 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 OMB. For fiscal year 2011, OMB M-11-33 provides instructions to heads of executive departments and agencies for meeting the fiscal year 2011 reporting requirements. OMB uses the information collected from the executive departments and agencies to:

(1) help evaluate agency-specific and government-wide information security and privacy program performance,
(2) develop its annual security report to Congress,
(3) assist in improving and maintaining adequate agency performance, and
(4) assist in developing the E-Government Scorecard under the President's Management Agenda.

Over the last year, OIT experienced major changes in its leadership, including a new CIO appointed in October 2010, a major reorganization, changes in senior OIT staff, and a new contractor brought in to oversee the SEC's daily OIT function.[3]

Objectives. The overall objective of the 2011 FISMA assessment was to assess the SEC's systems and provide the OIG with input to the Commission's response to OMB M-11-33. The assessment included a review of the Commission's information security posture, as required annually by FISMA. The 2011 FISMA assessment included the following mandated security requirements:

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

[3] The contractor is responsible for providing support services, including server and managed network services, end user computing, service desk, and pre-production services to OIT.

Results. The key findings and results for the 2011 FISMA assessment are as follows:

- OIT has formally documented information technology (IT) policies and procedures for the following FISMA controls: risk management, configuration management, incident response and reporting, security training, plan of action and milestones, remote access management, identity and access management, and contingency planning. Although OIT has documented the policies and procedures for the areas previously identified and the policies and procedures are centrally located, the policies and procedures are not updated based on the agency-defined frequency of three years as noted in OIT's IT Security Compliance Program Policy[4] or based on the individual policy's or procedure's defined frequency as specified in the policy or procedure. Additionally, OIT does not have documented procedures for risk management. Further, NIT found that OIT does not have documented policies or procedures for continuous monitoring management or for contractor systems.

- The SEC has established and is maintaining a risk management program that is generally in compliance with the applicable regulatory and statutory requirements. However, the current risk management policy does not address risk from an organizational (overall) perspective or a mission and business process perspective. Additionally, a tailored set of baseline security controls is not formally defined for each system.

- The SEC has established and is maintaining a configuration management program that is generally in compliance with FISMA requirements, OMB policy, and National Institute of Standards and Technology (NIST) guidelines. However, OIT has not updated the policies and procedures for configuration management. Further, OIT has not updated the baseline for conducting configuration compliance scans to ensure that configurations are in compliance with defined baseline configurations for major IT devices. Due to the lack of an updated defined baseline configuration template, OIT has not conducted configuration compliance scans.

- OIT has established and is maintaining an incident response and reporting program that is capable of detecting, responding to, and reporting incidents. Further, the SEC responds to and resolves incidents in a timely manner, is capable of tracking and managing risks, and is capable of correlating incidents.

[4] Operating Directive, IT Security Compliance Program, Policy Number OD24-04-10 (June 9, 2011), p. 7, section 5, No.12.

- Security training is provided to SEC personnel, including employees, contractors, and other agency users. In addition, the Commission has specialized training modules based on IT security roles and responsibilities.

- OIT is effectively tracking, prioritizing, and remediating weaknesses across the various systems, in accordance with the remediation dates stated in its Plan of Action and Milestones documentation.

- The SEC has established and is maintaining a remote access program for authorizing, monitoring, and controlling the following methods of remote access: [redacted]. The Commission's remote access infrastructure is located in a secure demilitarized zone.[9] Users must first be authenticated for remote access.

- OIT has established and is maintaining an identity and access management program that is generally consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices. However, the SEC does not use multi-factor authentication that is linked to a PIV card, as required by Homeland Security Presidential Directive-12 (HSPD-12)[10] and in accordance with NIST recommendations.

- The SEC has established and is maintaining an enterprise-wide continuous monitoring program that assesses the security state of information systems to include vulnerability scanning, patch management, and ongoing assessment of security controls.

- The SEC has established and is maintaining an enterprise-wide business continuity/disaster recovery program that is generally consistent with the applicable regulatory and statutory requirements. Disaster recovery plans are in place and can be implemented when necessary. Further, OIT performs annual contingency plan testing for major applications.

[redacted] is a [redacted] such as [redacted] o provide [redacted]

[9] A demilitarized zone is a firewall configuration that adds an extra layer of security for information systems.
[10] Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and Contractors* (July 1, 2011), http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm.

- The SEC has established and is generally maintaining a program to oversee systems operated on its behalf by contractors or other entities, including agency systems and services residing in the public cloud. Further, OIT consistently ensures that security controls of contractor systems are effectively implemented and comply with federal and agency guidelines.

- A security capital and planning program for information security has been established and is maintained at the SEC.

Summary of Recommendations. The report contains the following 13 recommendations:

(1) 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 policies and procedures.

(2) OIT should develop a comprehensive risk management strategy in accordance with National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* that will ensure management of system-related security risks is consistent with the Commission's mission/business objectives and overall risk strategy.

(3) OIT should update its current risk management policy to include language regarding developing a comprehensive governance structure and ensure management of system-related security risks is consistent with the Commission's mission/business objectives and overall risk strategy.

(4) OIT should develop and implement a formal risk management procedure that identifies an acceptable process for evaluating system risk and is consistent with the Commission's mission/business objectives and overall risk strategy.

(5) OIT should develop and implement formal policy that addresses tailoring baseline security control sets.

(6) OIT 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 tailoring), at the individual information

system level, or using a combination of organization-level and system-specific approaches.

(7) OIT 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*.

(8) OIT should review and update its configuration management policy to ensure that it complies with the requirements of the Federal Information Security Management Act and with the guidelines specified in National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems and Organizations,* as well as with its internal requirements.

(9) OIT should review and document its current standard baseline configuration, including identification of approved deviations and exceptions to the standard.

(10) OIT should conduct compliance scans of its information technology devices, according to the organizationally defined frequency in the policy and procedures, to ensure that all devices are configured as required by OIT's configuration management policy and procedures.

(11) OIT should update its policy and include language indicating that deviations from the baseline configurations that are identified and documented as a result of the configuration compliance scans are properly remediated in a timely manner.

(12) OIT should provide a new date to the Office of Management and Budget for implementing the technical solution for linking multi-factor authentication to the Personal Identity Verification (PIV) cards for system authentication.

(13) OIT 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 authentication factor by December 2012.

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

TABLE OF CONTENTS

Appendices

Figures

Background and Objectives

Background

In June 2011, the U.S. Securities and Exchange Commission (SEC or Commission) Office of Inspector General (OIG) contracted with Networking Institute of Technology, Inc. (NIT) to assist with completing and coordinating the OIG's response to Office of Management and Budget (OMB) Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (OMB M-11-33).[11]

The Federal Information Security Management Act of 2002 (FISMA)[12] 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 security for the information systems that support its operations and assets. All agencies must implement the requirements of FISMA and report annually to OMB, using OMB-issued reporting instructions, on the effectiveness of their information security and privacy programs. OMB uses the information to help evaluate agency-specific and government-wide information security and privacy program performance, develop its annual security report to Congress, help improve and maintain adequate agency performance, and develop the E-Government Scorecard under the President's Management Agenda.

OMB M-11-33 provides instructions to heads of executive departments and agencies for meeting the fiscal year 2011 reporting requirements. It also requires Inspectors General to independently evaluate and report how their department's or agency's chief information officer (CIO), senior agency official for privacy, and program officials implemented information security requirements related to risk management, configuration management, incident response and reporting, security training, plan of action and milestones, remote access management, identity and access management, continuous monitoring management, contingency planning, oversight of contractor systems, and security capital planning.

NIT began work on this project in June 2011. NIT reviewed and evaluated the Commission'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. NIT's responses are based on information provided

[11] OMB, Memorandum M-11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Privacy Management (Sept. 14, 2011), http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf.
[12] Title III, Pub. L. No. 107-347, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.

by Commission staff and obtained through interviews and review of documentation. Using NIT's assessment and recommendations, the OIG has submitted its responses to the 2011 FISMA questionnaire through Cyberscope to OMB.

Objectives

The overall objective of the 2011 FISMA assessment was to review the SEC's systems and provide the OIG with input to the Commission's response to OMB M-11-33. The assessment included a review of the Commission's information security posture, as required annually by FISMA. The 2011 FISMA assessment addressed the following security requirements:

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

Findings and Recommendations

Finding 1: OIT's FISMA Policies and Procedures Are Outdated or Nonexistent

> OIT's documented FISMA policies and procedures are outdated. In addition, OIT lacks documented procedures for risk management, continuous monitoring management, and information security oversight over systems operated by SEC contractors and other entities.

NIT found that OIT has formally documented IT policies and procedures for the following FISMA control areas: risk management, configuration management, incident response and reporting, security training, plan of action and milestones (POA&M), remote access management, identity and access management, and contingency planning. These policies are centrally accessible via the SEC's Intranet site, in OIT's policy library.[13]

NIT found, however, that these policies and procedures have not been reviewed and updated either within the timeframe specified in the policy or procedure itself or in accordance with the requirements of Operating Directive [redacted] which states that OIT policies and procedures are to be evaluated every three years. In addition, OIT did not maintain the policies and procedures consistent with the recommendations of the National Institute of Standards and Technology (NIST), as set forth in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* (NIST SP 800-53).[15] According to NIST SP 800-53, an organization should develop, disseminate, and review/update, as frequently as organization policy specifies, the following:

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

[13] OIT Policy Library, [redacted]
[14] Operating Directive, [redacted]
NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organization*, (August 2009), http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

b) Formal, documented procedures to facilitate the implementation of the [ ] policy and associated [ ] controls.[16]

As a consequence, staff may use inconsistent, informal, undocumented policies and procedures.

Additionally, NIT found that OIT does not have documented procedures for risk management or documented policies or procedures for continuous monitoring management or information security oversight of systems operated on the Commission's behalf by contractors or other entities (commonly referred to as contractor systems).

Our review of OIT's policy library found 45 OIT policies and procedures that were past due for updating. Of these, 24 are required to be updated annually, as specified in the policy or procedure, but 2 are eight years overdue for updates, 1 is seven years overdue for update, 7 are five years overdue for updates, 9 are four years overdue for updates, 4 are three years overdue for updates, and 1 is two years overdue for an update. The other 21 policies and procedures are required to be updated every three years in accordance with the IT Security Compliance Program policy, but 3 are six years overdue for updates, 7 are three years overdue for updates, 10 are two years overdue for updates, and 1 is one year overdue for an update. Appendix VI lists the specific OIT policies and procedures past due for updates.

OIT acknowledges that a significant number of OIT policies and procedures have not been reviewed and updated in accordance with the organization-defined frequency or the frequency specified in the individual policy or procedure. OIT has recently purchased a software tool, Archer, to help it manage and develop OIT policies and procedures. Archer centrally manages policies and procedures, maps them to objectives, and uses built-in alert notifications for reviewing policies and procedures.

Based on interviews with OIT staff and a review of the policies and procedures, NIT found that there is a lack of oversight to ensure that policy and procedure reviews and updates are conducted in accordance with the organization-defined frequencies.

Because OIT policies and procedures are not updated with the required frequency, OIT staff has not received adequate guidance to implement current NIST guidance and fulfill management's expectations for implementing controls

[16] NIST SP 800-53, Rev. 3, p. F-92, Risk Assessment, p. F-38, Configuration Management, p. F-61, Incident Response, p. F-21, Awareness and Training, p. F-32, Security Assessment and Authorization, p. F-3, Access Control, p. F-47, Contingency Planning, p. F-54, Identification and Authentication, http//csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

throughout the Commission. In addition, OIT staff may apply inconsistent, informal, undocumented policies and procedures within the IT environment.

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.

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.

Finding 2: OIT's Risk Management Policy Is Not Addressed From Mission and Business Process Perspectives or the Commission's Overall Strategy

OIT's risk management policy does not adhere to the requirements for a comprehensive governance structure and organizational overall risk management strategy. Further, it does not address risk from a mission and business process perspective, as described in NIST guidelines. As a result of not updating its risk management policy, OIT has not developed a comprehensive strategy to manage risk at the organizational or the mission and business process levels.

NIT found that OIT has a formally documented risk management policy—Implementing Instruction (II) [redacted][17]—which is accessible through the SEC's Intranet site in the OIT policy library and includes the roles and responsibilities of participants. NIT found that the policy has not been updated since 2005 and that it does not include formal risk management procedures that identify an acceptable process for evaluating risk at the organization and the mission and business process levels, as described in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (NIST SP 800-37), released in February 2010. Specifically, the OIT risk management policy

[17] II [redacted]

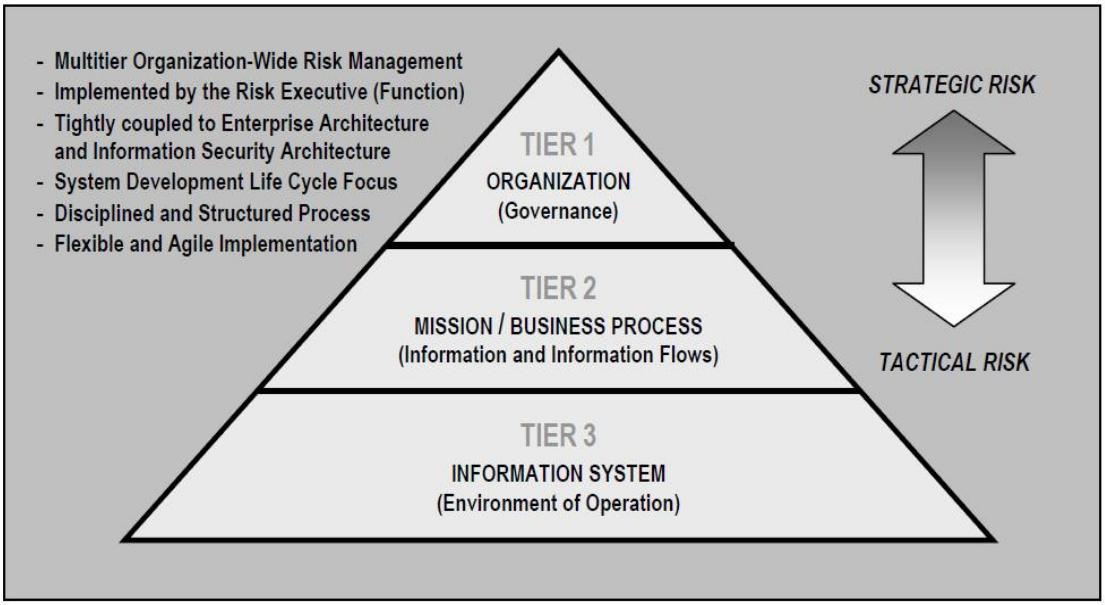
does not include the required comprehensive governance structure and organization-wide risk management strategy.

NIST SP 800-37 states the following:

> The guidelines have been developed to ensure that managing information system-related security risks is consistent with the organization's mission/business objectives and overall risk strategy established by the senior leadership through the risk executive (function).[18]

Additionally, OIT's risk management policy does not use the three-tiered approach to risk management, referred to as the Risk Management Framework (RMF), as illustrated in figure 1, below. [19]

Figure 1: Risk Management Framework



Source: NIST SP 800-37.

Tier 1 addresses risk from an organizational perspective through development of a comprehensive governance structure and organization-wide risk management strategy. Tier 2 addresses risk from a mission and business process perspective, and its activities are closely associated with enterprise architecture and are guided by Tier 1 risk decisions. Tier 3 addresses risk from an information system perspective and is guided by Tier 1 and Tier 2 risk

[18] NIST Special Publication 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 1.1, Purpose and Applicability, http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.
[19] NIST SP 800-37, Rev. 1, p. 5, section 2.1, Integrated Organization-Wide Risk Management, http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

decisions.[20] Currently, OIT is only addressing risk at the information system level.

Based on interviews with staff in the SEC's Office of Risk Management (ORM) and NIT's review of the OIT risk management policy, NIT has concluded that ORM is responsible for establishing and implementing standards to manage integrated risk management and operational readiness across the organization. ORM has developed a five-level maturity model to define the roadmap to advanced operational risk management within the SEC. The five levels are Functional Level 1, Coordinated Level 2, Standardized Level 3, Integrated Level 4, and Optimized Level 5.

Functional Level 1 is embedded in functional business units and divisions, relies on the initiative of key people, and focuses on financial and hazard risks. Risk management is not well understood at this level. At Coordinated Level 2, functional departments coordinate on high-profile risk, and risk management is driven by external compliance requirements. Standardized Level 3 focuses on management processes and controls. Risk processes are standardized in an enterprise framework communicated to staff. Integrated Level 4 includes a comprehensive risk agenda. At Optimized Level 5, formal ORM processes are embedded in strategic planning and risk management.[21]

ORM is currently working with OIT on Coordinated Level 2 of the roadmap, which incorporates the organizational level, mission and business level, and information systems level. Coordinated Level 2 addresses the following:

- Functional departments to coordinate on high-profile risk
- Formally documented controls
- Risk management driven by external compliance requirements
- Policies and procedures established by business units

Based on interviews with OIT, NIT found that OIT has begun working with ORM to develop a comprehensive risk management strategy in accordance with NIST SP 800-37, Rev 1.[22] OIT is currently conducting risk assessments at the information system level in compliance with the archived version of NIST 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,*[23] and is also in compliance with NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, released in July

[20] NIST SP 800-37, Rev. 1, p. 5, section 2.1, Integrated Organization-Wide Risk Management, http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.
[21] The definitions for the five risk levels are found in the SEC Office of Risk Management Office Stand Up file, dated September 8, 2011, p. 3.
[22] NIST SP 800-37, Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (February 2010), http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.
[23] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (May 2004), http://csrc.nist.gov/publications/PubsSPArch.html.

2002.[24] NIT did not compare OIG's risk management strategy against NIST SP 800-30, Rev. 1, *Draft Guide for Conducting Risk Assessments*,[25] because this NIST document has not been issued in final form.

Because it has not updated its risk assessment policy to address the RMF specified in NIST SP 800-37, the SEC has not developed a comprehensive strategy to manage risk at the organization level, the mission and business level, and the information system level. OIT is currently assessing risk only at the information system level and is not taking into consideration the impact of the cumulative information system risks that can be rolled up to the mission and business level and the organization level.

Recommendation 2:

The Office of Information Technology should develop a comprehensive risk management strategy in accordance with National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* that will ensure management of system-related security risks is consistent with the Commission's mission/business objectives and overall risk strategy.

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.

Recommendation 3:

The Office of Information Technology should update its risk management policy to include language regarding developing a comprehensive governance structure and ensure management of system-related security risks is consistent with the Commission's mission/business objectives and overall risk strategy.

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.

[24] NIST SP 800-30, *Risk Management Guide for Information Technology Systems* (July 2002), http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.
[25] NIST SP 800-30, Rev 1, *Draft Guide for Conducting Risk Assessments* (Sept. 19, 2011), http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-30-Rev.%201.

Recommendation 4:

The Office of Information Technology should develop and implement a formal risk management procedure that identifies an acceptable process for evaluating system risk and is consistent with the Commission's mission/business objectives and overall risk strategy.

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.

Finding 3: OIT Has Not Formally Defined a Tailored Set of Baseline Security Controls and Has Not Tailored Control Sets for Specific Systems

OIT has not developed formal policy or procedures that provide instructions for tailoring baseline security controls in accordance with NIST requirements. Further, OIT has not tailored its baseline security controls for each applicable SEC system that requires such controls.

NIT found that OIT has developed a System Security Plan (SSP) for each SEC critical system in accordance with NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems* (NIST SP 800-18).[26] The SSP is a "[f]ormal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements."[27] OIT identifies a generic set of baseline security controls in each SSP, based on the security categorization of the system, but has not taken any action to tailor the baseline security controls set consistent with the guidance in NIST SP 800-37.

NIST SP 800-37 states the following:

The security control selection process includes as appropriate:

[26] NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems,* http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf.
[27] NIST SP 800-18, p. 39, http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf.

> (i) choosing a set of baseline security controls; (ii) tailoring the baseline security controls by applying scoping, parameterization, and compensating control guidance; (iii) supplementing the tailored baseline security controls, if necessary, with additional controls …; and (iv) specifying minimum assurance requirements, as appropriate. 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.[28]

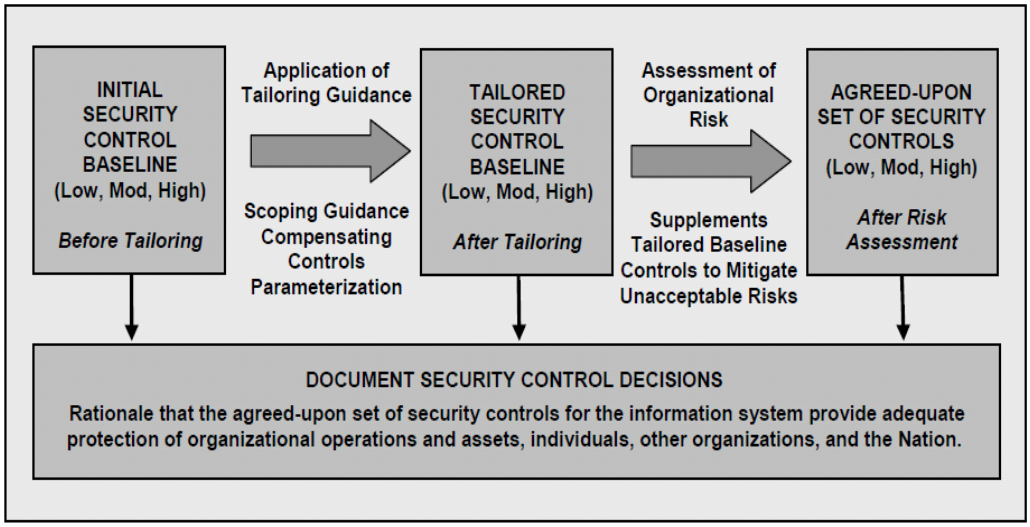
OIT has accomplished only the first of these four items. Without a formal tailored baseline security controls set, the security requirements for each system could be either understated or overstated and critical controls may not be identified.

NIT found that the baseline security controls for each system are evaluated as part of the SEC Security Test and Evaluation (ST&E). The ST&E is the security document that contains the assessment methods and the assessment results for the required security controls for each system.[29]

Through interviews with OIT staff and a review of system documentation, NIT found that OIT lacks formal policy and procedures to provide appropriate guidance to SEC IT security staff to ensure that the baseline security controls set is properly tailored in accordance with the requirements of NIST SP 800-53.[30] Figure 2, below, summarizes the process recommended by NIST for selecting security controls, including tailoring of the initial security control baseline and any additional modifications required based on an organizational assessment of risk.[31]

[28] NIST SP 800-37, Rev. 1, p. 25, http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.
[29] *See* NIST SP 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations* (June 2010), p. ix (NIST SP 800-53A), http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.
[30] NIST SP 800-53, Rev. 3, p. 25, fig. 3.2, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.
[31] NIST SP 800-53, Rev. 3, p. 25, fig. 3.2, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

Figure 2: Security Control Selection Process



Source: NIST SP 800-53.

NIT also found that OIT had not developed or defined a tailored set of baseline security controls in the SSP or other security documents for the [redacted] systems that it examined. The table 1 *SEC Systems and Date Accessed* lists the systems and the date that NIT accessed them.

Table 1: SEC Systems and Date Accessed

SEC System	Date Accessed on the SEC Intranet Site
[redacted]	August 15, 2011
[redacted]	August 29, 2011
[redacted]	September 7, 2011
[redacted]	September 7, 2011
[redacted]	August 29, 2011
[redacted]	September 7, 2011
[redacted]	September 8, 2011
[redacted]	September 8, 2011
[redacted]	September 8, 2011
[redacted]	September 8, 2011
[redacted]	September 8, 2011
[redacted]	September 8, 2011
[redacted]	September 8, 2011
[redacted]	September 8, 2011
[redacted]	September 8, 2011
[redacted]	September 8, 2011

Source: NIT Generated.

Further, NIT found that OIT mistakenly interpreted NIST SP 800-53 as requiring no tailoring of the baseline security controls set beyond selection of the appropriate set based on the system's security categorization. NIT's review of the Certification and Accreditation (C&A) packages, including the [redacted] systems' SSP and the ST&E documents, provided no indication that the baseline security controls set was tailored in accordance with the guidance in NIST SP 800-53.

OIT's use of a generic controls set based only on security categorization without additional tailoring may result in its understating or overstating the security requirements for systems. Additionally, without tailoring, OIT may fail to identify critical controls, resulting in risks to the information system, mission and business processes, and the organization.

Recommendation 5:

The Office of Information Technology should develop and implement formal policy that addresses tailoring baseline security controls sets.

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.

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

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.

Recommendation 7:

The Office of Information Technology should tailor a baseline security controls set (with rationale) for applicable systems in accordance with the guidance in 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*.

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.

Finding 4: OIT Has Not Conducted Configuration Compliance Scans and Needs a Defined Process to Address Compliance Scan Results in a Timely Manner

OIT's baseline configurations are outdated and are inconsistent with NIST guidance. OIT's current configuration management policies and procedures do not address the timely processing and remediation of deviations or exceptions from the defined configuration settings. Further, OIT has not conducted configuration compliance scans.

NIT found that the OIT has documented policies and procedures for configuration management[32] and a defined, standard baseline configuration for its major IT devices, including [redacted].[35] However, these policies and procedures and the standard baseline configuration are outdated by three or more years and are therefore inconsistent with current FISMA requirements, and NIST SP 800-53.[36]

The current baseline configurations are inconsistent with NIST guidance since they do not represent a "documented, up-to-date specification to which the information system is built." According to NIST SP 800-53, "Maintaining the baseline configuration involves creating new baselines as the information system changes over time."[37] In addition, based on interviews with OIT and examination

[32] The policies and procedures reviewed for a [redacted]
[33] Windows® Server is a brand name for a group of server operating systems released by Microsoft® Corporation.
[34] [redacted] are [redacted] that [redacted] Microsoft® Corporation.
[35] [redacted] are the [redacted] free and open [redacted]
[36] NIST SP 800-53, Rev. 3, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.
[37] NIST SP 800-53, Rev. 3, p. F-38, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

of OIT Implementing Instruction [redacted][38] NIT found that OIT's current configuration management policies and procedures do not address the timely processing and remediation of deviations or exceptions from the defined configuration settings.

As a result, OIT may be unaware of devices that do not meet its minimum configuration requirements and it may therefore be impossible for OIT to determine if the devices have been configured in accordance with approved baseline configuration. Improperly configured devices may present increased security related risks to the systems and the organization.

NIT also found that OIT has failed to conduct configuration compliance scans to ensure that current configurations comply with their defined, documented baseline configuration. OIT lacked an automated tool capable of conducting automated configuration scans, and it was not feasible for OIT to conduct manual compliance checks for its large population of devices. OIT has recently acquired an automated compliance tool, Qualys, which is capable of identifying and documenting deviations from the defined, standard baseline configuration. NIT also found that OIT has not identified, documented, and approved deviations or exceptions from its defined configuration settings.

With respect to configuration management, NIST SP 800-53 recommends that organizations develop, document, and maintain under configuration control "a current baseline of the information system." NIST SP 800-53 also states the following with respect to configuration settings:

> The organization:
>
> a. Establishes and documents 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. Implements the configuration settings;
> c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
> d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.[39]

[38] OIT Implementing Instruction [redacted]). The implementing instruction is [redacted]

[39] NIST SP 800-53, Rev. 3, p. F-42, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

Because OIT lacks up-to-date policies and procedures, its current configuration may not comply with current FISMA and NIST best practices. Also, without identifying, documenting, and approving deviations, OIT may inconsistently apply configurations to its IT devices, which could lead to weaknesses in its environment. In addition, without an automated tool, OIT may continue to fail to conduct compliance scans for its major IT devices, potentially leaving OIT unaware of devices that do not meet minimum configuration requirements. Thus, it may be impossible to determine if the devices have been properly configured in accordance with the approved baseline configurations. Improperly configured devices may present increased security related risks to the systems and the organization.

Recommendation 8:

The Office of Information Technology should review and update its configuration management policy and ensure that it complies with the Federal Information Security Management Act requirements, the guidelines specified in National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems and Organizations,* and its internal requirements.

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.

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.

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.

Recommendation 10:

The Office of Information Technology should conduct compliance scans of its information technology devices, according to the organizationally defined frequency in the policy and procedures, to ensure that all devices

are configured as required by the Office of Information Technology's configuration management policy and procedures.

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.

Recommendation 11:

The Office of Information Technology should update its policy and include language indicating that deviations from baseline configurations that are identified and documented as a result of the configuration compliance scans are properly remediated in a timely manner.

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.

Finding 5: Multi-Factor Authentication for System Access Has Not Been Linked to the SEC's Personal Identity Verification Program

OIT still has not implemented the technical solution for linking the Personal Identity Verification (PIV) cards to multi-factor authentication. As a result, the SEC continues to be noncompliant with Homeland Security Presidential Directive-12 (HSPD-12),[40] requirements. This noncompliance puts the SEC at a higher risk for unauthorized access to its information systems.

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 of two of the three factors for multi-factor authentication. The three factors of multi-factor authentication include:

[40] HSPD-12: *Policy for a Common Identification Standard for Federal Employees and Contractors,* (Aug. 27, 2004), http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm.

(1) something one knows such as a password or personal identification number (PIN),
(2) something one has such as a PIV card,[41] and
(3) something one is such as a physical security token, or a biometric[42] feature such as a fingerprint or retina scan.

Former President George W. Bush signed HSPD-12 in August 2004. It required federal agencies to have programs in place to ensure that identification issued by each agency to federal employees and contractors meets a common standard. HSPD-12 directed the Secretary of Commerce to promulgate a standard for secure and reliable forms of identification within 6 months after the date of the directive.[43] The standard, 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.[44] HSPD-12 also included the following deadlines:

- No more than four months after promulgation of the standard, heads of executive departments and agencies were to have a program in place to ensure that identification issued to employees and contractors met the standard.

- No more than eight months after promulgation of the standard, heads of executive departments and agencies were to require, to the maximum extent practicable, that employees and contractors use identification that met the standard to gain physical access to federally controlled facilities and logical access to federally controlled information systems.[45]

According to the OIG's report entitled, *The SEC's Implementation of and Compliance with HSPD-12*, Report No. 481, issued in March 2011, the SEC had missed virtually all the HSPD-12 deadlines.[46] We found that the SEC had not, to the maximum extent practical, required the use of identification by federal

[41] 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, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.
[42] 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, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.
[43] HSPD-12, para. 2, http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm.
[44] FIPS 201-1, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.
[45] HSPD-12, para. 4, http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm.
[46] OIG, *The SEC's Implementation of and Compliance with Homeland Security Presidential Directive 12*, Report No. 481 (Mar. 31, 2011), p. 3, http://www.sec-oig.gov/Reports/AuditsInspections/2011/481.pdf.

employees and contractors that met the standard in gaining physical access to federally controlled facilities and logical access to federally controlled information systems because the SEC had not completed background investigations for all employees who had more than 15 years of federal service in compliance with the prescribed deadline. As a result, in the OIG Report No. 481, we recommended to the SEC's Office of Human Resources immediately, but no later than 90 days after the issuance of the report, initiate background investigations for all current employees who did not have successfully adjudicated investigations on record.

While the Office of Human Resources concurred with the recommendation and has since initiated background investigations, as of this date, they have not completed background investigations for all employees and have not provided the OIG with a date as to when that the background investigations will be completed. It should be noted that a background investigation must be completed prior to receipt of a PIV badge.

At that time of the March 2011 report, the Office of Human Resources was responsible for oversight of the background investigations but has since transferred this responsibility to the Office of Security Services (OSS), Personnel Security Branch.

OSS's Physical Security Branch is responsible for enrolling PIV cards into its physical access control system and providing temporary SEC-issued badges while employees or contractors are awaiting receipt of their PIV cards. Physical Security has initiated the process for issuing PIV cards to all eligible employees and contractors. OIT is responsible for overseeing implementation of technological solutions for the use of PIV cards for multi-factor authentication for access to SEC information systems.

According to information obtained in interviews with OIT staff and a review of SEC information systems, OIT—more than six years after NIST's promulgation of FIPS 201-1—is still in the process of developing a technical solution for implementing PIV cards as a second authentication factor for accessing SEC information systems. According to the OIG's *2010 Annual FISMA Executive Summary Report*, OIT concurred with the OIG's recommendation that OIT complete the logical access integration of the PIV card no later than December 2011, as reported to OMB in the SEC's HSPD-12 Implementation Status Report on December 31, 2010.[47] OIT also concurred with the following recommendation in *The SEC's Implementation of and Compliance with Homeland Security Presidential Directive 12*:

[47] OIG, *2010 Annual FISMA Executive Summary Report*, Report No. 489 (Mar. 3, 2011), http://www.sec-oig.gov/Reports/AuditsInspections/2011/489.pdf.

Recommendation 16: The Office of the Executive Director should develop and implement a policy requiring the Personal Identity Verification badge to be used as a common and primary means of authentication for physical and logical access.[48]

Although OIT has concurred with the recommendations made in both reports, OIT has not completed the requirements to use the PIV card for multi-factor authentication for accessing SEC information systems.

As of the date of this report, OIT has not advised the OIG of a date for completing the implementation of PIV cards as a required second authentication factor for accessing SEC information systems.

Because it has not implemented multi-factor authentication that is linked to the PIV card program, the SEC is not in compliance with the requirements of HSPD-12[49] or with NIST SP 800-53, Identification and Authentication, IA-2.[50] Failure to implement multi-factor authentication may place the Commission at a higher risk for unauthorized access to its information systems.

Recommendation 12:

The Office of Information Technology should provide a new date to the Office of Management and Budget for implementing the technical solution for linking multifactor authentication to Personal Identity Verification cards for system authentication.

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.

Recommendation 13:

The Office of Information Technology should complete its implementation of the technical solution for linking multi-factor authentication to Personal Identity Verification (PIV) cards for system authentication and require use of the PIV cards as a second authentication factor by December 2012.

[48] OIG, *The SEC's Implementation of and Compliance with Homeland Security Presidential Directive 12*, p. 31, http://www.sec-oig.gov/Reports/AuditsInspections/2011/481.pdf.
[49] HSPD-12, para. 4, http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm.
[50] NIST SP 800-53, Rev. 3, pp. F-54 and F-55, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

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.

Abbreviations

BIA	business impact analysis
C&A	Certification and Accreditation
CIO	Chief Information Officer
CM	Configuration Management
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HSPD-12	Homeland Security Presidential Directive 12
IDS	Intrusion Detection System
II	Implementing Instruction
IPS	Intrusion Prevention System
ISA	Interconnection Security Agreement
IT	information technology
LAN	local area network
MOU	memorandum of understanding
NIST	National Institute of Standards and Technology
OSS	Office of Security Services
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PIN	personal identification number
PIV	Personal Identity Verification
POAM	Plan of Actions and Milestones
SEC or Commission	Securities and Exchange Commission
SSP	System Security Plan
ST&E	Security Test and Evaluation
US-CERT	United States Computer Emergency Readiness Team

Scope and Methodology

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

Scope. NIT conducted this review from June 2011 to October 2011. The scope of the review consisted of the following areas specified in OMB's fiscal year 2011 FISMA reporting instructions:

- risk management
- configuration management
- incident response and reporting
- security training
- evaluation of agency plan of action and milestones process
- remote access management
- identity and access management
- continuous monitoring management
- contingency planning
- agency oversight of contractor systems
- security capital planning[51]

We conducted our review at the SEC's Operations Center in Alexandria, VA and headquarters site in Washington, D.C.

Methodology. FISMA requires that federal agencies have an annual independent evaluation of their information security program and practices performed. The evaluation is to be conducted by the agency's inspector general or by an independent external auditor.[52] The overall objective of the 2011 FISMA assessment was to assess the SEC's systems and provide the OIG with input to the Commission's response to OMB M-11-33. To meet this object NIT conducted the 2011 review of the SEC's information security program based on guidance issued by OMB and NIST. NIT completed all data collection instruments required for 2011 FISMA reporting, performed the necessary evaluation procedures to answer questions to be published by OMB in its reporting guidance, and compiled this Executive Summary Report for the SEC OIG.

[51] OMB M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Privacy Management Act*, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf.
[52] Pub. L. No. 107-347, title III, § 3545(a), (b).

To complete the OIG's portion of the annual FISMA questionnaire, NIT interviewed key OIT personnel and examined policies, procedures, and other related documentation. The key personnel included system owners, OIT representatives, and OIG stakeholders. Follow-up interviews were conducted to gather additional evidence. NIT reviewed relevant documentation (such as policies, procedures, and roles and responsibilities) to address the evaluation objective. Our review of policies and procedures also included discussions with SEC officials to discuss and confirm our findings. NIT's review covered the 11 areas identified in the scope.

NIT IT security professionals reviewed OIT's C&A packages, including POA&M, SSP, Risk Assessments, ST&E, C&A memoranda, and applicable policies and procedures, to determine OIT's compliance with OMB, FISMA, and NIST guidelines. NIT also reviewed other documentation relating to the scope of the fiscal year 2011 annual FISMA assessment. Our analysis was based on information provided from various sources, interviews with key SEC OIT personnel, prior audit coverage, support documentation, and artifacts provided to NIT.

Management Controls. NIT did not assess OIT's management control structure or its internal controls because it did not pertain to the objectives of this review. NIT reviewed existing controls at the Commission considered specific to the 2011 FISMA OIG questionnaire. To thoroughly understand OIT's management controls pertaining to its policies and procedures and methods of operation, NIT relied on information requested from and supplied by OIT staff members and information from NIT interviews with various OIT personnel.

Use of Computer-Processed Data. NIT did not assess the reliability of OIT's computers because it did not pertain to our objectives for this review. Further, NIT 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 that 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 Report. NIT reviewed the *2010 FISMA Executive Summary*, which has eight recommendations.[53] OIT has implemented and closed seven of these recommendations, but one remains open. That recommendation called for OIT to complete the logical access integration of the HSPD-12 card no later than December 2011, as reported to the Office of Management and Budget on December 31, 2010.[54] NIT found that OIT is still in the process of addressing this recommendation.

[53] OIG, *2010 FISMA Executive Summary,* Report No. 489 (Mar. 3, 2011), http://www.sec-oig.gov/Reports/AuditsInspections/2011/489.pdf.
[54] *See 2010 FISMA Executive Summary,* page 9.

Judgmental Sampling. As required by FISMA, NIT conducted a limited review of the Commission's information security posture. The review consisted of NIT's reviewing the security assessment packages for a representative sample of [redacted] of approximately [redacted] SEC systems that were agreed upon between the SEC and NIT.[55]

[55] The [redacted] systems selected were the [redacted]

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 that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

OMB Memorandum 11-33, ***FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management***. Provides instructions to agencies for meeting fiscal year 2011 reporting requirements under FISMA.

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 RMF that address 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 SP 800-53). Covers the security control assessment and continuous monitoring steps in the RMF 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 RMF to federal information systems.

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 (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.

Recommendation 2:

The Office of Information Technology should develop a comprehensive risk management strategy in accordance with National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* that will ensure management of system-related security risks is consistent with the Commission's mission/business objectives and overall risk strategy.

Recommendation 3:

The Office of Information Technology should update its risk management policy to include language regarding developing a comprehensive governance structure and ensure management of system-related security risks is consistent with the Commission's mission/business objectives and overall risk strategy.

Recommendation 4:

The Office of Information Technology should develop and implement a formal risk management procedure that identifies an acceptable process for evaluating system risk is consistent with the Commission's mission/business objectives and overall risk strategy.

Recommendation 5:

The Office of Information Technology should develop and implement formal policy that addresses tailoring baseline security controls 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 tailoring), at the individual information system level, or by 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 in 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*.

Recommendation 8:

The Office of Information Technology should review and update its configuration management policy and ensure that it complies with the Federal Information Security Management Act requirements, the guidelines specified in National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems and Organizations,* and its internal requirements.

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.

Recommendation 10:

The Office of Information Technology should conduct compliance scans of its information technology devices, according to the organizationally defined frequency in the policy and procedures, to ensure that all devices are configured as required by the Office of Information Technology's configuration management policy and procedures.

Recommendation 11:

The Office of Information Technology should update its policy and include language indicating that deviations from baseline configurations that are identified and documented as a result of the configuration compliance scans are properly remediated in a timely manner.

Recommendation 12:

The Office of Information Technology should provide a new date to the Office of Management and Budget for implementing the technical solution for linking multifactor authentication to Personal Identity Verification cards for system authentication.

Recommendation 13:

The Office of Information Technology should complete its implementation of the technical solution for linking multi-factor authentication to Personal Identity Verification (PIV) cards for system authentication and require use of the PIV cards as a second authentication factor by December 2012.

OIG's Response to OMB Questionnaire

Section 1: Status of Risk Management

Background. Risk management is an essential component of a successful IT security program and should be consistent with OMB M-11-33*, FY 2011 Reporting Instructions for the Federal Information Security Management Act and the Agency Privacy Management Act,*[56] FISMA,[57] and NIST guidelines—specifically, NIST SP 800-53.[58] NIST SP 800-37[59] also provides guidance for applying the RMF to federal information systems. The principal goal of an IT security program's risk management process should be to protect the organization and its ability to perform its mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

The RMF, in accordance with NIST SP 800-37, consists of a three-tiered approach to risk management. The RMF is intended to improve information security and strengthen the risk management process. (See figure 1 in this report for a graphic summary of the RMF.) Tier 1 addresses risk from an organizational perspective through development of a comprehensive governance structure and organization-wide risk management strategy. Tier 2 addresses risk from a mission and business process perspective, and its activities are closely associated with enterprise architecture and are guided by Tier 1 risk decisions. Tier 3 addresses risk from an information system perspective and is guided by Tier 1 and Tier 2 risk decisions.[60]

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The ultimate goal is to help organizations to better manage risks throughout all levels of the organization. The objective of performing risk management is to enable the organization to accomplish its missions by better securing the IT systems that store, process, or transmit organizational information.

[56] OMB M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Privacy Management Act*, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf.
[57] FISMA, Title III, Pub. L. No. 107-347, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
[58] NIST SP 800-53, Rev. 3, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.
[59] NIST SP 800-37, Rev. 1, http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.
[60] NIST SP 800-37, Rev. 1, p. 5, http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

A risk assessment is the process in the risk management methodology that organizations use to identify the likelihood of a threat or vulnerability, the extent of the potential threat, and the risk associated with an IT system.
NIST SP 800-53 lists the following controls associated with risk assessment:

- RA-1 Risk Assessment Policy and Procedures
- RA-2 Security Categorization
- RA-3 Risk Assessment
- RA-5 Vulnerability Scanning[61]

A risk assessment helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

Response. In response to question 1 on the OMB template, based on interviews and reviews of C&A packages and other SEC documentation, NIT determined that the Commission has established and is maintaining a risk management program and that the risk management program is generally consistent with FISMA, OMB, and NIST requirements. A certification is "[a] comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system."[62] An accreditation is "[t]he official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls."[63]

In response to question 1.a(1), NIT found that OIT has a documented and centrally accessible risk management policy, II [redacted][64] but does not have formal risk management procedures. OIT's risk management policy includes the roles and responsibilities of participants.

In response to questions 1.a(2) through 1.a(4), NIT found that the current risk management policy has not been updated since December 22, 2005, and does not address risk from an organizational perspective or a mission and business process perspective, as described in NIST SP 800-37. However, the risk management policy does address risk from an information system perspective.

[61] NIST SP 800-53, Rev. 3, pp. F-92-95, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.
[62] NIST SP 800-18, Rev. 1, p. 32, http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf.
[63] NIST SP 800-18, Rev. 1, p. 31, http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf.
[64] IT [redacted] II [redacted], available in the OIT Policy Library, [redacted]

In response to question 1.a(5), NIT found that OIT categorizes information systems in accordance with government policies.

In response to questions 1.a(6) and 1.a(7), NIT found that OIT identifies a generic set of baseline controls that are evaluated as part of the ST&E process.[65] However, OIT has not developed any polices or procedures to define an approach for developing a tailored set of baseline controls for each system consistent with NIST SP 800-53.[66] In addition, OIT has not defined or implemented a process to tailor baseline security controls for each system. OIT conducts ST&Es based on the generic baseline set of security controls and not the tailored set of security controls.

In response to question 1.a(8), NIT found that OIT assesses security controls for the information systems using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

In response to questions 1.a(9) through 1.a(14), after review of the C&A documentation (including SSPs and POA&Ms) ,[67] NIT found that the Commission authorizes information systems based on the level of risk and monitors information security controls on a regular basis. The risks are appropriately communicated to SEC officials, system owners, chief information officers, senior information security officers, and other key SEC stakeholders.

Shown below, Table 2 contains OIG's response to question 1, as provided by NIT.

[65] The ST&E is the security document that contains the assessment methods and the assessment results for the required security controls for each system. NIST SP 800-53A, Rev. 1, p. ix, http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf.
[66] NIST SP 800-53, Rev. 3, pp. 16-29, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-0 1-2010.pdf.
[67] The SSP is a "[f]ormal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements." The POA&M is "[a] document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones." NIST SP 800-18, Rev. 1, p. 37.

Table 2: OIG Response to Question 1 From OMB Questionnaire

ID	Questions from OMB Questionnaire	Response
1.a	The Agency has established and is maintaining a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes.	Yes
1.a(1)	Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.	No
1.a(2)	Addresses risk from an *organization* perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev.1	No
1.a(3)	Addresses risk from a *mission and business process* perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev.1.	No
1.a(4)	Addresses risk from an *information system* perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1.	Yes
1.a(5)	Categorizes information systems in accordance with government policies.	Yes
1.a(6)	Selects an appropriately tailored set of baseline security controls.	No
1.a(7)	Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.	No
1.a(8)	Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	Yes
1.a(9)	Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.	Yes
1.a(10)	Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.	Yes
1.a(11)	Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization.	Yes
1.a(12)	Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO).	Yes
1.a(13)	Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.	Yes

Source: OMB FISMA Web Portal.

Section 2: Status of Configuration Management

Background. A configuration management program consists of the activities surrounding the maintenance of the security configuration of a system or network in order to effectively manage risk. The program consists of patch management and remediation of vulnerabilities, regular scans of the network for vulnerabilities, establishment of a standard baseline configuration, full hardware and software inventory, and a change management process.

The Federal Desktop Core Configuration (FDCC) is an OMB mandate that requires all federal agencies to standardize the configuration (baseline) of approximately 300 settings on every Windows computer, agencywide. The purpose of the OMB mandate is to secure an ever-widening array of workstations, servers, network devices, and software applications in terms of technology-specific controls. The reason for this standardization is to strengthen federal IT security by reducing opportunities for hackers to access and exploit government computer systems.

Patch management is a key component in maintaining the security posture of a system. Software vendors provide patches and updates to remediate security vulnerabilities identified in their software. These patches and updates are made available through the software vendor's website as they are released. Most vendors have a set day for releasing patches. For example, Microsoft releases patches and updates on the second Tuesday of each month. If a vulnerability is considered critical, a vendor may release patches outside of its usual cycle.

NIST SP 800-53 provides guidance to government organizations on flaw remediation, such as patching and updates, and lists the following controls associated with configuration management:

- CM-1 Configuration Management Policy and Procedures
- CM-2 Baseline Configuration
- CM-3 Configuration Change Control
- CM-4 Security Impact Analysis
- CM-5 Access Restrictions for Change
- CM-6 Configuration Settings
- CM-7 Least Functionality
- CM-8 Information System Component Inventory
- CM-9 Configuration Management Plan[68]

The NIST guidance recommends that organizations identify, report, and correct information system flaws, test software updates related to flaw remediation for

[68] NIST SP 800-53, Rev. 3, pp. F-38-46, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

effectiveness and potential side effects on organizational information systems before installation, and incorporate flaw remediation into the organizational configuration management process.

Response. In response to question 2 on the OMB template, NIT determined, based on interviews and reviews of the patching process, that the Commission has established and is maintaining a configuration management program. In addition, the SEC is maintaining a configuration management program that is generally consistent with FISMA, OMB, and NIST requirements.

In response to questions 2a(1) and 2.a(2), NIT found that OIT has a documented IT security configuration management policy, II [redacted] which indicates the policy will be reviewed and updated annually. However, NIT's review found that the policy has not been reviewed or updated since March 13, 2007. NIT also found that OIT has standard baseline configuration documents that define the baseline configuration for critical devices but that these documents have not been reviewed or updated within the past three years. Because the baseline configuration documents have not been reviewed, the documents are not in compliance with NIST guidelines.

In response to questions 2a(3) and 2.a(4), NIT found that OIT is not conducting configuration compliance scans to ensure that configurations comply with the defined baseline configurations. OIT is in the process of developing baseline compliance templates that will be used to determine compliance with baseline configurations. NIT also found that OIT does not have a formal policy that identifies the process for timely remediation of scan result deviations.

In response to questions 2a(5) through 2.a(7), NIT found that secure configuration settings are implemented and that any deviations from FDCC baseline settings were documented and reported to NIST. Also, after watching a demonstration of the patch process and reviewing provided documentation, NIT concluded that OIT is adequately applying patches in a timely and secure manner.

Shown below, Table 3 contains OIG's response to question 2, as provided by NIT.

[69] See IT [redacted] available in the OIT Policy Library.

Table 3: OIG Response to Question 2 From OMB Questionnaire

ID	Questions from OMB Questionnaire	Response
2.a	The Agency has established and is maintaining a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	Yes
2.a(1)	Documented policies and procedures for configuration management.	No
2.a(2)	Standard baseline configurations defined.	No
2.a(3)	Assessing for compliance with baseline configurations.	No
2.a(4)	Process for timely, as specified in agency policy or standards, remediation of scan result deviations.	No
2.a(5)	For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented	Yes
2.a(6)	Documented proposed or actual changes to hardware and software configurations.	Yes
2.a(7)	Process for timely and secure installation of software patches.	Yes

Source: OMB FISMA Web Portal.

Section 3: Status of Incident Response and Reporting

Background. Incident response is the documented (through policies and procedures) and organized approach to addressing and managing the aftermath of a security breach or attack, also known as an incident. Incidents may include lost or stolen assets, such as laptops and Blackberry devices, or the compromise of an organization's system resulting, for example, from unauthorized access or a computer virus. NIST SP 800-53 lists the following controls associated with incident response:

- IR-1 Incident Response Policy and Procedures
- IR-2 Incident Response Training
- IR-3 Incident Response Testing and Exercises
- IR-4 Incident Handling
- IR-5 Incident Monitoring
- IR-6 Incident Reporting
- IR-7 Incident Response Assistance
- IR-8 Incident Response Plan[70]

[70] NIST SP 800-53, Rev. 3, pp. F-61–F-65, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

The goal of incident response is to handle a situation in a way that limits damage and reduces recovery time and cost. Organizations develop an incident response plan to include policies that define, in specific terms, what constitutes an incident and to provide a step-by-step process, based on the type and severity of the incident, to be followed when an incident occurs. NIST SP 800-61, *Computer Security Incident Handling Guide,* recommends that an incident response plan address the following elements:

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization
- Metrics for measuring the incident response capability
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization[71]

In addition, organizations should have a designated computer incident response team consisting of carefully selected members that may include, in addition to security and general IT staff, representatives from legal, human resources, and public relations departments. The team's roles and responsibilities are documented, defined, and communicated thoroughly.[72]

Response. In response to question 3 on the OMB template, NIT determined, based on interviews and reviews of documentation, that the Commission has established and is maintaining an incident response and reporting program that is generally consistent with FISMA, OMB, and NIST requirements.

In response to question 3a(1), NIT found that OIT has documented policies and procedures for detecting, responding to, and reporting incidents. The policies indicate that they will be reviewed and updated annually. However, our review found that the [redacted] has not been reviewed or updated since August 9, 2007, and that the [redacted] has not been updated since March 2007. Therefore, NIT determined the documentation does not comply with NIST guidelines. In addition, neither document has not been updated in accordance with the SEC-defined frequency of three years specified in the SEC IT Security [redacted] [73]

[71] NIST SP 800-61, Rev. 1, *Computer Security Incident Handling Guide* (March 2008), pp. 2-4, http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf.
[72] NIST SP 800-61, Rev. 1, *Computer Security Incident Handling Guide* (March 2008), pp. 2-12, http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf.
[73] IT Security [redacted] available in the OIT Policy Library, [redacted]

In response to question 3.a(2), NIT reviewed incident reports and found that they contain comprehensive analysis, validation, and documentation of incidents at the SEC.

In response to question 3.a(4), NIT reviewed the [redacted] and determined that OIT specifies timeframes for reporting applicable incidents to US-CERT.[74]

In response to questions 3.a(5) and 3.a(6), NIT concluded that OIT responds to and resolves incidents in a timely manner, is capable of tracking and managing risks in a virtual/cloud environment, and is capable of correlating incidents.

Table 4 contains OIG's response to question 3, as provided by NIT.

Table 4: OIG Response to Question 3 From OMB Questionnaire

ID	Questions from OMB Questionnaire	Response
3.a	The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	Yes
3.a(1)	Documented policies and procedures for detecting, responding to and reporting incidents.	No
3.a(2)	Comprehensive analysis, validation and documentation of incidents.	Yes
3.a(3)	When applicable, reports to US-CERT within established timeframes.	Yes
3.a(4)	When applicable, reports to law enforcement within established timeframes.	Yes
3.a(5)	Responds to and resolves incidents in a timely manner, as specified in agency policy or standards, to minimize further damage.	Yes
3.a(6)	Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.	Yes
3.a(7)	Is capable of correlating incidents.	Yes

Source: OMB FISMA Web Portal.

Section 4: Status of Security Training Program

Background. NIST SP 800-16, *Information Technology Security Training Requirements: A Role and Performance-Based Model,* provides guidance for designing a role-based training program.[75]

Federal agencies and organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved understands his or her roles and

[74] See [redacted], available in the OIT Policy Library, [redacted]

[75] NIST SP 800-16, *Information Technology Security Training Requirements: A Role and Performance-Based Model*, http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.

responsibilities and is adequately trained to perform them. NIST SP 800-53 lists the following controls associated with security awareness training:

- AT-1 Security Awareness and Training Policy and Procedures
- AT-2 Security Awareness
- AT-3 Security Training
- AT-4 Security Training Records
- AT-5 Contacts with Security Groups and Associations[76]

Security awareness and training policies and procedures can be developed for the security program in general and, when required, for a particular information system.

Response. In response to question 4 on the OMB template, NIT determined, based on interviews and reviews of documentation, that the SEC has established and is maintaining a security training program that is generally consistent with FISMA, OMB, and NIST requirements.

In response to question 4.a(1), NIST found OIT has policies and procedures for security awareness training. The document containing the policies and procedures, IT Security [redacted] indicates that it will be reviewed and updated annually, but it was last updated on December 29, 2005.[77]

In response to questions 4.a(2) and 4.a(3), NIT found that the Commission has specialized training modules based on IT security roles and responsibilities.

In response to questions 4.a(4) and 4.a(5), NIT found that the Commission has conducted security awareness for its personnel, including employees, contractors, and other agency users. In addition, the identification and tracking of the status of specialized training for all personnel are formally documented.

Table 5 contains OIG's response to question 4, as provided by NIT.

[76] NIST SP 800-53, Rev. 3, pp. F-21-23, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

[77] IT Security [redacted] available in the OIT Policy Library, [redacted]

Table 5: OIG Response to Question 4 From OMB Questionnaire

ID	Questions from OMB Questionnaire	Response
4.a	The Agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	Yes
4.a(1)	Documented policies and procedures for security awareness training.	No
4.a(2)	Documented policies and procedures for specialized training for users with significant information security responsibilities.	Yes
4.a(3)	Security training content based on the organization and roles, as specified in agency policy or standards.	Yes
4.a(4)	Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other agency users) with access privileges that require security awareness training.	Yes

Source: OMB FISMA Web Portal.

Section 5: Status of POA&M Report

Background. The POA&M is a key document in a C&A package. It is used to document identified weaknesses and vulnerabilities discovered through security control assessments, security impact analyses, risk assessments, and continuous monitoring activities. A POA&M document should contain information on the system, the identified vulnerability, severity and risk level of the vulnerability, applicable control family based on NIST SP 800-53, recommended remediation and timeline, and responsible party or organization for mitigating the weakness or vulnerability. NIST SP 800-53 includes the following specific guidance related to POA&Ms:

Control—Certification and Accreditation

- CA-5 Plan of Action and Milestones

  The organization:

a. Develops 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
b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from

> security controls assessments, security impact analyses, and continuous monitoring activities.[78]

Response. In response to question 5 on the OMB template, NIT determined, based on interviews and reviews of documentation, that the SEC has established and is maintaining a POA&M management program that is generally consistent with FISMA, OMB, and NIST requirements.

In response to 5.a(1), NIT found OIT has documented policies and procedures for managing IT security weaknesses discovered during security control assessments and required remediation. OIT has developed IT Security [redacted], which addresses POA&M management and remediation. Although the policy indicates that it will be reviewed annually,[80] NIT found that it has not been reviewed since June 2005.

In response to questions 5.a(2) through 5.a(4), NIT confirmed that OIT is effectively tracking, prioritizing, and remediating weaknesses across the various systems in accordance with the remediation dates specified in the POA&M documentation.

In response to questions 5.a(5) and 5.a(6), NIT found that OIT has provided the appropriate resources for correcting the weaknesses and that the progress of the remediation is reported to the appropriate SEC officials on a regular basis.

Table 6 contains OIG's response to question 5, as provided by NIT.

[78] NIST SP 800-53, Rev. 3, pp. F-35, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.
[79] IT Security [redacted] available in the OIT Policy Library [redacted]
[80] IT Security [redacted]

Table 6: OIG Response to Question 5 From OMB Questionnaire

ID	Questions from OMB Questionnaire	Response
5.a	The Agency has established and is maintaining a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	Yes
5.a(1)	Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation.	No
5.a(2)	Tracks, prioritizes and remediates weaknesses.	Yes
5.a(3)	Ensures remediation plans are effective for correcting weaknesses.	Yes
5.a(4)	Establishes and adheres to milestone remediation dates.	Yes
5.a(5)	Ensures resources are provided for correcting weaknesses.	Yes
5.a(6)	Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly.	Yes

Source: OMB FISMA Web Portal.

Section 6: Status of Remote Access Management

Remote access is the ability to access a computer or a network from a remote location. Most commonly this type of access is used by telecommuters working from home, personnel on travel, consultants and contractors, and others who are not permanently based at a facility. NIST SP 800-53 includes the following guidance pertaining to remote access:

Control—Access Control

- AC-17 Remote Access

The organization:

a. Documents allowed methods of remote access to the information system;
b. Establishes usage restrictions and implementation guidance for each allowed remote access method;
c. Monitors for unauthorized remote access to the information system;
d. Authorizes remote access to the information system prior to connection; and

e. Enforces requirements for remote connections to the information system.[81]

Remote access is any access to an organization's information system by a user communicating through an external network (e.g., the Internet). Remote access requires strong authentication for security purposes and therefore should require multi-factor authentication. Multi-factor identification consists of a combination of a password, passcode from a secure token, a user name, and personal identification number (PIN) to establish connection to the network, followed by the user's account domain user name and password to access applications or workstations.

Response. In response to question 6 on the OMB template, NIT determined, based on interviews and reviews of documentation, that the SEC has established and is maintaining a remote access management program that is generally consistent with FISMA, OMB, and NIST requirements.

In response to question 6.a(1), NIT found that OIT has documented policies and procedures for authorizing, monitoring, and controlling the following methods of remote access: [redacted] OIT has developed policies and procedures that address remote access. However, three of the policies have not been reviewed or updated since 2002, one has not been reviewed or updated since 2005, and one has not been reviewed or updated since 2006. Therefore, NIT determined that the documents are not in full compliance with NIST guidelines.

In response to questions 6.a(2) and 6.a(3), NIT found that the Commission's remote access infrastructure is located in a secure demilitarized zone[86] and that all users must first be authenticated for remote access.

In response to questions 6.a(4) through 6.a(6), NIT found that a new user must have an OIT network account and an RSA token to use the Commission's remote access, both which must be authorized by the appropriate OIT manager for employees or by the Contracting Officer's Technical Representative for contractors. The methods used for remote access meet the encryption

[81] NIST SP 800-53, Rev. 3, p. F-14, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

[82] A [redacted] client is [redacted] the [redacted] which is a [redacted] that [redacted] such as [redacted] allows users to [redacted] from [redacted].

[84] [redacted] provides users device [redacted] for [redacted]

[85] [redacted] s the [redacted] used by the SEC. [redacted] allows [redacted]

[redacted]

[86] A demilitarized zone is firewall configuration that adds an extra layer of security for information systems.

requirements specified in NIST SP 800-63, version 1.0.2, *Electronic Authentication Guide*[87] and are properly implemented.

Shown below, Table 7 contains OIG's response to question 6, as provided by NIT.

Table 7: OIG Response to Question 6 From OMB Questionnaire

ID	Questions from OMB Questionnaire	Response
6.a	The Agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	Yes
6.a(1)	Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.	No
6.a(2)	Protects against unauthorized connections or subversion of authorized connections.	Yes
6.a(3)	Users are uniquely identified and authenticated for all access.	Yes
6.a(4)	If applicable, multi-factor authentication is required for remote access.	Yes
6.a(5)	Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.	Yes
6.a(6)	Defines and implements encryption requirements for information transmitted across public networks.	Yes
6.a(7)	Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication are required.	Yes

Source: OMB FISMA Web Portal.

Section 7: Status of Identity and Access Management

Background. Identity and access management refers to how personnel are identified and authorized across computer networks (logical access) and facilities (physical access). It covers issues such as how users are given an identity, the protection of that identity, and the technologies supporting that protection (e.g., network protocols, digital certificates, passwords). NIST SP 800-53 lists the following controls pertaining to identity and access management:

Control—Identification and Authentication

- IA-2 Identification and Authentication (Organizational Users) [88]

[87] NIST SP 800-63, version 1.0.2, *Electronic Authentication Guide* (Apr. 2006).
[88] NIST SP 800-53, Rev. 3, pp. F-54–F-55, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

Control—Access Management

- AC-2 Account Management
- AC-3 Access Enforcement
- AC-5 Separation of Duties[89]

ID badges and cardkeys are most commonly used for physical access, although biometrics may also be used.[90] Badges generally have a photograph of an individual and his or her location of employment, as well as an assigned serial number that is entered into the access system with the name of the assignee. The badge is scanned into a reader that authorizes and records the person's entry, and sometimes exit, into a facility. The access badges can also be programmed based on the individuals job function. For example, access to a data center or secure operations center would be granted only to individuals who work in that area.

For logical access, users are given a unique identifier, usually their first initial and last name, that they will use to access computers, networks, and applications appropriate to their role in the organization. For both logical and physical access, organizations develop their own processes and procedures to communicate to security and network operations the level of access an individual requires. This communication is usually handled through an electronic request or a form generated by the individual's supervisor.

In August 2004, HSPD-12 was published to establish consistent identity and access controls throughout the federal government. This directive was a result of inconsistent identity management throughout federal agencies and the need to provide secure and reliable forms of identification for physical and logical access.[91]

Response. In response to question 7 on the OMB template, NIT found, based on interviews and reviews of documentation, that the SEC has established and is maintaining an identity and access management program that is generally consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and that identifies users and network devices. NIT found that OIT has developed policies and procedures that address account and identity management.

[89] NIST SP 800-53, Rev. 3, pp. F-3–F-9, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.
[90] A "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 201-1, p. 70, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.
[91] HSPD-12, para. 3, http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#1.

In response to question 7.a(1), NIT found that OIT has developed policies and procedures that address account and identity management. [redacted] is currently in draft form. [redacted] was last updated on April 6, 2006. [redacted], has not been updated since July 9, 2008. Each of these policies indicates that it will be reviewed annually.

In response to question 7.a(2), NIT found that OIT was able to provide the requested list of all users, including federal employees, contractors, and others who access agency systems.

In response to questions 7.a(3) and 7.a(4), NIT found that the SEC does not use multi-factor authentication linked to the PIV card to access information systems, as required by HSPD-12 and in accordance with NIST recommendations. The PIV card is used only for physical access and is not used to access SEC systems.

In response to questions 7.a(5) and 7.a(6), NIT found that separation of duties is sufficiently enforced. NIT also concluded that OIT keeps a record of its asset inventory, including printers, desktops, laptops, and mobile devices.

In response to questions 7.a(7) and 7.a(8), NIT found that accounts are terminated or deactivated once access is no longer required. No shared accounts are used at the Commission.

Table 8 contains OIG's response to question 7, as provided by NIT.

Table 8: OIG Response to Question 7 From OMB Questionnaire

ID	Questions from OMB Questionnaire	Response
7.a	The Agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	Yes
7.a(1)	Documented policies and procedures for account and identity management.	No
7.a(2)	Identifies all users, including federal employees, contractors, and others who access Agency systems.	Yes
7.a(3)	Identifies when special access requirements (e.g., multi-factor authentication) are necessary.	No
7.a(4)	If multi-factor authentication is in use, it is linked to the Agency's PIV program where appropriate.	No
7.a(5)	Ensures that the users are granted access based on needs and separation of duties principles.	Yes
7.a(6)	Identifies devices that are attached to the network and	Yes

ID	Questions from OMB Questionnaire	Response
	distinguishes these devices from users.	
7.a(7)	Ensures that accounts are terminated or deactivated once access is no longer required.	Yes
7.a(8)	Identifies and controls use of shared accounts.	Yes

Source: OMB FISMA Web Portal.

Section 8: Status of Continuous Monitoring Management

Background. Continuous monitoring is the process of tracking the security state of an information system on an ongoing basis and maintaining the security authorization for the system over time. Understanding the security state of information systems is essential in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and mission and business processes. Network vulnerability assessments, intrusion detection systems (IDS), intrusion prevention systems (IPS), and C&A are all components of continuous monitoring programs. NIST SP 800-53 provides guidance on continuous monitoring includes the following:

- CA-7—Continuous Monitoring

The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. A configuration management process for the information system and its constituent components;
b. A determination of the security impact of changes to the information system and environment of operation;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and
d. Reporting the security state of the information system to appropriate organizational officials [Assignment: organization-defined frequency].[92]

Successful network monitoring and incident handling includes the following key components: assisting in rapid breach response; conducting a thorough investigation of the system; containing the damage; gathering and analyzing evidence; improving system practices, plans, and procedures; providing expert reports and testimony, if necessary; and minimizing the loss of revenue. Continuous monitoring ensures that all security-related incidents are handled in a timely manner.

[92] NIST SP 800-53, Rev. 3, pp. F-36 - F-37 http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

Response. In response to question 8 on the OMB template, based on interviews and reviews of documentation, the SEC has established and is maintaining an enterprise-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

Concerning question 8.a(1), the OIT has a template for preparing continuous monitoring reports, but has not developed policy or procedures to address continuous monitoring.

In response to question 8.a(2), NIT found that a template for preparing continuous monitoring reports has been developed.

Concerning question 8.a(3), NIT found that there is an approved continuous monitoring plan, and the provided continuous monitoring reports are constructed based on the approved continuous monitoring plan.

In response to question 8.a(4), NIT found that the continuous monitoring plan includes a defined frequency for OIT to provide authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions and updates, and that OIT provides the reports with the frequency specified. NIT reviewed a General Support System continuous monitoring overview report and found that it covers updates to the SSPs and POA&Ms. Table 9 contains OIG's response to question 8, as provided by NIT.

Table 9: OIG Response to Question 8 From OMB Questionnaire

ID	Questions from OMB Questionnaire	Response
8.a	The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	Yes
8.a(1)	Documented policies and procedures for continuous monitoring.	No
8.a(2)	Documented strategy and plans for continuous monitoring.	Yes
8.a(3)	Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.	Yes
8.a(4)	Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions and updates with the frequency defined in the strategy and/or plans.	Yes

Source: OMB FISMA Web Portal.

Section 9: Status of Contingency Planning

Background. Contingency planning refers to development of processes, policies, and procedures for reestablishing operations for an enterprise after a man-made or natural disaster. Examples of issues addressed in contingency planning are reactivation of systems, communication to personnel, alternate work location for personnel, roles and responsibilities, and utilities (telecommunications, power, water). NIST SP 800-53 lists the following controls pertaining to contingency planning:

- CP-1 Contingency Planning Policy and Procedures
- CP-2 Contingency Plan
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing and Exercises
- CP-6 Alternate Storage Site
- CP-7 Alternate Processing Site
- CP-8 Telecommunications Services
- CP-9 Information System Backup
- CP-10 Information System Recovery and Reconstitution[93]

Contingency planning focuses on recovery strategies that provide a means to restore operations quickly and effectively following a service disruption, as well as the strategies to address disruption impacts and allowable outage times.

Response. In response to question 9 on the OMB template, NIT found, based on interviews and reviews of documentation, that the SEC has established and is maintaining an enterprise-wide business continuity/disaster recovery program that is generally consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

In response to question 9.a(1), NIT determined that OIT has documented business continuity and disaster recovery policies and procedures. However, the policies have not been updated since 2002, and the procedures have not been updated since 2003. [redacted], was last updated on August 6, 2002, and [redacted] was last updated on February 4, 2003.

In response to question 9.a(2), NIT found that a business impact analysis (BIA has been executed for all major applications at the SEC. [94]

[93] NIST SP 800-53, Rev. 3, pp. F-47 - F-53, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

[94] The purpose of the BIA is to help "identify and prioritize information systems and components critical to supporting the organization's mission/business processes." NIST SP 800-34, Rev. 1, p. ES-1, http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.

In response to questions 9.a(3) and 9.a(4), NIT reviewed disaster recovery plans across all the systems being evaluated and determined that those plans, along with the documented recovery exercises, demonstrate the documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures. Further, NIT found that OIT performs annual contingency plan testing at the OIT level for major applications.

In response to question 9.a(5), NIT reviewed the disaster recovery plans across multiple systems at the SEC and determined that disaster recovery plans are in place and can be implemented when necessary.

In response to questions 9.a(6) and 9.a(7), NIT determined, after reviewing test, training, and exercise documentation, that the development of test, training, and exercise programs happens in the weeks prior to the exercise's execution date. NIT determined that annual exercises to determine the effectiveness of and to maintain current business continuity/disaster recovery plans are performed.

Table 10 contains OIG's response to question 9, as provided by NIT.

Table 10: OIG Response to Question 9 From OMB Questionnaire

ID	Questions from OMB Questionnaire	Response
9.a	The Agency established and is maintaining an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	Yes
9.a(1)	Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.	No
9.a(2)	The agency has performed an overall Business Impact Analysis (BIA).	Yes
9.a(3)	Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.	Yes
9.a(4)	Testing of system specific contingency plans.	Yes
9.a(5)	The documented business continuity and disaster recovery plans are in place and can be implemented when necessary.	Yes
9.a(6)	Development of test, training, and exercise (TT&E) programs.	Yes
9.a(7)	Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans.	Yes

Source: OMB FISMA Web Portal.

Section 10: Status of Contractor Systems

Background. Outside contractors play an integral role in federal government operations. Their services range from staff augmentation to technology system

development, operation, and maintenance. Contractors are subject to the same rules of conduct as employees of the organization they are brought in to support and therefore must adhere to all of the organization's policies and procedures. Contractor systems deployed in the federal government are subject to a full C&A prior to implementation and are also governed by policies and procedures of the agency for compliance with NIST, FISMA, and OMB guidance. NIST SP 800-53 provides the following guidance pertaining to contractor systems:

- CA-3 Information System Connections

The organization:

a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements;
b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.[95]

Response. In response to question 10 on the OMB template, NIT found, based on interviews and reviews of documentation, that the SEC has established and is generally maintaining a program to oversee systems operated on its behalf by contractors or other entities, including SEC systems and services residing in the public cloud.

In response to question 10.a(1), NIT found that OIT does not have documented policies and procedures to address security oversight of systems operated on the SEC's behalf by contractors or other entities.

In response to question 10.a(2), NIT found that the SEC does consistently assure that security controls of contractor systems are effectively implemented and comply with federal and SEC guidelines.

In response to question 10.a(3), NIT found that OIT has a complete inventory of systems operated on the SEC's behalf by contractors or other entities, including SEC systems and services residing in the public cloud.

In response to questions 10.a(4) and 10.a(5), NIT found, after reviewing the risk assessment documents, that the SEC identifies the interface between contractor/external systems and SEC-operated systems. In addition, NIT found

[95] NIST SP 800-53, Rev. 3, p. F-34, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

that OIT has the appropriate agreements in place for systems that maintain a persistent connection to the SEC.

In response to questions 10.a(6) and 10.a(7), NIT found that the inventory of contractor systems is updated at least annually. NIT also determined that systems that are owned or operated by contractors or entities, including SEC systems and services residing in the public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

Table 11 contains OIG's response to question 10, as provided by NIT.

Table 11: OIG Response to Question 10 From OMB Questionnaire

ID	Questions from OMB Questionnaire	Response
10.a	The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	Yes
10.a(1)	Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.	No
10.a(2)	The Agency obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and agency guidelines.	Yes
10.a(3)	A complete inventory of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.	Yes
10.a(4)	The inventory identifies interfaces between these systems and Agency-operated systems.	Yes
10.a(5)	The agency requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.	Yes
10.a(6)	The inventory of contractor systems is updated at least annually.	Yes

Source: OMB FISMA Web Portal.

Section 11: Status of Security Capital Planning

Background. Security capital planning is the process of applying funding toward high-priority security investments to support the objective of implementing and maintaining appropriate security controls for information systems. It provides a systematic approach to selecting, managing, and evaluating IT security investments.

Implementation of IT security within the federal government is guided by a combination of legislation, rules and regulations, and agency-specific policies. Specifically, FISMA requires agencies to integrate IT security into their capital planning and enterprise architecture processes, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to OMB. NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process,* outlines the security capital planning initiatives for federal agencies.[96]

Under FISMA, an organization is responsible for establishing and maintaining a security capital planning and investment program for information security. Documentation for the program must include policies and procedures relative to security capital planning and address the information security requirements as part of the capital planning and investment process. An organization's budget must contain a discrete line item for information security in organizational programming and documentation. When required, a business case/Exhibit 300/Exhibit 53 must be submitted to record the information security resources required, and planned resources must be available for expenditure.[97]

Response. In response to question 11 on the OMB template, based on interviews and reviews of documentation, NIT found that the SEC has established and is maintaining a security capital planning program for information security.

In response to questions 11.a(1) and 11.a(2), NIT determined that the SEC has documented policies and procedures to address information security in the capital planning and investment control process. NIT found that OIT includes information security requirements as part of the capital planning and investment process.

[96] NIST SP 800-65, *Integrating IT Security Into the Capital Planning and Investment Control Process* (January 2005), http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf.
[97] The Exhibit 300 reflects an investment's plan for capital asset management. The Exhibit 53 includes a rollup of all Exhibit 300s and additional IT expenses from across the agency. NIST SP 800-65, p. 7, http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf.

In response to question 11.a(3), NIT found, after reviewing the appropriate documentation, that OIT establishes a discrete line item for information security in organizational programming and documentation.

In response to question 11.a(4), NIT found that OIT employs a business case to record the information security resources required and has submitted the required Exhibit 300 and Exhibit 53 to OMB.

In response to question 11.a(5), NIT found that security resources are available for expenditure as planned.

Table 12 contains OIG's response to question 11, as provided by NIT.

Table 12: OIG Response to Question 11 From OMB Questionnaire

ID	Questions from OMB Questionnaire	Response
11.a	The Agency has established and maintains a security capital planning and investment program for information security. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	Yes
11.a(1)	Documented policies and procedures to address information security in the capital planning and investment control process.	Yes
11.a(2)	Includes information security requirements as part of the capital planning and investment process.	Yes
11.a(3)	Establishes a discrete line item for information security in organizational programming and documentation.	Yes
11.a(4)	Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.	Yes
11.a(5)	Ensures that information security resources are available for expenditure as planned.	Yes

Source: OMB FISMA Web Portal.

OIT Policies and Procedures Past Due for Updates

Table 13: OIT Policies and Procedures and Date of Last Update

FISMA Controls	Name of Policy	Policy Number	Date Last Updated	Defined Frequency	Where Frequency Specified	Number of Years Outdated
[redacted]	[redacted]	[redacted]	12/22/05	Annual	Specified in policy or procedure	5
[redacted]	[redacted]	[redacted]	3/13/07	Annual	Specified in policy or procedure	3
	[redacted]	[redacted]	1/3/06	Annual	Specified in policy or procedure	4
	[redacted]	[redacted]	12/30/05	Annual	Specified in policy or procedure	5
	[redacted]	[redacted]	4/24/06	Annual	Specified in policy or procedure	4
	[redacted]	[redacted]	4/17/06	Annual	Specified in policy or procedure	4
	[redacted]	[redacted]	1/11/06	Annual	Specified in policy or procedure	4
	[redacted]	[redacted]	12/30/05	Annual	Specified in policy	5
	[redacted]	[redacted]	4/17/06	Annual	Specified in policy or procedure	4
	[redacted]	[redacted]	4/17/06	Annual	Specified in policy or procedure	4
	[redacted]	[redacted]	4/17/06	Annual	Specified in policy or procedure	4
	[redacted]	[redacted]	12/30/05	Annual	Specified in policy or procedure	5
	[redacted]	[redacted]	12/28/05	Annual	Specified in policy or procedure	5

[98] The site was accessed for the [redacted] policy on August 15, 2011.
[99] The site was accessed for the [redacted] policies on September 14, 2011.

FISMA Controls	Name of Policy	Policy Number	Date Last Updated	Defined Frequency	Where Frequency Specified	Number of Years Outdated
	[redacted]	[redacted]	12/29/05	Annual	Specified in policy or procedure	5
	[redacted]	[redacted]	1/11/06	3 years	IT Security Compliance Program Policy	2
	[redacted]	[redacted]	1/11/06	3 years	IT Security Compliance Program Policy	2
	[redacted]	[redacted]	12/30/05	3 years	IT Security Compliance Program Policy	3
	[redacted]	[redacted]	12/30/05	3 years	IT Security Compliance Program Policy	3
	[redacted]	[redacted]	12/ 30/05	3 years	IT Security Compliance Program Policy	3
	[redacted]	[redacted]	1/ 3/06	3 years	IT Security Compliance Program Policy	2
	[redacted]	[redacted]	1/ 3/06	3 years	IT Security Compliance Program Policy	2
	[redacted]	[redacted]	12/30/05	3 years	IT Security Compliance Program Policy	3
	[redacted]	[redacted]	4/17/06	3 years	IT Security Compliance Program Policy	2
	[redacted]	[redacted]	1/11/06	3 years	IT Security Compliance Program Policy	2
	[redacted]	[redacted]	1/11/06	3 years	IT Security Compliance Program Policy	2
	[redacted]	[redacted]05	1/11/06	3 years	IT Security Compliance Program Policy	2
	[redacted]	[redacted]	1/11/06	3 years	IT Security Compliance Program Policy	2

FISMA Controls	Name of Policy	Policy Number	Date Last Updated	Defined Frequency	Where Frequency Specified	Number of Years Outdated
	[redacted]	[redacted]				
	[redacted]	[redacted]	12/30/05	3 years	IT Security Compliance Program Policy	3
	[redacted]	[redacted]	12/30/05	3 years	IT Security Compliance Program Policy	3
	[redacted]	[redacted]	12/30/05	3 years	IT Security Compliance Program Policy	3
	[redacted]	[redacted]	4/17/06	3 years	IT Security Compliance Program Policy	2
[redacted]	[redacted]	[redacted]	8/9/07	Annual	Specified in policy or procedure	3
	[redacted]	[redacted]	3/6/07	3 years	IT Security Compliance Program Policy	1
[redacted]	[redacted]	[redacted]	12/29/05	Annual	Specified in policy or procedure	3
[redacted]	[redacted]	[redacted]	6/29/05	Annual	Specified in policy or procedure	3
[redacted]	[redacted]	[redacted]	8/20/02	3 years	IT Security Compliance Program Policy	6
	[redacted]	[redacted]	4/16/02	3 years	IT Security Compliance Program Policy	6
	[redacted]	[redacted]	4/16/02	Annual	Specified in policy or procedure	8
	[redacted]	[redacted]	8/10/06	Annual	Specified in policy or procedure	4
	[redacted]	[redacted]	12/30/05	Annual	Specified in policy or procedure	5

[100] The site was accessed for the [redacted] and reporting policies on September 13, 2011.
[101] The site was accessed for the [redacted] training policy on September 13, 2011.
[102] The site was accessed for the [redacted] on August 15, 2011.
[103] The site was accessed for the [redacted] management policies on September 19, 2011.

FISMA Controls	Name of Policy	Policy Number	Date Last Updated	Defined Frequency	Where Frequency Specified	Number of Years Outdated
	[redacted]	[redacted]	12/30/05	3 years	IT Security Compliance Program Policy	3
[redacted]	[redacted]	[redacted]	7/9/08	Annual	Specified in policy or procedure	2
	[redacted]	[redacted]	4/ 6/06	Annual	Specified in policy or procedure	4
[redacted]	[redacted]	[redacted]	8/6/02	Annual	Specified in policy or procedure	8
	[redacted]	[redacted]	2/4/03	Annual	Specified in policy or procedure	7

Source: NIT Generated.

[104] The site was accessed for the [redacted] management policies on September 12, 2011.
[105] The site was accessed for the [redacted] policies on September 9, 2011.

Management Comments

MEMORANDUM

TO: Noelle Maloney, Acting Inspector General, Office of Inspector General

FROM: Thomas A. Bayer, Director, Office of Information Technology

RE: Office of Information Technology's Response to the Office of Inspector General's Draft Report, *2011 Annual FISMA Executive Summary Report, Report No. 501*

DATE: February 2, 2012

This memorandum is in response to the Office of Inspector General's (OIG) Draft Report No. 501 entitled, *2011 Annual FISMA Executive Summary Report*. Thank you for the opportunity to review and respond to this report.

OIG Recommendation:

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.

OIT concurs with this recommendation. We are currently revising all policies and will develop a plan to review and update on a regular basis.

Recommendation 2:

The Office of Information Technology should develop a comprehensive risk management strategy in accordance with National Institute of Standards and Technology, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach that will ensure management of system-related security risks is consistent with the Commission's mission/business objectives and overall risk strategy.

OIT concurs with this recommendation. OIT will develop an information system-related security risk management program consistent with NIST SP800-37 and the mission/business risk strategy established by senior Commission leadership.

Recommendation 3:

1

The Office of Information Technology (OIT) should update its risk management policy to include language regarding developing a comprehensive governance structure and ensure management of system-related security risks is consistent with the Commission's mission/business objectives and overall risk strategy.

OIT concurs with this recommendation. OIT will update its risk management policy to be consistent with NIST SP800-37 and the mission/business risk strategy established by senior Commission leadership. While OIT Security already works with Divisions, Offices and Regional Offices on a business impact analysis, OIT Security will document risk, beginning with the finalization of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments. *As of January 2, 2012, NIST anticipates finalization in June 2012.*

Recommendation 4:

The Office of Information Technology should develop and implement a formal risk management procedure that identifies an acceptable process for evaluating system risk and is consistent with the Commission's mission/business objectives and overall risk strategy.

OIT concurs with this recommendation. OIT will implement an information system-related security risk management procedure consistent with NIST SP800-37 and the mission/business risk strategy established by senior Commission leadership. While OIT Security already works with Divisions, Offices and Regional Offices on a business impact analysis, OIT Security will document risk, beginning with the finalization of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments. *As of January 2, 2012, NIST anticipates finalization in June 2012.*

Recommendation 5:

The Office of Information Technology should develop and implement formal policy that addresses tailoring baseline security controls sets.

OIT concurs with this recommendation. OIT Security is working on a comprehensive update of its policies and procedures, including documentation to address 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 tailoring), at the

individual information system level, or by using a combination of organization-level and system-specific approaches.

OIT concurs with this recommendation. OIT Security is working on a comprehensive update of its policies and procedures, including documentation to address tailoring baseline security control sets.

Recommendation 7:

The Office of Information Technology should tailor a baseline security controls set (with rationale) for applicable systems in accordance with the guidance in 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*.

OIT concurs with this recommendation. OIT Security is working on a comprehensive update of its policies and procedures, including documentation to address tailoring baseline security control sets.

Recommendation 8:

The Office of Information Technology should review and update its configuration management policy and ensure that it complies with the Federal Information Security Management Act requirements, the guidelines specified in National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems and Organizations*, and its internal requirements.

OIT concurs with this recommendation. OIT Security is working on a comprehensive update of its policies and procedures, including documentation to address configuration management.

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.

OIT concurs with this recommendation. OIT Security is working on a comprehensive update of its policies and procedures, including identification of approved deviations and exceptions to the standard.

Recommendation 10:

The Office of Information Technology should conduct compliance scans of its information technology devices, according to the organizationally defined frequency in the policy and procedures, to ensure that all devices are configured as required by the Office of Information Technology's configuration management policy and procedures.

OIT concurs with this recommendation. OIT Security is working on configuring automated devices to conduct compliance scans of information technology devices to ensure that all are configured as required by OIT's configuration management policy and procedures.

Recommendation 11:

The Office of Information Technology should update its policy and include language indicating that deviations from baseline configurations that are identified and documented as a result of the configuration compliance scans are properly remediated in a timely manner.

OIT concurs with this recommendation. OIT Security is working on comprehensive documentation of its standard baseline configuration including identification of approved deviations, exceptions to the standard and timely remediation of exceptions.

Recommendation 12:

The Office of Information Technology should provide a new date to the Office of Management and Budget for implementing the technical solution for linking multifactor authentication to Personal Identity Verification cards for system authentication.

OIT concurs with this recommendation. SEC OIT, as many other agencies, is working through technical challenges for successful implementation to be able to effectively provide remote access using PIV authentication to the user community. OIT will reach out to agencies that have successfully implemented multifactor authentication using the Personal Identity Verification (PIV) cards.

Recommendation 13:

The Office of Information Technology should complete its implementation of the technical solution for linking multi-factor authentication to Personal Identity Verification (PIV) cards for system authentication and require use of the PIV cards as a second authentication factor by December 2012.

OIT concurs with this recommendation. OIT is working through technical challenges for successful implementation to be able to effectively provide remote access via PIV authentication to the user community. OIT will reach out to agencies that have

successfully implemented multifactor authentication using the Personal Identity Verification (PIV) cards.

OIG Response to Management's Comments

We are pleased that OIT concurred with the report's 13 recommendations. We are also encouraged that OIT has indicated that they will initiate actions to address the findings described in the report. We believe that OIT's proposed actions are responsive to the report's findings and recommendations and their implementation of the recommendations will further aid in strengthening the SEC's information security program and its systems.

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

Telephone: 202-551-6061
Fax: 202-772-9265
E-mail: oig@sec.gov

Hotline

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

Telephone: 877.442.0854

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