



U.S. Securities and Exchange Commission
Office of Inspector General
Office of Audits

2010 Annual FISMA Executive Summary Report



March 3, 2011
Report No. 489



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

MEMORANDUM

March 3, 2011

To: Thomas Bayer, Chief Information Officer, Office of Information Technology (OIT)

From: H. David Kotz, Inspector General, Office of Inspector General *HDK*

Subject: *2010 Annual FISMA Executive Report, Report No. 489*

This memorandum transmits the U.S. Securities and Exchange Commission's Office of Inspector General's (OIG) final report on the *2010 Federal Information Security Management Act of 2002 (FISMA)* review. The final report contains eight recommendations which if implemented, should strengthen the Commission's security posture. OIT concurred with all eight recommendations. Your written response to the draft report is included in Appendix VI.

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

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

Attachment

cc: Kayla J. Gillan, Deputy Chief of Staff, Office of the Chairman
Luis A. Aguilar, Commissioner
Troy A. Paredes, Commissioner
Elisse Walter, Commissioner
Jeff Heslop, Chief Operating Officer, Office of Chief of Operations
Diego T. Ruiz, Executive Director, Office of the Executive Director
Lewis W. Walker, Deputy Director and Chief Technology Officer, Office of Information Technology

2010 FISMA Executive Summary Report

Executive Summary

In August 2010, the U.S. Securities and Exchange Commission (SEC or Commission), Office of Inspector General (OIG), contracted C5i Federal, Inc. (C5i) to assist with the completion and coordination of the OIG's input to the Commission's response to the Office of Management and Budget (OMB), *Memorandum M-10-15 FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.¹ This memorandum provides the instructions and templates for meeting the fiscal year (FY) 2010 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347).²

C5i commenced work on this project in September 2010. C5i's tasks included completing the OIG portion of the FISMA template (Section C) and developing an Executive Summary Report that communicates the Inspector General's response to the 2010 FISMA submission. C5i's responses were based on information that was provided in agency staff interviews and a review of supporting documentation. C5i did not conduct detailed control tests to verify the accuracy of the data the SEC provided. Based on C5i's assessment and recommendations, the OIG submitted its responses to the 2010 FISMA questionnaire using OMB's on-line reporting tool, CyberScope.

Background. FISMA, 44 U.S.C. § 3541, *et seq.*, is a United States federal law enacted in 2002 as the *Title III of the E-Government Act of 2002*. The statute recognizes the importance of information security to the economic and national security interests of the United States. Further, the statute requires federal agencies to develop, document, and implement an agency-wide program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by other agencies, contractors, or other sources.

FISMA requires agency program officials, Chief Information Officers, Privacy Officers, and OIGs to conduct annual reviews of the agency's information security and privacy programs, and report the results to OMB. The OMB then uses this data to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with the statute.

¹ Office of Management and Budget's Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf.

² Federal Information Security Management Act of 2002 (Title III, Pub. L. No. 107-347), <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>.

FISMA provides the framework for securing the Federal Government's information technology. All agencies must implement the requirements of FISMA and report annually to OMB and Congress on the effectiveness of their information security and privacy programs. OMB uses this information 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 the development of the E-Government Scorecard under the President's Management Agenda.

As part of its FISMA review, C5i also conducted reviews to examine the SEC's continuous monitoring program and covering the SEC's oversight of contractor held personally identifiable information. The results of these audits will be issued later, in separate OIG reports.

Objectives. The overall objective for the FISMA assessment was to independently evaluate and report on how the Commission has implemented its mandated information security requirements. Secondly, the objective was to provide clarity regarding the OIG's input and responses to the OMB questionnaire.

Results. The key findings and results for the 2010 FISMA assessment are as follows:

- The Commission has developed a Certification and Accreditation (C&A) program, and is in compliance with applicable regulatory and statutory requirements. However, as noted in the SEC OIG's *Assessment of the SEC's Privacy Program*, Report No. 485, September 29, 2010 (Report No. 485), the Office of Information Technology's (OIT) categorization of network vulnerabilities may impact the C&A process. OIT concurred with the recommendation and is currently re-evaluating its risk categorization process.
- The SEC has a Security Configuration Management program that has policies and procedures, baselines, and an inventory of software and hardware. However, as also noted in Report No. 485, OIT has not fully implemented the Federal Desktop Core Configuration (FDCC), exceptions have not been reported to the National Institute of Standards and Technology (NIST), and justifications for identified "exceptions" have not been fully documented.
- OIT has an Incident Response & Reporting Program with documented policies and procedures. The SEC Incident Response handbook details

the SEC employees and contractors roles and responsibilities in reporting/responding to incidents. Incidents are documented from the moment of reporting until resolution.

- Annual Security Awareness Training was provided to all SEC employees and contractors. In 2010, the SEC developed its own training and incorporated its “SEC Rules of the Road” training into the sessions. As of November 15, 2010, 4,732 of 4,778 (99.04 percent) SEC employees and contractors successfully completed the Annual Cybersecurity Awareness training.
- OIT maintains a Plan of Actions & Milestones (POA&M) process. The POA&M details the vulnerability, associated NIST controls, remediation/mitigation strategy, risk level, and projected/planned remediation date. The POA&M is reviewed and updated quarterly. POA&M items are tracked using the Cyber Security Assessment and Management (CSAM) tool.
- The SEC has a “Remote Access” program that complies with federal guidance and employs security measures. The remote access program using a two factor authentication requirement comprised of an account password and a RSA token that has a Personal Identification Number (PIN). SEC employees and contractors can remotely access the SEC’s systems with an account password and RSA token and PIN. OIT’s policies and procedures are documented and comply with NIST, OMB, and FISMA guidance.³
- The SEC has an account and identity management program with policies and procedures for both establishing and deactivating physical and logical (network) accounts. However, the HSPD-12 card program completion date was delayed from September 30, 2010 to June 30, 2011, for both physical access and logical access. Also, in several instances, “least-privilege,” e.g., access only required to perform the functions of a user’s position, was not effectively applied for network accounts having “indefinite administrative” privileges, which provide the user with the ability to install software and make changes to mandatory settings. In the event this level of privilege is granted to a user, it should be only for a set amount of time such as 60 - 90 minutes, that is needed to perform a specific and approved function and then the privilege should be disabled.
- The SEC has a continuous monitoring program that includes vulnerability scanning, patch management policies and procedures, and ongoing assessment of security controls. However, as noted in Report No. 485,

³ RSA tokens are two-factor authentication devices based on something you know such as a password or PIN and something you have such as an authenticator device.

there remains a problem with the timely implementation of new patches. Further, OIT maintains insufficient documentation on what patches were deployed and the date of deployment.

- The SEC has a Contingency Planning program with documented policies and procedures. Contingency plan testing is performed bi-annually in April and November. Further, “Lessons Learned” from the exercises are developed and addressed.
- The SEC has a contractor oversight program and has documented policies and procedures utilizing adequate security controls in accordance with the NIST and OMB guidance.

Summary of Recommendations. We developed eight recommendations to address vulnerabilities identified in the current assessment. Specifically, we recommend that:

- (1) OIT should identify all exceptions to the Federal Desktop Core Configuration standards and submit them to National Institute of Standards and Technology within 90 days of the issuance date of this report.
- (2) OIT should ensure justifications for deviations from Federal Desktop Core Configurations requirements are fully documented.
- (3) OIT should:
 - 3a. Perform a thorough review and identify the universe of all Commission user accounts;
 - 3b. Once the universe has been identified, OIT should then identify all “active” and “inactive” user accounts and determine whether or not the account should be disabled; and
 - 3c. Take immediate action to disable the accounts of employees and contractors who no longer work at the Commission.
- (4) OIT should review their policies and procedures for disabling accounts to ensure they are well-documented and thorough, and provide training to appropriate staff regarding account termination procedures.
- (5) OIT should complete the logical access integration of the HSPD-12 card program no later than December 2011, as it reported to OMB on December 31, 2010.
- (6) OIT should conduct a full review and identify the universe of all users with elevated privileges.

- (7) Based on the review results of recommendation 6, OIT should enforce or develop procedures to ensure:
 - 7a. Only users whose job function require permanent elevated access have the needed privileges;
 - 7b. Business justifications are fully documented; and
 - 7c. Elevated privileges are only issued for the finite amount of time needed to complete assigned task.

- (8) OIT should establish and maintain an accurate and current list of all users that have elevated privileges.

TABLE OF CONTENTS

Executive Summary	iii
Table of Contents	viii
Background and Objectives	1
Findings and Recommendations	3
Finding 1: Exceptions to Federal Desktop Core Configuration Deviations are not Fully Documented	3
Recommendation 1	4
Recommendation 2	5
Finding 2: Accounts Are Not Properly Terminated when Users No Longer Require Access	5
Recommendation 3	7
Recommendation 4	7
Finding 3: SEC Has Not Adequately Implemented the Personal Identity Verification for Logical Access to All Employees and Contractors	7
Recommendation 5	9
Finding 4: Privileges Granted are Excessive	9
Recommendation 6	10
Recommendation 7	10
Recommendation 8	11
Appendices	
Appendix I: Acronyms	12
Appendix II: Scope and Methodology	14
Appendix III: Criteria and Guidance	17
Appendix IV: List of Recommendations	20
Appendix V: OIG’s Response to the OMB Questionnaire	22
Appendix VI: Management Comments	57
Appendix VII: OIG Response to Management’s Comments	59
Appendix VIII: Screenshots	60
Tables	
Table 1: OIG Response to Question 1	25
Table 2: OIG Response to Questions 2 and 3	31
Table 3: OIG Response to Question 4	36
Table 4: OIG Response to Question 5	37
Table 5: OIG Response to Question 6	39

Table 6: OIG Response to Question 7	42
Table 7: OIG Response to Question 8	48
Table 8: OIG Response to Question 9	51
Table 9: OIG Response to Question 10	54
Table 10: OIG Response to Question 11	56

Figures

Figure 1: SEC Administrative Notice, Issued 11/23/2010.....	60
Figure 2: CSAM Home Page.....	61
Figure 3: Inventory of GAO POA&Ms.....	62
Figure 4: POA&M Entry Page	63
Figure 5: POA&M Page.....	64
Figure 6: Incident Escalation Flow Chart.....	65

Background and Objectives

Background

Overview. In August 2010, the U.S. Securities and Exchange Commission (SEC or Commission), Office of Inspector General (OIG), contracted with C5i Federal, Inc. (C5i) to assist with the completion and coordination of the OIG's input to the Commission's response to the Office of Management and Budget (OMB), Memorandum M-10-15 *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.⁴ This memorandum provides the instructions and templates for meeting the fiscal year (FY) 2010 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347).⁵

FISMA provides the framework for securing the Federal Government's information technology. All agencies must implement the requirements of FISMA and report annually to OMB and Congress 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, assist in improving and maintaining adequate agency performance, and assist in the development of the E-Government Scorecard under the President's Management Agenda.

C5i commenced work on this project in September 2010. C5i's tasks included completing the OIG portion of the FISMA template (Section C) and developing an executive summary report that communicates the Inspector General's (IG) response to the 2010 FISMA submission. C5i's responses are based on information that was provided by agency staff and through interviews and the review of supporting documentation. C5i did not conduct detailed control tests to verify the accuracy of the data the SEC staff provided. Based on C5i's assessment and recommendations, the OIG submitted its responses to the 2010 FISMA questionnaire via OMB's on-line reporting tool, CyberScope.

Further, as part of the FISMA assessment, C5i will further conduct audits examining the SEC's continuous monitoring program reviewing the SEC's oversight of contractor held personally identifiable information. These audits will be issued later, in separate OIG reports.

⁴ Office of Management and Budget's Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

⁵ Federal Information Security Management Act of 2002 (Title III, Pub. L. No. 107-347), <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>

Objectives

The overall objective for the FISMA assessment was to provide an independent evaluation and report on how the Commission has implemented its mandated information security requirements. Secondly, the objective was to provide clarity regarding the OIG's input and responses to the OMB questionnaire.

Findings and Recommendations

Finding 1: Exceptions to Federal Desktop Core Configuration Deviations Have Not Been Fully Documented

OIT has not fully documented its “management decisions” for deviating from the Federal Desktop Core Configuration (FDCC) requirements. In addition, the Office of Information Technology (OIT) has not reported its deviations to the National Institute of Standards and Technology (NIST).

FDCC Security Requirements and Standards

As identified in the SEC OIG’s *Assessment of the SEC’s Privacy Program*, Report No. 485, September 29, 2010 (Report No. 485), the Commission maintains a list of deviations from the FDCC security requirements/standards. However, OIT has not submitted its list of deviations from FDCC to NIST, as required by *OMB Memorandum M-09-29, FY 2009 Reporting Instruction for the Federal Information Security Management Act and Agency Privacy Management* (OMB Memorandum M-09-29). OIT provided C5i with a list of its deviations from FDCC standards. The list consists of a comment field entitled “management decisions.” Based on interviews with OIT staff, C5i requested clarification on the “management decisions” contained in the comment field. OIT staff acknowledged that OIT management made a determination in an OIT management meeting that it would deviate from FDCC standards. When asked for the meeting notes or information about who attended the meeting, OIT staff stated that meeting minutes were not taken and that staff could only recall from memory that the Assistant Director for Infrastructure Engineering was in attendance at the meeting. Per OMB Memorandum M-09-29,⁶ exceptions to FDCC security configuration requirements are permitted for requirements that may impair the operations of agency-specific applications. However, such deviations from the FDCC security configuration requirements must be documented and submitted to NIST, and OIT must be able to justify the deviations.

As of January 10, 2011, OIT had not provided NIST with its deviations from the FDCC requirements. As a result, OIT has not met the OMB requirements set forth in OMB’s Memorandum for Heads of Executive Departments and

⁶ OMB Memorandum M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

Agencies, *M-10-15, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, which states, “Agencies must document and provide NIST with any deviations from the common security configurations⁷ and be prepared to justify why they are not using them. IGs should review such use.”⁸ Further, OIT was unable to justify to the OIG why it is not using the common security configurations.

In addition, during our review of the deviations concerning the SEC’s password policy, we found some exceptions had only “management decision” as the stated justification. For example, current SEC policy requires that passwords have at least [REDACTED] and that the password expires every [REDACTED]. FDCC security configuration requires passwords to consist of a minimum of 12 characters with upper and lower case letters and numbers, and that the passwords expire every 90 days. C5i requested documentation from OIT staff to obtain an understanding regarding the nature of OIT’s “management decision” to deviate from this FDCC requirement, but we were informed that supporting documentation was unavailable and no substantive explanation was provided for the decision. Without proper documentation to support its decision to deviate from the FDCC security requirements, OIT cannot adequately justify its management decision to not fully implement FDCC’s security requirements.

Recommendation 1:

The Office of Information Technology should identify all exceptions to the Federal Desktop Core Configuration standards and submit them to National Institute of Standards and Technology within 90 days of the issuance date of this report.

Management Comments. OIT concurred with this recommendation. See Appendix VI for management’s full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation.

⁷ Documentation should be sent to this email address: checklists@nist.gov.

⁸ OMB’s Memorandum for Heads of Executive Departments and Agencies, M-10-15, Subject: *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf.

Recommendation 2:

The Office of Information Technology should ensure justifications for deviations to Federal Desktop Core Configurations requirements are fully and adequately documented.

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

OIG Analysis. We are pleased that OIT concurred with this recommendation.

Finding 2: Network Accounts Are Not Properly Terminated When Users No Longer Require Access to the Network

SEC network accounts for 14 employees who no longer require access to the network were not disabled in a timely manner. Additionally, two accounts were used to access the SEC's network *after* the assigned account users were no longer employed.

SEC Network Systems and User Accounts for SEC Employees and Contractors

To ensure the protection of the SEC's network systems and data, user accounts for SEC employees and contractors that leave the SEC (e.g., separated/terminated staff) should be disabled on the employee's or contractor's last day of work at the Commission. Account termination requests are completed by an Information Technology (IT) Specialist or administrative contact for the office/division where the person works. Completed requests are submitted electronically to OIT. In the event of an "involuntary termination," the Technical Assistance Center (TAC) and OIT security should be notified immediately of the termination and the account should then be disabled. User accounts for SEC employees and contractors that are separated/terminated from the SEC but remain active after their departure pose a significant security risk to the Commission, because the SEC's network systems are vulnerable and could be compromised by these separated/terminated staff whose access privileges remain active. In addition, separated/terminated staff could provide the SEC system information to a malicious party.

OMB Circular A-123, *Management's Responsibility for Internal Control, Appendix A, Internal Control over Financial Reporting* requires agency management to assess, document, test, and report on the effectiveness of Internal Control over Financial Reporting (ICFR) in its annual Performance and Accountability Report. The ICFR is a methodology designed to provide reasonable assurance regarding the reliability of financial reporting. The following internal control elements are evaluated:

- (1) Control environment;
- (2) Risk assessment;
- (3) Control activities;
- (4) Information and communication; and
- (5) Monitoring.

C5i reviewed the results of the SEC's ICFR A-123 assessment that was conducted by the Office of Financial Management's (OFM) independent contractors. As part of its assessment the OFM IT controls team issued a Notice of Findings and Recommendations (NFR) to OIT in August 2010, which identified the aforementioned deficiency and asked OIT, the control owners, to validate the results. The ICFR identified Active Directory (AD) network accounts for separated/terminated SEC employees that were not being disabled in a timely manner. Specifically, the ICFR identified 14 SEC employees who had departed from the SEC and whose AD network accounts were not disabled after their departure. Further, the NFR indicated that two of these employees' AD network accounts were logged into **after** the employees' SEC termination date. As a result of OIT not promptly disabling user accounts when access is no longer needed (i.e., because of separation or termination from the Commission), former employees accounts remained active. Hence, a malicious party could have gained access to sensitive SEC data and compromised the Commission's system. Further, terminated/separated users with elevated privileges, (e.g., local administrative rights),⁹ pose an even greater potential threat to the SEC data/network because these staff's privilege levels allow for access to data/network that is generally not available to normal users. OIT responded to OFM that they agreed with the deficiency and would include it in their remediation efforts for IT security.

⁹ Local Administrative access provides users with higher privileges on their workstations than normal users. This level of privilege allows the user to perform functions, such as installation of third party software, removing or turning off settings, e.g., forced encryption.

Recommendation 3:

The Office of Information Technology (OIT) should:

- 3a. Perform a thorough review and identify the universe of all Commission user accounts.
- 3b. Once the universe has been identified, OIT should then identify all “active” and “inactive” user accounts and determine whether any accounts should be disabled.
- 3c. Take immediate action to disable the accounts of employees and contractors who no longer work at the Commission.

Management Comments. OIT concurred with this recommendation. See Appendix VI for management’s full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation.

Recommendation 4:

The Office of Information Technology should review their policies and procedures for disabling accounts to ensure they are well-documented and thorough, and provide training to appropriate staff regarding account termination procedures.

Management Comments. OIT concurred with this recommendation. See Appendix VI for management’s full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation.

Finding 3: The SEC Has Not Adequately Implemented the Personal Identity Verification for Logical Access to All Employees and Contractors

The SEC has not completed logical access integrations of Personal Identity Verification (PIV) cards as required by the Homeland Security Presidential Directive 12 (HSPD-12).

Personal Identity Verification

The SEC has not completed its rollout of the PIV badge to all employees and contractors, as required by the HSPD-12 directive. As a result, all employees and contractors are not utilizing the PIV badge for logical access, as required by the HSPD-12 directive. Further, rollout of the technology to support the PIV program has not been completed. The HSPD-12 directive was published in August 2004, and outlined a “Common Identification Standard for Federal Employees and Contractors.” Per the HSPD-12 directive, the HSPD-12 badge should be used for both physical access (facilities) and logical access (networks). The directive states, “the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems.”¹⁰

C5i was initially informed that the HSPD-12 badge rollout for all SEC staff and contractors was to be completed by September 30, 2010. However, the full rollout date has now been changed to June 2011. As of December 31, 2010, 3,311 of 5,334¹¹ SEC employees and contractors were issued HSPD-12 badges.¹² However, C5i was unable to verify whether the total number of contractors requiring PIV credentials is accurate because the Commission has not been able to provide the OIG with a consolidated list of its current contractors.

OIT reported in its September 30, 2010 report to OMB that the projected completion of the HSPD-12 logical access integration was to be December 30, 2011. However, OIT has now stated that it will not complete its roll-out of the logical access requirement for HSPD-12 until it moves to a new operating system, because this will provide a cost savings to the government. OIT also indicated that it has identified concerns pertaining to the remote access of users that use the HSPD-12 card. OIT stated it is performing further work on identifying technology solutions for these remote access issues. In addition,

¹⁰ Homeland Security Presidential Directive-12 (HSPD-12), Subject: Policies for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004, http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#1.

¹¹ The 3,311 SEC employees and contractors that were issued HSPD-12 badges was derived from the total number of PIV credentials the SEC issued to its employees 2,669 and the total number of PIV credentials that were issued to contractors 642; as reported in the SEC's HSPD-12 Implementation Status Report submitted to OMB on December 31, 2010. The 5,334 population of SEC employees and contractors that were issued badges was derived from the total number of PIV credentials that were issued to SEC employees 2,669; the total number of PIV credentials that were issued to contractors 642; the number of SEC employees needing PIV credentials 1,238; and the number of contractors needing PIV credentials 785; as reported in the SEC's HSPD-12 Implementation Status Report submitted to OMB on December 31, 2010.

¹² SEC's HSPD-12 Implementation Status Report submitted to OMB on December 31, 2010. http://www.sec.gov/about/piv_report_for_omb.pdf. SEC's HSPD-12 Implementation Status Report submitted to OMB on December 31, 2010.

as a result of delays in the SEC completing and adjudicating National Agency Check Inquiries background investigations, the SEC has not completed its issuance of PIV credentials to all employees and contractors. Further, the delays have impacted OIT's acquisition of technology to support logical access using PIV credentials. As a result and by not adequately planning the implementation of PIV for logical access, the agency is non-compliant with the HSPD-12 directive.

Recommendation 5:

The Office of Information Technology should complete the logical access integration of the HSPD-12 card no later than December 2011, as reported to the Office of Management Budget on December 31, 2010.

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

OIG Analysis. We are pleased that OIT concurred with this recommendation.

Finding 4: Administrative Access Privileges Granted to Some SEC Staff are Excessive

An excessive number of SEC employees and contractors were unnecessarily granted administrative access privileges on a permanent basis.

SEC Administrative Access Privileges

Approximately 1,000 SEC employees and contractors (users) have been given local administrative access privileges, which are considered "elevated privileges," on a permanent basis, but their job functions do not necessarily require this level of privilege, other than on a temporary basis. The NIST *Recommended Security Controls for Federal Information Systems and Organizations*, guidance states, "The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions".¹³ Local

¹³ The National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 3, page F-9, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

administrative access privileges for workstations consist of elevated privileges that allow users to install software on their systems, change configurations, i.e., disabling mandatory encryption for portable media, etc. Local administrative privileges are usually granted to SEC employees and contractors such as system administrators, whose job function requires a higher level of access in order to manage the network and workstations that are a part of their job responsibilities. There are occasions when users may need to install software on their desktops, such as CyberScope to respond to the OMB FISMA questionnaire. However, these user privileges should generally be granted within a set or limited amount of time, such as 60 - 90 minutes. Based on interviews conducted with OIT personnel and of the users that were identified as having elevated privileges, C5i determined that administrative access was unnecessarily granted to an excessive number of users on a permanent basis.

We also took a judgmental sampling of the names of current SEC employees and contractors who had elevated privileges and compared them to the SEC's email and phone directory and determined that some SEC employees and contractors with elevated privileges appeared to no longer work at the Commission. Having an excessive number of users with elevated administrative access privileges that are not needed for daily job responsibilities increases the risk that unauthorized software may be installed on workstations and the standard controls set by OIT may be altered. Also, if user accounts with elevated privileges are compromised, a malicious party may have an easier time accessing the SEC's networks.

Recommendation 6:

The Office of Information Technology should conduct a full review and identify the universe of all users with elevated privileges.

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

OIG Analysis. We are pleased that OIT concurred with this recommendation.

Recommendation 7:

Based on the review results from recommendation 6, the Office of Information Technology should enforce or develop procedures to ensure:

- 7a. Only users whose job function require permanent elevated access have the needed privileges;

- 7b. Business justification are fully documented; and
- 7c. Elevated privileges are only issued for the finite amount of time needed to complete assigned task.

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

OIG Analysis. We are pleased that OIT concurred with this recommendation.

Recommendation 8:

The Office of Information Technology should maintain an accurate and current list of all users that have elevated privileges.

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

OIG Analysis. We are pleased that OIT concurred with this recommendation.

Acronyms

AD	Active Directory
BIA	Business Impact Assessment
C&A	Certification and Accreditation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM/QA	Configuration Management and Quality Assurance
CMU/SEI	Carnegie Mellon University Software Engineering Institute
COOP/DR	Continuity of Operations/Disaster Recovery
COTR	Contracting Office Technical Representative
CSAM	Cyber Security Assessment and Management
DOJ	Department of Justice
ESM	Enterprise Security Manager
FCD	Federal Continuity Directive
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
GSA	General Services Administration
GSS	General Support System
HSPD-12	Homeland Security Presidential Directive 12
ICFR	Internal Control over Financial Reporting
IDS	Intrusion Detection System
IG	Inspector General
II	Implementing Instruction
IPS	Intrusion Prevention System
ISA	Interconnection Security Agreement
IT	Information Technology
JSAS	Joint State-USAID
LAN	Local Area Network
MEF	Mission Essential Functions
MOU	Memoranda of Understanding
NEF	National Essential Functions
NIST	National Institute of Standards and Technology
O-CCB	Operations Configuration Change Board
OD	Operating Directive
OFM	Office of Financial Management
OHR	Office of Human Resources

OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OP	Operating Procedure
PIN	Personal Identification Number
PIV	Personal Identity Verification
PMEF	Primary Mission Essential Functions
POA&M	Plan of Actions and Milestones
QM	Quality Management
SANS	SysAdmin, Audit, Network, Security
SCR	System Change Request
SEC	Securities and Exchange Commission
SP	Special Publication
SSL	Secure Sockets Layer
SSP	System Security Plan
ST&E	Security Test and Evaluation
TAC	Technical Assistance Center
US-CERT	United States Computer Emergency Readiness Team

Scope and Methodology

Scope. We conducted our fieldwork for this evaluation from September 2010 to November 2010. The FISMA evaluation was conducted from August 2010 to November 2010 and the scope of the review consisted of the following areas that are found in “OMB Memorandum M-10-15,” for completing the OIG section of the Fiscal Year 2010 OMB FISMA questionnaire:

- Certification and Accreditation Processes and Procedures.
- Configuration Management.
- Incident Response and Reporting.
- Annual Security Awareness Training.
- Plan of Action and Milestones (POA&M) Processes and Procedures.
- Remote Access Processes and Procedures.
- Identity and Account Management.
- Continuous Monitoring.
- Contingency Planning and Testing.
- Commission Oversight of Contractor Systems.

This evaluation focused on the FISMA which requires the SEC OIG to perform an annual, independent evaluation of the agency’s information security policies, practices, and procedures. C5i conducted a review of the Commission’s IT security program (as required by the Act) based on guidance that was issued by the OMB and NIST. In order to provide OIG’s recommended responses to the OMB online tool (e.g., information security and privacy items) C5i’s review included an evaluation of the major security components for FISMA 2010.

C5i completed all data collection instruments related to FISMA 2010 and (1) Performed the necessary evaluation procedures to answer those questions to be published by OMB in its reporting guidance, (2) Compiled an Executive Summary for the SEC’s OIG, and (3) Performed a detailed security evaluation of two of the SEC’s major security components. The applicable government laws, directives, regulations, and publications pertinent in support of this evaluation include the following:

- Federal Information Systems Control Audit Manual (FISCAM);
- OMB Circular A-130 Management of Federal Information Resources;
- OMB’s FY 2007 FISMA Evaluation and Reporting Guidance;
- Computer Security Act of 1987;
- The Clinger-Cohen Act of 1996 (the Information Technology Management Reform Act);
- Federal Information Security Management Act of 2002 (FISMA);
- NIST Federal Information Processing Standards (FIPS);
- Special Publications from the NIST 800 Series;
- E-Government Act of 2002;

- OMB Memorandum M-06-16;
- SEC employees and contractors; and
- OIT policies and procedures pertinent to required areas.

Methodology. To meet the objective to complete the IG portion of the annual FISMA questionnaire, C5i conducted interviews with key personnel, made independent observations, and examined documentation provided by SEC officials. Interviews with key personnel included systems owners, business line managers, OIT representatives, and OIG personnel. These interviews were further held to garner issues that were germane to completing the OIG portion of the 2010 FISMA reporting requirement for OMB. We reviewed pertinent records and supporting documentation (such as policies, procedures, roles and responsibilities) to address the evaluation objective. Our review of policies and procedures also included discussions with SEC officials and covered the ten areas identified in the scope.

C5i staff members reviewed OIT's C&A packages, including POA&Ms, Incident Response documentation, pertinent policies and procedures, etc., to ensure compliance with FISMA, NIST, and OMB guidance. In addition to interviewing key personnel, C5i, Inc. also reviewed an extensive collection of system artifacts, policies, procedures and other documentation relating to the systems and issues identified above. Our analysis was based on all the information provided from various sources, including testimonial evidence, prior audit coverage, and documentation and artifacts provided to C5i.

Management Controls. Consistent with the audit objectives, we did not assess OIT's management control structure or its internal controls. C5i reviewed existing controls at the Commission considered specific to 2010 FISMA OIG Questionnaire (detailed above in the Scope). To thoroughly understand OIT's management controls pertaining to its policies and procedures, methods of operation, and procedures, we relied on information requested and supplied by OIT staff member and interviews we had with various OIT personnel.

Use of Computer-Processed Data. We did not assess the reliability of OIT's computers because it did not pertain to our objectives for this evaluation. Further, we did not perform any tests on the general or application controls over OIT's automated systems, as this was not in scope. The information that was retrieved from this system as well as the requested artifacts provided to us were sufficient, reliable, and adequate enough to use in meeting our stated objectives. We further reviewed the following computer processed data (e.g., Excel spreadsheets and MS Project plans) that OIT staff members provided to us:

- Hardware and software inventory to document C5i's response to Section 2, Questions 2 and 3;
- Compliance workbook detailing the status of Certification and Accreditation of SEC systems (Section 1);

- List of patches deployed on SEC systems January 1, 2010 – September 30, 2010 (Section 2);
- List of SEC Network Users with Local Administrative Access Privileges (Section 7);
- List of FDCC exceptions (Section 2); and
- HSPD-12 Implementation Plan (Section 7).

Prior Audit Coverage. C5i reviewed the *2009 FISMA Executive Summary*, Report No. 472, March 26, 2010, which had no recommendations. In the OIG report entitled, *The Evaluation of the SEC Privacy Program*, Report No. 475, March 26, 2010, all the recommendations have all been fully implemented and closed. Our review of the *Evaluation of the SEC Encryption Program*, Report No. 476, March 26, 2010 and the *Assessment of SEC's Privacy Program*, Report No. 485, September 29, 2010 found that OIT is diligently working on the recommendations. Though OIT has implemented and closed several recommendations, several recommendations are still pending and remain open.

Judgmental Sampling. C5i reviewed an Excel spreadsheet OIT staff provided us which consisted of approximately 1,000 SEC users (employees and contractors) that were identified as having indefinite local administrative privileges, as of October 31, 2010. The spreadsheet included the names of current SEC employees and contractors, the type of privilege authorized, office phone number, grade/contractor, and assigned office. We judgmentally selected names from the spreadsheet based on the type of privilege that had been granted and checked whether the users had active SEC email accounts and phone numbers. This was done to verify whether or not these personnel still worked at the Commission. We did not identify any separated/terminated SEC users.

Criteria and Guidance

OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. Provides instructions for meeting agency FY 2010 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347).

OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007). Requires agencies to develop and implement a breach notification policy. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002 (FISMA) and the Privacy Act of 1974.

OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 12, 2006). Provides updated guidance on the reporting of security incidents involving personally identifiable information and to remind you of existing requirements, and explain new requirements your agency will need to provide addressing security and privacy in your fiscal year 2009 budget submissions for information technology.

OMB Memorandum M-06-16, *Protection of Sensitive Agency Information* (June 23, 2006). Recommends actions that are needed to protect sensitive information.

OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information* (May 22, 2006). Re-emphasizes agency responsibilities under law and policy to appropriately safeguard sensitive personally identifiable information and to train employees on their responsibilities.

OMB Memorandum M-03-22, *Guidance for Implementing Privacy Provisions of the E-Government Act of 2002* (September 30, 2003). Provides information to agencies on implementing the E-Government Act of 2002 privacy provisions, signed by the President on December 17, 2002 and effective April 17, 2003.

NIST SP 800-53, Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 3. Provides details for the 18 Security Control families that are used to assess information systems and it provides guidance for implementation.

NIST SP 800-72, *Guidelines on PDA Forensics*. This guide provides an in-depth look into PDAs and explaining the technologies involved and their relationship to forensic procedures. It covers three families of devices: (1) Pocket PC, (2) Palm OS, and (3) Linux-based PDAs, and the characteristics of the devices associated operating system.

NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*. This publication provides recommendations for improving an organizations malware incident prevention measures. It also gives extensive recommendations for enhancing an organizations existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones. The recommendations address several major forms of malware, including viruses, worms, Trojan horses, malicious mobile code, blended attacks, spyware tracking cookies, and attacker tools such as backdoors and rootkits. The recommendations encompass various transmission mechanisms, including network services (e.g., e-mail, Web browsing, file sharing) and removable media.

NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*. This guide provides detailed information on establishing a forensic capability, including the development of policies and procedures. The guide's focus is primarily on using forensic techniques to assist with computer security incident response, but much of the material is also applicable to other situations.

NIST SP 800-101, *Guidelines on Cell Phone Forensics*. The objective of the guide is twofold: (1) Helps organizations evolve appropriate policies and procedures for dealing with cell phones, and (2) Prepares forensic specialists to contend with new circumstances involving cell phones, when they arise.

CMU/SEI-2003-HB-001, *Organizational Models For Computer Security Incident Response Teams (CSIRTs)*. The handbook describes different organizational models for implementing incident handling capabilities, including each model's advantages and disadvantages and the kinds of incident management services that are the best fit.

CMU/SEI-2003TR-001, *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*. Provides an objective study of the state of the practice of incident response, based on information about how CSIRTs around the world are operating. The report covers CSIRT services, projects, processes, structures, and literature, as well as training, legal, and operational issues.

CMU/SEI-2003-HB-002, *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Proposes an intrusion-aware design model called trustworthy refinement through intrusion-aware design (TRIAD). TRIAD helps information system decision makers formulate and maintain a coherent, justifiable, and affordable survivability strategy that addresses mission-compromising threats for their organization.

CMU/SEI-2004-TR-015, *Defining Incident Management Processes for CSIRTs*. Presents a prototype best practice model for performing incident management processes and functions. It defines the model through five high-level incident management processes: Prepare/Sustain/Improve, Protect Infrastructure, Detect Events, Triage Events, and Respond. Workflow diagrams and descriptions are provided for all processes.

CMU/SEI-2005-HB-001, *First Responders Guide to Computer Forensics*. The handbook is for technical staff charged with administering and securing information systems and networks and it targets a critical training gap in the fields of information security, computer forensics, and incident response.

SAND98-8667, *A Common Language for Computer Security Incidents*. Presents the results of a project to develop a common language for computer security incidents. The project results are based on the cooperation of the Security and Networking Research Group and the CERT® Coordination Center.

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.

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.

E-Government Act of 2002 (P.L. 107-347). Enacted on December 17, 2002 with an effective date of April 17, 2003, to improve the management and promotion of electronic government services and processes.

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.

List of Recommendations

Recommendation 1:

The Office of Information Technology should identify all exceptions to the Federal Desktop Core Configuration standards and submit them to National Institute of Standards and Technology within 90 days of the issuance date of this report.

Recommendation 2:

The Office of Information Technology should ensure justifications for deviations to Federal Desktop Core Configurations requirements are fully documented.

Recommendation 3:

The Office of Information Technology (OIT) should:

- 3a. Perform a thorough review and identify the universe of all Commission user accounts.
- 3b. Once the universe has been identified, OIT should then identify all “active” and “inactive” user accounts and determine whether or not the accounts should be disabled.
- 3c. Take immediate action to disable the accounts of employees and contractors who no longer work at the Commission.

Recommendation 4:

The Office of Information Technology should review policies and procedures for disabling accounts to ensure they are well-documented and thorough, and provide training to appropriate staff regarding account termination procedures.

Recommendation 5:

The Office of Information Technology should 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.

Recommendation 6:

The Office of Information Technology should conduct a full review and identify the universe of all users with elevated privileges.

Recommendation 7:

Based on the review results from recommendation 6, the Office of Information Technology should enforce or develop procedures to ensure:

- 7a. Only users whose job function require permanent elevated access have the needed privileges;
- 7b. Business justification are fully documented; and
- 7c. Elevated privileges are only issued for the finite amount of time needed to complete assigned task.

Recommendation 8:

The Office of Information Technology should maintain an accurate and current list of all users that have elevated privileges.

OIG's Response to the OMB Questionnaire

Section 1: Status of Certification and Accreditation Program

Background. Certification and Accreditation (C&A) is required by the Federal Information Security Management Act (FISMA) of 2002,¹⁴ and is the process used to evaluate systems and major applications to ensure adherence to formal and established security requirements that are well documented and authorized. All systems and applications that reside on U.S. government networks must be evaluated with a formal C&A before it is put into production. Systems are evaluated annually (referred to as "Continuous Monitoring") and are re-accredited every three years, or sooner if major changes to the systems are made. The documents that comprise a C&A package include:

- System Security Plan (SSP);
- Risk Assessment – Business and System;
- Categorization and Certification Level Recommendation;
- Hardware and Software Inventory;
- Self-Assessment;
- Security Awareness and Training Plan;
- Rules of Behavior for the End User;
- Incident Response Plan;
- Security Test and Evaluation (ST&E);
- Privacy Impact Assessment;
- Contingency Plan & Recent Test Results;
- Configuration Management Plan;
- Security Assessment Reports – Physical and Environmental, Network and Application Assessments;
- Plan of Action and Milestones (POA&M); and
- Authorization Memorandum.

In the performance of a C&A, all information systems are given a risk impact categorization based on the Federal Information Processing Standards (FIPS) Publication 199 *Standards for Security Categorization of Federal Information and Information Systems*.¹⁵ The impact level category for the system determines the scope of the C&A effort, for example, a low impact system will not be assessed as stringently as a high impact system. Information systems are categorized and

¹⁴ Federal Information Security Management Act of 2002 (Title III, Pub. L. No. 107-347), <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>.

¹⁵ Federal Information Processing Standards (FIPS) Publication 199 *Standards for Security Categorization of Federal Information and Information Systems*, <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.

designated as low, moderate, or high impact and are based on the level of adverse effect a data breach could have on an organization’s operations, assets, and personnel. If a data breach occurs on a low impact system, the impact is expected to be limited. If a data breach occurs on a moderate system, there is a more serious impact. Data breaches on high systems have a severe or catastrophic impact.

NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*¹⁶ provides control families (e.g., Access Control, Incident Response, Identification and Authentication) that are used when assessing a system for a C&A and what impact level system that apply. The examples shown below demonstrate that the control applies to Low, Medium and High impact level systems.

Example

AU-11 AUDIT RECORD RETENTION ¹⁷		
Control: The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.		
LOW AU-11	MOD AU-11	HIGH AU-11

Results of Assessment. The SEC has developed, documented, and implemented policies and procedures for their C&A program that follows NIST, OMB, and FIPS¹⁸ framework and guidance.¹⁹ We found that the SEC’s C&A process provides risk categories, has adequate risk assessments, uses the selection of appropriate controls, testing of controls are done, and regularly

¹⁶ The National Institute of Standards and Technology Special Publication 800-53, “*Recommended Security Controls for Federal Information Systems and Organizations*,” Appendix F, p. F1-F132.

¹⁷ *Id.* Appendix F, p. F-30.

¹⁸ Federal Information Processing Standard Publications 199, “*Standards for Security Categorization of Federal Information and Information Systems*”; FIPS 200, “*Minimum Security Requirements for Federal Information and Information Systems*”, The National Institute of Standards and Technology Special Publication 800-53, “*Recommended Security Controls for Federal Information Systems and Organizations*”; Special Publication 800-60, “*Guide for Mapping Types of Information and Systems to Security Categories*”, The National Institute of Standards and Technology Special Publication 800-53, “*A Guide for Assessing Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*”, The National Institute of Standards and Technology Special Publication 800-37, “*Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*,” Office of Management and Budget Circular A-130, *Appendix III, Security of Federal Automated Information Resources*.

¹⁹ SECR 24-04, *Information Technology Security Program*, October 4, 2005, OD 24-04.10 *IT Security Compliance Program*, April 12, 2006, II 24-04.10.01 *Implementing Instruction: IT Security Certification and Accreditation*, June 29, 2005, II 24-04.10.02 *Implementing Instruction: IT Security Risk Management*, December 22, 2005, II 24-04.10.03 *IT Security Assessments*, April 28, 2006, OD 24-04.10 *IT Security Compliance*, April 12, 2006.

monitors system risks and the adequacy of controls.²⁰ Our review of a C&A package found that OIT applies guidance and the best practices defined in the NIST and OMB guidance. Further, we found that authorizing officials are presented with a complete C&A package to facilitate informed system authorizations, to operate decisions based on risks and controls that are implemented. OIT staff documents deficiencies in the POA&M and tracks them for remediation.

In 2008, the Commission purchased the Department of Justice (DOJ) sponsored, web-enabled Cyber Security Assessment and Management (CSAM) tool to assist in performing and tracking all C&A activities. The CSAM tool was deployed at the Commission in March 2009. OIT uses CSAM to track system inventory, the security categorization of each information system, the status of C&A activities, weakness descriptions and remediation plans in the form of POA&M's, NIST 800-53 control assessment results, audit finding maintenance, monitoring, FISMA quarterly reports, and OIG and Government Accountability Office (GAO) audit recommendations.²¹ See screenshots of the CSAM functions OIT uses to track C&A activities in Appendix VIII.

Specific to question 1.a.1, C5i found that the Commission has documented its policies and procedures for performing C&A's. Staff's roles and responsibilities are defined and documented to ensure the process is completed and guidance from NIST standards and OMB guidance are used.²² ²³ The SEC has developed and implemented policies and procedures to establish the Commission's C&A program.²⁴

Further, C5i found through its review of artifacts provided by OIT (e.g., ST&E, POA&M, System Security Plan (SSP), and Risk Assessment) that the artifacts were consistent with guidance and best practices defined in relevant NIST standards and OMB guidance. The Commission's C&A's are performed by an independent third-party.²⁵ ²⁶

²⁰ As noted in the Assessment of SEC's Privacy Program, Report No. 485, dated September 29, 2010, C5i recommended that OIT should evaluate its risk assessment process for scoring risk to ensure that it adequately weighs all appropriate factors, including the identification of risk levels by vendors.

²¹ The National Institute of Standards and Technology Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations."

²² The National Institute of Standards and Technology's 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems"; The National Institute of Standards and Technology 800-53, "Recommended Security Controls for Federal Information Systems and Organizations"; The National Institute of Standards and Technology 800-53A, and "Guide for Assessing the Security Controls in Federal Information Systems."

²³ Office of Management and Budget Circular A-130 "Security of Federal Automated Information Resources."

²⁴ SEC Policy II 24-04.10.01 (02.0) *Implementing Instruction: IT Security Certification and Accreditation*, June 29, 2005.

²⁵ The National Institute of Standards and Technology 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems"; The National Institute of Standards and Technology 800-53, "Recommended Security Controls for Federal Information Systems and Organizations"; The National Institute of Standards and Technology 800-53A, and "Guide for Assessing the Security Controls in Federal Information Systems."

²⁶ Office of Management and Budget Circular A-130 "Security of Federal Automated Information Resources."

Response. In response to question 1 on the OMB template, based on interviews and reviews of C&A packages and as indicated above, we determined that the Commission has an established a C&A program. In addition, the SEC is maintaining a C&A program that is generally consistent with NIST's and OMB's FISMA requirements.

In questions 1.a.2 through 1.a.7, C5i found that the C&A process provides appropriate risk categories, risk assessments, the selection of appropriate controls, the testing of controls, and regular monitoring of system risks and the adequacy of controls. However, as was recommended in Report No. 485, OIT should evaluate its risk assessment process for scoring risk to ensure that it adequately weighs all appropriate factors, including the identification of risk levels by vendors.

Concerning question 1.a.8, the accreditation official is presented with complete and reliable C&A information²⁷ related to the risks and controls of the system which facilitates the authorizing office's ability to make informed decisions. All deficiencies are documented in the POA&M which contains the plan for remediation, responsible party, etc. We provided our response to question 1 as shown in Table 1 below.

Table 1: OIG Response to Question 1

ID	Questions from OMB Questionnaire	Response
1a.	The Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	Yes
1.a.1	Documented policies and procedures describing the roles and responsibilities of participants in the certification and accreditation process.	
1.a.2	Establishment of accreditation boundaries for agency information systems.	
1.a.3	Categorizes information systems.	
1.a.4	Applies applicable minimum baseline security controls.	
1.a.5	Assesses risks and tailors security control baseline for each system.	
1.a.6	Assessment of the management, operational, and technical security controls in the information system.	
1.a.7	Risks to Agency operations, assets, or individuals analyzed and documented in the system security plan, risk assessment, or an equivalent document.	
1.a.8	The accreditation official is provided (i) the security assessment report from the certification agent providing the results of the independent assessment of the security controls and	

²⁷ The accreditation official is provided (i) the security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective actions; (ii) the plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and (iii) the updated system security plan with the latest copy of the risk assessment.

	recommendations for corrective actions; (ii) the plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and (iii) the updated system security plan with the latest copy of the risk assessment.	
--	--	--

Source: OMB FISMA Web Portal

Section 2: Status of Security Configuration Management

Background. A Security 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 the 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 FDCC is an OMB mandate that requires all Federal Agencies to standardize the configuration (baseline) of approximately 300 settings on every Windows computer, agency wide. The reason for this standardization is to strengthen the federal IT's security by reducing opportunities for hackers to access and exploit government computer systems. At this time, there are no standard configuration settings for Macintosh or UNIX based operating systems, but they are reportedly under review by OMB for possible standardized configuration guidelines.

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 its software. These patches and updates are made available through the software vendor's website as they are released. Most vendors have a set day that patches are released. For example, Microsoft releases patches/updates on the 2nd Tuesday of each month. If vulnerability is considered critical, then a vendor may release patches out-of-cycle, based on the severity of the vulnerability.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organization* provides guidance to government organizations on flaw remediation, such as patching and updates. The NIST guidance provides that an organization should identify, report, and correct information system flaws; test software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and incorporate flaw remediation into the organizational configuration management process.²⁸

²⁸ The National Institute of Standards and Technology, Special Publication 800-53, Rev 3, "*Recommended Security Controls for Federal Information Systems and Organizations*," August 2009, p. F-124.

Results of Assessment. C5i determined that the Commission has developed and issued formal, written configuration management policy (implementing instructions) that addresses project configuration management.²⁹ These implementing instructions establish uniform policies, authorities, responsibilities, and procedures for IT security configuration management.³⁰ Further, the instruction identify configuration management planning as a process that is managed by the Configuration Management and Quality Assurance (CM/QA) Branch and other OIT organizations engaged in Information Technology project activities and provides a Project Configuration Management Plan template that describes configuration management activities in terms of configuration identification, baseline management, configuration control, status accounting, audits, and configuration management tools. These implementing instructions are consistent with guidance provided in NIST SP 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*.³¹

The SEC has implemented appropriate policies to perform oversight and evaluation of contractor information systems.³² The Quality Management (QM) policy “identifies the use of QM for the systematic implementation and use of planning, control, assurance, and improvement activities to align the business goals, quality objectives, and process measures. QM may involve providing information on standards, facilitating a team, or identifying and analyzing a process. Another expectation of QM is to collect measurement data and lessons learned as input to other process and product assurance management activities. QM resources act as consultants in continuous process improvement activities.” QM has specific objectives, e.g., quality planning, quality control, quality assurance, and quality improvement, helping to ensure successful implementation. Effective QM designs, develops, and implements guidance processes that assure accuracy and integrity. The OIT’s CM/QA Branch is responsible for conducting the review, control, and enforcement of the process and product assurance for IT products within OIT as well as agency-wide, to ensure quality planning and quality control are addressed.

A change request is prepared and initiated by a requester using the enterprise change control tool. The enterprise change control tool is administered by the CM/QA Branch. The information that requesters put into the change control tool generates a System Change Request (SCR). An Operations Configuration

²⁹ 24-03.01.02(01.0) *Implementing Instruction Process and Product Assurance Management Configuration Management* and 24-04.04.02 (01.1), *Implementing Instruction for IT Security Configuration Management*.

³⁰ OD 24-04.04, *IT Security Operations and Communications Security Management Program*, SECR 24-04, *Information Technology Security Program*.

³¹ The National Institute of Standards and Technology Special Publication 800-53 “*Recommended Security Controls for Federal Information Systems and Organizations*,” Appendix F-CM, pages F-38 – F46, Control Family: Configuration Management.

³² 24-1.2 *Introduction of New Technology Into the Agency*, 24-1.6 *Enterprise Architecture*, OD 24-03.01 *Process and Product Assurance Management*, OD 24-03.01.01 *Process and Product Assurance Management: Quality Management*.

Control Board (O-CCB)³³ has been established to review and approve SCR's. Members of the O-CCB include representatives from:

- Office of Applications and Software Development;
- Central Operations Branch;
- Configuration Management and Quality Control Branch (non-voting member);
- Data and Application Management Branch;
- Electronic Data Gathering, Analysis, and Retrieval System (EDGAR);
- End User Technology Branch;
- Information Security Group;
- Network Engineering Branch;
- Servers and Storage Branch; and
- Technical Assistance Center (TAC).³⁴

O-CCB members evaluate the SCR's and assess any IT security implications. Information system components such as hardware, operating system, utility, and applications, with IT security features require testing prior to the implementation of the change into the production environment, which prevent unwarranted downtime of the production environment.

When a change to an existing information system is proposed, the OIT Security Group O-CCB member conducts an impact analysis to determine the effects on the integrity and availability of the information and the information system. This analysis ensures that changes do not introduce new vulnerabilities or diminish existing IT security controls. In addition to the impact analysis, IT security testing and evaluation is conducted for all proposed changes that have IT security implications and features. Upon completion of testing and after all IT security implications are evaluated and assessed, the O-CCB approves or disapproves the proposed changes. The results of the analysis and any IT security testing and evaluation are documented within the change control tool.

In September 2010, OIT deployed the appropriate FDCC setting to all Windows-based workstations. However, some requirements were not implemented due to the incompatibility with OIT's internal applications and management's decision not to implement them.

While compliance with the FDCC standards is required by the OMB for all desktops and laptops, OMB does allow for exceptions. Per OMB Memorandum M-09-29 *FY2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*,³⁵ any and all exceptions must be documented and submitted to NIST electronically. As documented in Report, No. 485, and based on interviews conducted with OIT senior

³³ OD 24-03.01-C01 *Operations Configuration Control Board (O-CCB) Charter*.

³⁴ *Id.*

³⁵ Office of Management and Budget Memorandum M-09-29 *FY2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

management, as of February 2, 2011, OIT's exceptions list was still outstanding and OIT had not submitted it to NIST.

Our review of OIT's exceptions list found some exceptions were annotated with "management decision" as the justification for the exception. However, OIT staff could not provide us with support documentation for its decisions. For example, OIT staff informed us that the FDCC password requirement is an exception. OIT's password policy indicates passwords at a minimum must be [REDACTED] and must be changed every [REDACTED]. The FDCC requires passwords to be at a minimum 12 characters, and the password must be changed every 60 days. OIT's decision to non-comply with the FDCC's password requirement is noted on the exception report as "management decision" with no additional information.

The SEC has developed policies and procedures for patch management for their network servers, as well as workstations (e.g., desktops and laptop computer systems).³⁶ When vendors release a patch, OIT first tests the patch in its development environment to ensure the patch will not have an adverse effect on the SEC's systems. This is done by applying the patch to a test workstation or to a server and then verifying the results. OIT uses a commercial product to test patches and to deploy patches that have been successfully tested.

Once patches are tested and it is determined that they do not adversely affect the SEC's systems and applications, a "change" is then submitted to the change control board for approval. If it is determined that a patch could adversely affect the SEC's systems/applications, the security risk posed by not applying the patch is reviewed by the security group to determine if appropriate compensating controls exist, e.g., firewalls, intrusion protection etc. Once approved, patches are "pushed out" to all SEC workstations via a "group policy update" that is issued.

Administrative notices (see Appendix VIII) are sent prior to the push to ensure that SEC personnel are aware of the upcoming change to remind staff to keep their workstations powered on and connected to the network in order for their machine to be updated. For employees off-site, their machines will automatically be updated the next time they connect to the SEC network.

We found OIT has documented and incorporated guidance from NIST requirements in its policies and procedures, however, we determined that they are not always followed. For example, OIT informed us that patches for high-level vulnerabilities are generally deployed within [REDACTED] after a patch is released (OIT policy indicates high-level patches are to be deployed within [REDACTED]).

³⁶ OP 24-03.01.02.07 *Configuration Control: Change Management*, 24-05.04.03 (01.0) *Implementing Instruction: Patch Management*, 24-05.04.03.01 *UNIX Server Patch Procedure*, 24-05.04.03.02 *Windows Server Patch Installation*, and 24-05.04.03.03 *Security-Related Patch Management for Windows-based Workstations*.

[REDACTED] and patches for medium or low-level vulnerabilities are generally deployed in [REDACTED].³⁷

Further, we found significant delays in the deployment of patches. For example, Microsoft Service Pack 3 was issued by the vendor in May 2008, but was only recently deployed to the SEC's systems. NIST 800-53 guidance does not require that patching be done within a certain time frame; however it does state that "the organization promptly installs security-relevant software updates (e.g., patches, services packs, and hot fixes)."³⁸

Response. In response to question 2, C5i found that the Commission is maintaining a configuration management program with documented processes and procedures for configuration management - hardware and software inventory, change management, vulnerability scanning, and identified baseline configuration; however, improvements are needed. As a result, C5i recommended selecting 2.b.

In response to question 2.a.8, C5i found that the SEC needs to improve its documentation of deviations from FDCC requirements. In addition, as discussed in Report No. 485, the SEC does maintain a list of exceptions/deviations from the common security standards (e.g., FDCC). However, OIT has not submitted its deviations from FDCC to NIST, as required by OMB Memorandum M-09-29, "FY 2009 Reporting Instruction for the Federal Information Security Management Act and Agency Privacy Management." Additionally, OIT does not maintain supporting documentation to justify "management decisions" to deviate from FDCC standards.

Regarding question 2.a.11, C5i found that the SEC's patch management process is not fully developed and implemented. Additionally, Report No. 485 found that OIT has not applied patches in a timely and effective manner. For example, OIT applied Microsoft's XP Professional Service Pack 3 in calendar year 2010, even though Microsoft issued the patch in May 2008. In addition, OIT has applied multiple patches since November 2009; however, at the time the OIG reported to OMB for FISMA, OIT was unable to provide the exact dates when the patches were applied. As a result, C5i was unable to determine the timeliness and effectiveness of OIT's patch management process. Subsequent to the November 15, 2010 report to OMB for FISMA, OIT provided C5i a list of all of the patches applied and was able to determine that OIT's patch management is improving. However, we are unable to fully determine the effectiveness of the SEC's patch management process. We provided our response to questions 2 and 3 as shown in Table 2 below.

³⁷ OP24-05.04.03.03, Security-Related Patch Management for Window-based Workstations.

³⁸ The National Institute of Standards and Technology, Special Publication 800-53, Rev 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009, p. F-124, Control: System and Information Integrity, SI-2 Flaw Remediation.

Table 2: OIG Response to Questions 2 and 3³⁹

ID	Questions from OMB Questionnaire	Response
2b	The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.	Yes
2.a.8	<p>FDCC is not fully implemented (OMB) and/or all deviations are not fully documented.</p> <p>Comments: As was illustrated in OIG Report No. 485, the SEC does maintain a list of exceptions/deviations from the common security standards (i.e., FDCC). However, OIT has not submitted its deviations list from FDCC to NIST, as required by OMB Memorandum M-09-29, "FY2009 Reporting Instruction for the Federal Information Security Management Act and Agency Privacy Management". Additionally, OIT does not maintain supporting documentation to justify the "management decisions" used to deviate from FDCC standards.</p>	Yes
2.a.11	<p>Patch management process is not fully developed (NIST 800-53: CM-3, SI-2).</p> <p>Comments: As was noted in Report No. 485, OIT did not apply patches in a timely and effective manner. For example, the SEC's OIT applied Microsoft's XP Professional Service Pack 3 in calendar year 2010, even though Microsoft issued the patch in May 2008. In addition, OIT has applied multiple patches since November 2009; however, OIT is unable to provide the exact dates for when the patches were applied. Therefore, we are unable to fully determine the effectiveness of the SEC's patch management process.</p>	Yes
3.	<p>[REDACTED]</p>	[REDACTED]

Source: OMB FISMA Web Portal

³⁹ Table 2 does not reflect all components of question 2. The table identifies areas where OIT needs improvement.

Section 3: Status of Incident Response & Reporting Program

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 can include lost/stolen assets (laptops, Blackberry devices, etc.) or the compromise of an organizations system (unauthorized access, computer virus, etc.). NIST SP 800-53 provides the following controls regarding Incident Response:

Control Family - Incident Response⁴⁰

- 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

The goal of incident response is to handle the situation in a way that limits damage and reduces recovery time and costs. Organizations develop an incident response plan to include policies that define, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs based on the type and severity of the incident.

Organizations have a designated computer incident response team which is a carefully selected group that, in addition to security and general IT staff, may include representatives from legal, human resources, and public relations departments. The teams' roles and responsibilities are documented, defined and communicated thoroughly.

The SANS™ (SysAdmin, Audit, Network, and Security) training Institute has identified the following six steps that should be used to effectively address an incident.⁴¹

1. *Preparation:* The organization educates users and IT staff of the importance of updated security measures and trains them to respond to computer and network security incidents quickly and correctly.

⁴⁰ The National Institute of Standards and Technology's (NIST), Special Publication 800-53, Rev 3, "Recommended Security Controls for Federal Information Systems and Organizations", August 2009, Pages F-61 – F-65, Control Family: Incident Response.

⁴¹ The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. (Source <http://www.sans.org/about>).

2. Identification: The response team is activated to decide whether a particular event is, in fact, a security incident. The team may contact the Computer Emergency Response Team Coordination Center, which tracks Internet security activity and has the most current information on viruses and worms.
3. Containment: The team determines how far the problem has spread and contains the problem by disconnecting all affected systems and devices to prevent further damage.
4. Eradication: The team investigates to discover the origin of the incident. The root cause of the problem and all traces of malicious code are removed.
5. Recovery: Data and software are restored from clean backup files, ensuring that no vulnerabilities remain. Systems are monitored for any sign of weakness or recurrence.
6. Lessons Learned: The team analyzes the incident and how it was handled, making recommendations for better future response and for preventing a recurrence.

Results of Assessment. The SEC has implemented policies and procedures⁴² to address Incident Response which are well documented and address the NIST and OMB⁴³ guidance. C5i's review of the SEC's Incident Response Capability (IRC) Handbook provided evidence of the SEC's attributes for its incident response and reporting program. The SEC IRC Handbook was developed to assist in the mission of the SEC Computer Security Incident Response Team. The handbook defines processes and procedures, roles and responsibilities, types of incidents, reporting criteria and timeframes, evidence collection and handling, event categories and incident severity, etc., as well as post-mortem procedures, e.g., lessons learned.

The handbook also defines which types of incidents are required to be reported to the United States Computer Emergency Readiness Team (US-CERT) (based on OMB A-130 and FISMA) and which do not. The types of incidents that are not required to be reported are incidents that are self-inflicted, did not result in unauthorized access, or were not a result of attackers' actions. All other

⁴² OD 24-04.07 *Information Security Incident Management*, II 24-04.07.01 *Computer Security Incident Response Capability*, OP 24-04.07.01.02 *Handling Inappropriate Usage Incidents*, OP 24-04.07.01.03 *Handling of Denial of Service Incidents*, OP24-04.07.01.04 *Handling Unauthorized Access Incidents*, OP 24-04.07.01.05 *Handling Laptop Theft and Tampering Incidents*, OP 24-04.07.01.05.A01 *Laptop Theft and Tampering Incident Materials SEC Incident Response Capability Handbook*, and II 24-04.07.01.A01 *SEC Incident Response Capability Handbook*.

⁴³ Office of Management and Budget Circular A-130, *Appendix III, Security of Federal Automated Information Resources*.

incidents require reporting to US-CERT. For further detail, the Incident Escalation Flow Chart is included in Appendix VIII.

C5i found that that the Commission has incident prevention, detection, response, and reporting capabilities. This capability features a number of tools including, but not limited to:

- Archer;⁴⁴
- ArcSight Enterprise Security Manager (ESM);⁴⁵
- Encase®;⁴⁶
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

⁴⁴ Archer Incident Management centralizes and streamlines the complete case management lifecycle for cyber and physical incidents and ethics violations. Archer’s web-based solution allows the SEC to capture organizational events that may escalate into incidents, evaluate incident criticality, and assign response team members based on business impact and regulatory requirements. You can also consolidate response procedures, manage investigations end-to-end, and report on trends, losses, recovery efforts and related incidents.

⁴⁵ ArcSight delivers real-time event management with ArcSight ESM. As a key component of the ArcSight SIEM Platform, ArcSight ESM delivers “forensics on the fly,” the ability to drill down from an alert to the source events that triggered the alert. The advanced real-time correlation capability of ArcSight ESM identifies the relevance of any given event by placing it within context of who, what, where, when and why that event occurred and its impact on business risk. ArcSight ESM correlates incoming events with asset prioritization and vulnerability, user activity, and threat history to deliver accurate and automated prioritization of security risks and compliance violations. The powerful correlation engine of ArcSight ESM processes many millions of log entries down to the few critical events that matter.

⁴⁶ EnCase® Forensic is the premier computer forensic application available. It gives investigators the ability to image a drive and preserve it in a forensic manner using the EnCase® evidence file format (LEF or E01), a digital evidence container validated and approved by courts worldwide. EnCase® Forensic also contains a full suite of analysis, bookmarking and reporting features. Guidance Software and third party vendors provide support for expanded capabilities to ensure that forensic examiners have the most comprehensive set of utilities.

[REDACTED]

In addition, C5i found that local processes and procedures are based on guidance as described by NIST,⁵¹ OMB⁵² and industry best practices. The incident reporting procedures are widely used, and fully integrated into the SEC's IT management processes.

Response. In question 4, we found the SEC has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements based on the description provided above. C5i found that the SEC has documented policies and procedures for reporting incidents internally to the US-CERT and law enforcement. These policies and procedures were developed using guidance and best practices from NIST and OMB.

Concerning questions 4.a.1 through 4.a.5, as indicated above, C5i determined through interviews and documentation review that the SEC has established and is maintaining an incident response program consistent with NIST, OMB's FISMA requirements. The program consists of documented policies and procedures for reporting and responding to incidents, tracking resolution, reporting to US-CERT, and involving law enforcement when appropriate. We provided our response to question 4 as shown in Table 3 below.

[REDACTED]

The National Institute of Standards and Technology, Special Publication 800-61, Rev 1, "Computer Security Incident Handling Guide," March 2008, The National Institute of Standards and Technology Special Publication 800-72, "Guidelines on PDA Forensics," November 2004, The National Institute of Standards and Technology Special Publication 800-83, "Guide to Malware Incident Prevention and Handling," November 2005, The National Institute of Standards and Technology Special Publication 800-86, "Guide to Integrating Forensic Techniques into Incident Response," August 2006, The National Institute of Standards and Technology Special Publication 800-101, "Guidelines on Cell Phone Forensics," May 2007, Carnegie Mellon University Software Engineering Institute CMU/SEI-2003-HB-001, *Organizational Models For Computer Security Incident Response Teams (CSIRTs)*, Carnegie Mellon University Software Engineering Institute (CMU/SEI) CMU/SEI-20030TR-001, *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*, Carnegie Mellon University Software Engineering Institute CMU/SEI-20030HB-002, *Handbook for Computer Security Incident Response Teams (CSIRTs)*, Carnegie Mellon University Software Engineering Institute CMU/SEI-2004-TR-015, *Defining Incident Management Processes for CSIRTs*, Carnegie Mellon University Software Engineering Institute CMU/SEI-20050HB-001, *First Responders Guide to Computer Forensics*, Sandia National Laboratories (SAND) SAND98-8667, *A Common Language for Computer Security Incidents*, Howard and Longstaff.

⁵² Office of Management and Budget Circular A-130, *Appendix III, Security of Federal Automated Information Resources* and Memorandum M-06-19 *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 12, 2006.

Table 3: OIG Response to Question 4

ID	Questions from OMB Questionnaire	Response
4.a	The Agency has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements. 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 responding and reporting to incidents.	
4.a.2	Comprehensive analysis, validation and documentation of incidents.	
4.a.3	When applicable, reports to US-CERT within established timeframes.	
4.a.4	When applicable, reports to law enforcement within established timeframes.	
4.a.5	Responds to and resolves incidents in a timely manner to minimize further damage.	

Source: OMB FISMA Web Portal

Section 4: Status of Security Training Program

Background. Annual Cybersecurity Awareness Training is a FISMA and OMB Circular A-130, Appendix III, requirement for all federal government employees and contractors. NIST SP 800-16 *Information Technology Security Training Requirements: A Role and Performance-Based Model* provides guidance for designing a standard training program which includes good computer security practices, information on latest threats and vulnerabilities, those requiring specific role-based training, etc. Specialized training is designed for personnel with significant IT security or system administration responsibilities to enhance their knowledge and skill-sets.

Results of Assessment. OIT has developed and implemented II 24-04.03.01 *Implementing Instruction IT Security Awareness and Training Program* and Operating Directive (OD) 24-04.03 *Operating Directive IT Security Human Resources Security Program* documenting the roles and responsibilities for Security Training and documenting the requirements for SEC staff and contractors. C5i has reviewed these policies and has determined that they are thorough and incorporate NIST, FISMA, and OMB guidance, as well as Cybersecurity best practices.

In 2007, the OIT purchased the Department of State's *Cybersecurity Awareness Training Module* (Joint STATE-USAID (JSAS)). This computer based training provided standard cyber security training across the federal government and it had a tracking mechanism to provide user completion statistics. In 2010, OIT returned to using its in-house Cybersecurity Awareness training module which provided the office the ability to tailor its training. OIT's tailored training included the SEC's *Rules of the Road* to ensure employees and contractors were familiar

with not only Cybersecurity best practices, but all the SEC-specific practices for handling and protecting information. OIT takes Cybersecurity Awareness training very seriously. Personnel (employees and contractors) who do not successfully complete the training by the established deadline, risk having their access credentials frozen until the training is completed. As of November 15, 2010, 4,732 of 4,778 (99.04 percent) of SEC employees and contractors successfully completed the training. In addition, 535 of 539 (99.26 percent) of users with special roles completed the specialized “role based access training.”

Response. Concerning questions 4.a.1 through 4.a.5, as described above, based on our review of the SEC’s policies and procedures surrounding Cybersecurity Awareness Training, and completing the required training ourselves, we determined that the SEC has developed and is maintaining an appropriate training program. The program has documented and implemented policies and procedures, roles and responsibilities, training statistics are compiled and maintained to track the completion of the training, and the training content is clear and in accordance with appropriate federal guidance and industry best practices.

Below, C5i provided our response to question 5 as shown in Table 4.

Table 4: OIG Response to Question 5

ID	Questions from OMB Questionnaire	Response
5.a	The Agency has established and is maintaining a security training program that is generally consistent with NIST's and OMB's FISMA requirements. 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 security awareness training.	
5.a.2	Documented policies and procedures for specialized training for users with significant information security responsibilities.	
5.a.3	Appropriate training content based on the organization and roles.	
5.a.4	Identification and tracking of all employees with login privileges that need security awareness training.	
5.a.5	Identification and tracking of employees without login privileges that require security awareness training.	
5.a.6	Identification and tracking of all employees with significant information security responsibilities that require specialized training.	

Source: OMB FISMA Web Portal

Section 5: Status of Plans of Actions & Milestones (POA&M) Program

Background. The Plan of Action and Milestones (POA&M) is a key document in a C&A package. It is used to document identified weaknesses/vulnerabilities discovered through security control assessments, security impact analyses, and

continuous monitoring activities. A POA&M document will 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/organization.⁵³

Results of Assessment. Through interviews and reviews of the Automated Procurement System (APS) and the General Support System (GSS) POA&M's, C5i has determined that the Commission maintains an effective POA&M process. OIT effectively consolidates agency plans to correct security weaknesses found during various security reviews, including audits performed by the OIG, system certification and accreditation, GAO audits, financial system audits, and critical infrastructure vulnerability assessments. The POA&Ms are tracked using a compliance spreadsheet which allows for quarterly tracking and updates. OIT's POA&M process provides an effective roadmap for continuous security improvement, assists with prioritizing corrective action and resource allocation, and is a valuable management and oversight tool.

The SEC's POA&M process is documented and implemented through SEC Policy 24-04.10.01 (02.0) *IT Security Certification and Accreditation* and SEC Policy 24-04.10, *IT Security Compliance Program* (01.0). The POA&M process is centrally managed by OIT, and includes both Commission and contractor operated systems. The POA&M is developed by the C&A Coordinator, with assistance from the Chief Information Security Officer (CISO) and OIT Technical Liaison, and captures the decisions made regarding mitigation and/or acceptance of each of the risks enumerated in the Risk Assessment Report. The POA&M describes each risk, lists the selected mitigation (if any) and its cost (in staff or other resources), assigns responsibility for implementing the mitigation, lists the completion date for the mitigation activity, and provides justification if the risk is to be accepted. The C&A Coordinator is responsible for ensuring resources are applied to POA&M activities to meet the milestones therein. The CISO is responsible for monitoring progress of mitigation activities described in the POA&M, and for periodic security compliance reviews of all information systems.

When a security weakness is identified, program officials quickly develop, implement, and manage POA&Ms for Commission systems. They report their progress to the Chief Information Officer (CIO) on a quarterly basis, and centrally track, maintain, and review POA&M activity on a quarterly basis. In addition, OIG recommendations are routinely incorporated into the POA&M process, and the POA&M process effectively prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner, and the appropriate resources are received. OIT staff member's track POA&M's by using the DOJ sponsored CSAM application tool. DOJ externally host the tool and OIT has used it since March 2009. Screenshots of the various CSAM functions used by OIT for tracking POA&M's can be found in Appendix VIII.

⁵³ The National Institute of Standards and Technology, Special Publication 800-53, Rev 3, "*Recommended Security Controls for Federal Information Systems and Organizations*," August 2009.

While OIT is no longer required to submit quarterly updates of its POA&M's, the office has made quarterly updates its standard procedure to ensure timely remediation and the closure of POA&M findings.

Response. Concerning questions 6.a.1 through 6.a.6, as described above, OIT has established and is maintaining a POA&M program that is generally consistent with NIST and OMB's FISMA requirements to track and monitor known information security weaknesses. OIT has developed policies and procedures documenting the roles and responsibilities of staff for the C&A process as it pertains to POA&M's. Weaknesses documented on a POA&M are documented and may include vulnerability description, responsible party, severity of weakness, plan and timeline of remediation, and responsible party. POA&M items are tracked using CSAM and OIT staff performs quarterly updates to ensure the accuracy of the POA&M. We provided our response to question 6 as shown in Table 5 below.

Table 5: OIG Response to Question 6

ID	Questions from OMB Questionnaire	Response
6.a	The agency has established and is maintaining a POA&M program that is generally consistent with NIST's and OMB's FISMA requirements 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
6.a.1	Documented policies and procedures for managing all known IT security weaknesses.	
6.a.2	Tracks, prioritizes and remediates weaknesses.	
6.a.3	Ensures remediation plans are effective for correcting weaknesses.	
6.a.4	Establishes and adheres to reasonable remediation dates.	
6.a.5	Ensures adequate resources are provided for correcting weaknesses.	
6.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.	

Source: OMB FISMA Web Portal

Section 6: Status of Remote Access Program

Background. 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/contractors, and others who are not permanently based at a facility.

Establishing a remote connection requires internet access and, for network/account security reasons, should require multi-factor authentication – a user name, personal identification number (PIN) and passcode from a secure token to establish connection to the network, followed by the users account domain user name and password to access applications and/or workstations.

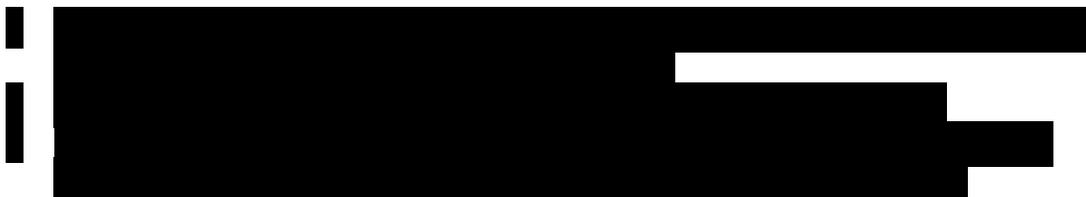
NIST SP 800-53 provides specific guidance for remote access in the Access Control section. It specifically states:

The organization:

- Documents allowed methods of remote access to the information system;
- Establishes usage restrictions and implementation guidance for each allowed remote access method;
- Monitors for unauthorized remote access to the information system;
- Authorizes remote access to the information system prior to connection; and
- Enforces requirements for remote connections to the information system.⁵⁴

Results of Assessment. The SEC has documented policies and procedures surrounding remote access (authorization, monitoring, and controlling): Operating Procedure (OP) 24-04.06.03.02 *Security Configuration of Remote Access* and OP 24-04.06.03.04 *SecurID Token Assignment* and 24-04.06.03.02.T01 *Remote Access Checklist* as well as the *SEC Rules of the Road*, which outline user roles and responsibilities in securely accessing systems remotely.

Accessing SEC systems remotely can be performed in the following ways:



Accessing email [REDACTED] allows the user to read and respond to their email, but does not allow the users to access any SEC internal systems, i.e., intranet or other SEC applications (HUB, Momentum). That access is available only via login to [REDACTED]. All remote access at the SEC requires multi-factor authentication – user name, RSA token⁵⁵ [REDACTED], as well as a network password is required. As a security measure for remote access, all remote sessions will terminate after [REDACTED] of inactivity. This helps to protect the system from unauthorized access if a user leaves their workstation unattended for a period of time. Once a session has terminated, the user will have to re-authenticate to resume their remote session.

⁵⁴ The National Institute of Standards and Technology, Special Publication 800-53, Rev 3, “*Recommended Security Controls for Federal Information Systems and Organizations*,” August 2009, p. F-14, Control: Access Control, AC-17 Remote Access.

⁵⁵ An RSA token or SecurID is a two-factor authentication mechanism.

Through interviews conducted, we found that OIT documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method. All users who need remote access must complete and submit the Rules of Behavior for Remote Access. This document must be approved in writing by the user, users' supervisor, and Information System Security Officer. The approved document is delivered to the OIT Security for processing.

The SEC requires that sensitive files transmitted across public networks or are stored on mobile devices and removable media such as compact discs and flash drives, to be encrypted. OIT implements information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Firewalls and routers are used to restrict information flows between GSS and interconnected systems. The SEC implements flow control through user roles, Secure Sockets Layer (SSL) connections, and individual accounts.

Underlying network protocols provide confidentiality and integrity protection, as do higher-layer cryptographic mechanisms (such as SSL for client/server communications). Application components are segregated, and each segment of the system is located on a single server. The GSS supports authorized remote login to the SEC's networks via the virtual private network and Citrix, both of which provide encryption during transmission over the internet.

Response. Concerning questions 7.a.1 - 7.a.7, the SEC has well documented and communicated remote access policies and procedures that comply with NIST and OMB guidance for identification and multi-factor authentication, protection of the information via encryption, firewalls, and monitoring remote connections. Our response to question 7 is shown in Table 6 below.

Table 6: OIG Response to Question 7

ID	Questions from OMB Questionnaire	Response
7.a	The Agency has established and is maintaining a remote access program that is generally consistent with NIST's and OMB's FISMA requirements. 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 authorizing, monitoring, and controlling all methods of remote access.	
7.a.2	Protects against unauthorized connections or subversion of authorized connections.	
7.a.3	Users are uniquely identified and authenticated for all access.	
7.a.4	If applicable, multi-factor authentication is required for remote access.	
7.a.5	Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.	
7.a.6	Requires encrypting sensitive files transmitted across public networks or stored on mobile devices and removable media such as CDs and flash drives.	
7.a.7	Remote access sessions are timed-out after a maximum of 30 minutes of inactivity after which re-authentication is required.	

Source: OMB FISMA Web Portal

Section 7: Status of Account and Identity Management Program

Background. Account and Identity Management is the process of 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, etc.).

For physical access, an ID badge or cardkey are the most common forms; however biometrics are also used. The badge generally has a photograph of the individual and their location of employment. The badge also has a serial number assigned to it that is entered into the access system with the name of the assignee when issued. The badge is then 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 datacenter or secure operations center would only be granted to those individuals who work in that area.

For logical access, users are given a unique identifier, usually their first initial and last name – that will be used to access computers, networks, and/or applications based on the individuals role. For both logical and physical access, organizations have developed their own processes and procedures to communicate to the various areas (security and network operations) the level of

access an individual will require. This is usually handled through an electronic request or form generated by the supervisor.

In August, 2004, Homeland Security Presidential Directive-12 (HSPD-12) *Policies for a Common Identification Standard for Federal Employees and Contractors* 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"⁵⁶ for physical and logical access.

*There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. In order to eliminate these variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification.*⁵⁷

Results of Assessment. Through our interviews and reviews, C5i found that the SEC has established an entity-wide Account and Identity Management program that is generally consistent with NIST and OMB's FISMA requirements.⁵⁸ Below are procedures provided to the IT specialist and/or administrative specialist at the SEC to establish physical and logical access.

Logical Access

The procedures for establishing, terminating, or modifying a Local Area Network (LAN) account are documented in SEC Operating Procedure 24-05.01.02.02 *LAN Account Creation, Modification, Termination, and Transfer*. All requests for creating new accounts, making account modifications (name change, change in access levels, etc.), and the termination of accounts are handled by completing the OP Template 24-05.01.02.T01 *Request for Account Creation, Modification, Termination, or Transfer*. Pertinent IT specialists or the office/division's administrative contact is responsible for completing and submitting the form to the TAC, LAN account management group. Once approved, the TAC will set-up an account for the user (based on the request) and provide the user with access

⁵⁶ Homeland Security Presidential Directive-12, August 27, 2004, Section 3.

⁵⁷ HSPD-12 Abstract, Source: http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm

⁵⁸ Federal Information Processing Standard Publication 201-1 *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006, The National Institute of Standards and Technology, Special Publication 800-73-1 *Interfaces for Personal Identity Verification*, March 2006, The National Institute of Standards and Technology, Special Publication 800-76-1 *Biometric Data Specification for Personal Identity Verification*, January 2007, The National Institute of Standards and Technology, Special Publication 800-79 *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, July 2005.

credentials (e.g. user name and temporary password) which the user will be prompted to change upon their first login. When a user receives login credentials, if requested they will also receive their RSA token for remote access and the instructions on how to activate the token, set-up the PIN, and remote access procedures.

Access to SEC specific applications (e.g., HUB, Momentum, etc.) is handled by individual office/division application system owners and is based on the users' role in the SEC. LAN accounts are also created for contractors working at the SEC and are requested and authorized by the Contacting Office Technical Resource (COTR) for each specific contract. Each month OIT staff conducts an audit of user accounts that are not active for SEC employees and contractors. An IT specialist reviews the list of the inactive employee accounts and designated COTRs are sent a list of inactive accounts for assigned contractors. The TAC is advised about the status of the list.

Accounts that are inactive for [REDACTED] are put into a "dormant" status and the user will only be able to log in only to emails. Only the TAC can fully reactivate dormant accounts. Accounts having no activity for [REDACTED] are disabled. Though the user's name still appears on the system, the user cannot log into the network. Once an account is inactive for [REDACTED], an IT specialist is contacted to determine whether to keep the account in a disabled status or delete it. A good reason an IT specialist should not delete an account would be the determination to continue monitoring a person's emails. Account terminations are handled in the exact same manner as when an account is established. The account is disabled on the user's (employee or contractor's) date of separation, as documented by the IT specialist or administrative contact. In the event of involuntary terminations, the TAC and OIT security are immediately notified and the account is terminated.

Through a separate audit performed by the SEC ICFR group, it was discovered that active directory accounts for 14 separated employees were not terminated, and two of those accounts were identified as being logged into after the employees' termination dates.⁵⁹ Login credentials that are not properly disabled at the time of separation/termination of a user pose a serious security risk. The credentials can be used by a malicious party to gain access to sensitive SEC data and compromise the system. If the terminated/separated user had elevated privileges, e.g., local administrative rights, there would be an even greater threat of serious compromise or damage to the SEC data/network due to the higher level of access.

The level of access given to a user is specific to their job function and is known as "least privilege." Least privilege is defined by NIST SP 800-53 as "allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with

⁵⁹ SEC A-123 FY 2010, Notification of Finding and Recommendation GSS-NFR 08.

organization missions and business functions.”⁶⁰ We found there are a large number of users at the SEC who have escalated privileges, specifically local administrative access⁶¹ on a permanent basis, but whose job function does not necessarily require that function. Having local administrative access allows users to install software on their computer without any oversight of OIT and make configuration changes, etc. It is also a significant risk to SEC systems if the user’s account is compromised by a malicious party, as they will have the ability to infiltrate further into the network. There are reasons for granting temporary admin access, e.g., 90 minutes, to perform a function such as installing Cyberscope to perform OMB reporting, but this privilege should have a finite timeframe.

The HSPD-12 program referenced earlier in this section applies not only to physical access, but is also intended for logical access. When the program is fully implemented, personnel will not be able to access information systems – network, email, etc., without their card scanned and input of their specific HSPD-12 password. This is a different password than the current network and application passwords that employees use.

In order for this to be implemented, the card issuance must be completed and the acquisition of the equipment completed and deployed. For users who do not work in the field or remotely, their system will be equipped with either a keyboard with a card scanner or a scanner that connects to their equipment via USB port. However, there are users at the SEC (employees and contractors) who are not located at SEC offices who always access the SEC systems remotely, and those solutions are not feasible. OIT is currently researching solutions for the remote issues.

Physical Access

The current badge process for employees and contractors is to complete the pertinent forms – personal data form, release of credit, etc. In order for the forms to be processed, they must be sponsored. Employees and contractors requiring access for a period greater than six months must get a PIV card. This employee/contractor's name must be provided by an Office of Human Resources (OHR) Talent Management for new employees or the payroll system for current employees. Contractor requests come from the COTR. Both OHR and the COTR are responsible for getting the documents and providing them to OHR Personnel Security for the individual to be sponsored. Once sponsored, OHR Personnel Security will review the Office of Personnel Management’s Personnel Investigation Processing System's application to verify if the person has a

⁶⁰ The National Institute of Standards and Technology, Special Publication 800-53, Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, p. F-9, Control: Access Control, AC-6, Least Privilege.

⁶¹ Local Administrative access provides users with higher privileges on their workstations than normal users. This level of privilege allows the user to perform functions, such as installation of third party software, removing or turning off settings, e.g., forced encryption, etc.

background investigation on record that meets the SEC's minimum requirements. If they do, the file is adjudicated and the employee is approved for a badge. If not, then the employee/contractor's fingerprints are sent to the FBI for verification and then the adjudicator reviews the results and sends out the rest of the documentation to complete the cross agency verification. Once all results are received, the adjudicator reviews the information and makes a determination for suitability for employment at the agency. Once the person has been successfully adjudicated then the person is authorized to get their badge and obtain access to the SEC network.

All access badges are programmed with access privileges based on the individual roles and responsibilities. NIST SP 800-53 provides guidance on physical access authorization and control.

Physical Access Authorizations - The organization:

- a. Develops and keeps current a list of Personnel with authorized access to the facility where the information system resides) except for those areas within the facility officially designated as publicly accessible);
- b. Issues authorization credentials; and
- c. Reviews and approves the access list and authorization credentials, removing from the access list personnel no longer requiring access.⁶²

Physical Access Control - the organization:

- a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);
- b. Verifies individual access authorizations before granting access to the facility;
- c. Controls entry to the facility containing the information systems using physical access devices and/or guards;
- d. Controls access to areas officially designated as publicly accessible in accordance with the organizations assessment of risk;
- e. Secures keys, combinations, and other physical access devices;
- f. Inventories physical access devices; and
- g. Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.⁶³

The SEC is currently implementing the HSPD-12 card rollout through an interagency agreement with the General Services Administration (GSA) for the

⁶² The National Institute of Standards and Technology, Special Publication 800-53, Rev 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009, p. F-76, Control: Physical and Environmental Protection, PE-2 Physical Access Authorizations.

⁶³ *Id.* at p. F-77

express purposes of using the GSA HSPD-12 Shared Services Solution, consisting of Enrollment/Activation Stations for sending data (i.e., scanned fingerprint images with authentication information) to request issue of Personal Identity Verification (PIV) credentials, also referred to as an HSPD-12 card. The SEC selected the GSA Shared Service solution because the cost to acquire the technology to support the program would have been expensive. In addition, the GSA Shared Service solution provided the equipment, personnel, and has already acquired the equipment and technology needed to implement the program. Further, the GSA Shared Service solution had completed a certification and accreditation of its system.

For an employee or contractor that requires an HSPD-12 badge, the employee/contractor is sponsored into the GSA USAccess system for the processing of the card, and if needed, a background investigation is initiated – this applies to employees and contractors. Once the investigation is successfully completed, the individual will receive notification that they can begin the enrollment process for their card. This notification includes instructions on how to register for the enrollment, locations and hours, and the ability to schedule the appointment.

As of the date of our interviews (September 20, 2010), the initial card rollout was estimated to be completed by September 30, 2010. However, the date has since been revised to June 30, 2011 and this change was reported to OMB.

Response. Concerning question 8b, C5i found that the SEC has implemented and is maintaining an Identity and Access management program that has documented policies and procedures; however through our interviews and review, we found three areas of improvement:

In response to question 8.a.7, C5i found that logical accounts are not properly terminated when users no longer require access. In addition, we found that the SEC's Internal Control for Financial Reporting group identified Active Directory (AD) network accounts for separated/terminated employees have not been disabled in a timely manner. Specifically, it was found that 14 separated SEC employees AD network accounts had been disabled. Two of these employees AD network accounts were identified as having been logged into after the employee's SEC termination date and a disabled AD account was identified as being logged into after another SEC employee's terminated date.

In response to question 8.a.9, C5i found that the SEC has not adequately planned for implementation of PIV for Logical Access. In addition, we found that the SEC has not completed its rollout of the PIV badge to all employees and contractors, as required by the HSPD-12 directive. As a result, all employees and contractors are not utilizing the PIV badge for physical access and logical access. Further, a complete rollout of technology to support the PIV program has not been completed.

Regarding question 8.a.10, C5i found that privileges granted are excessive or result in capability to perform conflicting functions. Additionally, we found that the SEC has an excessive number of persons who have been granted administrative access on a permanent basis but whose job function may not require this level of privilege on an indefinite basis. We provided our response to question 8 as shown in Table 7 below.

Table 7: OIG Response to Question 8

ID	Questions from OMB Questionnaire	Response
8.b	The Agency has established and is maintaining an account and identify management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below. If b. checked above check areas that need significant improvement:	Yes
8.a.7	Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2). Comments: The SEC's Internal Control for Financial Reporting group identified Active Directory (AD) network accounts for separated/terminated employees have not been disabled in a timely manner. Specifically, it was found that 14 separated SEC employees AD network accounts had been disabled. Two if these employees AD network accounts were identified as having been logged into after the employee's SEC termination date and a disabled AD account was identified as being logged into after another SEC employee's terminated date.	Yes
8.a.9	Agency has not adequately planned for implementation of PIV for logical access (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, and OMB M-08-01). Comments: The SEC has not completed its rollout of the PIV badge to all employees and contractors, as required by the HSPD-12 directive. As a result, all employees and contractors are not utilizing the PIV badge for physical access and logical access. Further, a complete rollout of technology to support the PIV program has not been completed.	Yes
8.a.10	Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, and AC-6). Comments: The SEC has an excessive number of persons who have been granted administrative access on a permanent basis but whose job function may not require this level of privilege on an indefinite basis.	Yes

Source: OMB FISMA Web Portal

Section 8: Status of Continuous Monitoring Program

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 missions/business processes. Network vulnerability assessments, Intrusion Detection System (IDS), Intrusion

Prevention System (IPS), and C&A are all components of a continuous monitoring program. NIST SP 800-53 provides guidance on continuous monitoring, specifically:

Security Assessment and Authorization, 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 systems 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;
- d. Reporting the security state of the information system to appropriate organizational officials;
- e. Employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis; and
- f. Plans, schedules, and conducts assessments to ensure compliance with all vulnerability mitigation procedures.⁶⁴

Results of Assessment. Through interviews and documentation review, C5i found that the SEC has an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST and OMB's FISMA requirements; however, improvements need to be made. Specifically, OIT's continuous monitoring procedures should be improved to provide sufficient detail regarding when patches have been implemented. In addition, patches are not applied in a consistent manner as noted in Report No. 485. C5i noted that the SEC documented many policies addressing the various facet of continuous monitoring.

- *Patch Management: 24.05.04.03.01 UNIX Server Patch Management, 24.05.04.03.02 Windows Server Patch Installation, 24.05.04.03.03 Security-Related Patch Management for Windows-based Workstations*
- *C&A: 24-04, Information Technology Security Program, 24-04.10 IT Security Compliance Program, Implementing Instruction: IT Security Certification and Accreditation, 24-04.10.02 Implementing Instruction: IT Security Risk Management.*

⁶⁴ The National Institute of Standards and Technology, Special Publication 800-53, Rev 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009, page F-37, Control: Security Assessment and Authorization, CA-7 Continuous Monitoring.

As noted in the Section 1 of this report, C5i found that the SEC C&A process adequately provides appropriate risk categories, adequate risk assessments, selection of appropriate controls, adequate testing of controls, and regular monitoring of system risks and the adequacy of controls.

OIT is responsible for performing monthly vulnerability scans on the SEC network, as well as performing IDS and IPS functions. For vulnerability scanning, the SEC recently upgraded their vulnerability scanning tool from [REDACTED], both are commercial-off-the-shelf products and are widely used in government and commercial enterprises. For intrusion prevention and detection, OIT uses [REDACTED] as its [REDACTED], and [REDACTED] as its [REDACTED].

OIT has documented policies and procedures for Patch Management; however, as previously mentioned in the SEC OIG's Assessment of the SEC's Privacy Program Report⁶⁵ and in Section 2 of this report, patches are not being deployed in a timely manner and OIT is unable to provide documentation and/or evidence of when a patch was actually deployed. Moreover, as noted in Section 2 of this report, SEC patching policies and procedures are not being fully adhered to and there is insufficient documentation supporting the implementation of patches.

Response. In response to question 9.a.2, C5i found that the SEC's continuous monitoring procedures are not fully developed or consistently implemented. Also, C5i found that OIT's continuous monitoring procedures do not provide sufficient detail regarding when patches have been implemented. In addition, patches are not applied in a consistent manner as noted in the Report No. 485. Concerning question 9b, C5i found that the SEC has established an agency-wide continuous monitoring program to assess, however improvement is needed. We provided our response to question 9 as shown in Table 8 below.

⁶⁵ SEC OIG *Assessment of SEC's Privacy Program*, Report No. 485, September 29, 2010.

Table 8: OIG Response to Question 9

ID	Questions from OMB Questionnaire	Response
9b	The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.	Yes
	If b. checked above, check areas that need significant improvement	
9.b.2	Continuous monitoring procedures are not fully developed, sufficiently detailed, or consistently implemented.	Yes
	Comments: OIT's continuous monitoring procedures do not provide sufficient detail for when patches have been implemented. In addition, patches are not applied in a consistent manner as noted in the OIG's Report No. 485.	

Source: OMB FISMA Web Portal

Section 9: Status of Contingency Planning Program

Background. Continuity of Operations/Disaster Recovery (COOP/DR) is the processes, policies and procedures for re-establishing operations for an enterprise after a man-made or natural disaster. These procedures include, but are not limited to: re-activation of systems; communication to personnel; alternate work location for personnel; roles and responsibilities; and utilities (telecommunications, power, water). NIST SP 800-53 provides guidance on with a specific control for Contingency Planning which includes:

- 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: Telecommunications Service
- CP-9: Information Service Backup
- CP-10 Information system Recovery and Reconstitution⁶⁶

Organizations perform tests of their disaster recovery plans, usually bi-annually, to ensure the full functionality of the plan and the fail-over systems, and document any problems for remediation.

Results of Assessment. C5i found that the SEC has established and is maintaining an entity-wide business COOP/DR that is consistent with NIST, FISMA, and OMB requirements; as well is consistent with the Federal Continuity Directive⁶⁷ (FCD) for developing continuity plans and programs. OIT has

⁶⁶ The National Institute of Standards and Technology, Special Publication 800-53, Rev 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009, p. F-47, Control: Contingency Planning.

⁶⁷ Federal Continuity Directive (FCD), *Federal Executive Branch Continuity Program and Requirements*, February 2008.

developed and implemented OIT-00047-001.0 *Disaster Recovery Planning Procedures*, 24-04.09 *IT Security Business Continuity Management Program*, SEC Implementing Instruction 24-04.09.01 (02.0) *System Business Impact Analysis*, and OIT-00003-001.0 *Disaster Recovery Planning Policy* to provide the authority and guidance necessary to reduce the impact of a disruptive event or disaster. These documents were reviewed and are compliant with appropriate Federal guidance.

C5i found that the SEC's continuity planning facilitates the performance of essential functions during all-hazards, emergencies and other situations that may disrupt normal operations. The COOP/DR plans are used to conduct assessments and track system performance at all times and under all conditions, to include natural disasters, man-made incidents, terrorism, and war. Further, C5i found that the SEC COOP/DR program meets the requirements of the FCD. FCD 1⁶⁸ requires that essential functions be performed continuously following a disaster, national emergency or other emergency event, or continuity of operations; and disaster recovery plan procedures must support their resumption within 12 hours or less after an event. In addition, COOP/DR capabilities must support continued performance of the functions for up to 30 days or until normal operations can be resumed. Given the requirements and parameters established in FCD 1, the Recovery Time Objectives for SEC applications are as follows:

- Applications supporting SEC Primary Missions Essential Functions (PMEF) - [REDACTED];
- Applications supporting SEC Mission Essential Functions (MEF) - [REDACTED]; and
- All other applications - [REDACTED].

The critical activities that are performed by the SEC, especially after a disruption of normal activities, are divided into three categories of essential functions: National Essential Functions (NEF), PME F, and MEF. The SEC Office of the Executive Director (OED) has completed an analysis of its systems and has identified them according to the essential functions they perform. The specific Federal government and SEC requirements requiring and defining the performance of business continuity and disaster recovery are contained in the policy and procedural references:

- Federal Continuity Directive 1 (FCD 1), *Federal Executive Branch Continuity Program Requirements*, February 2008;
- Operating Directive (OD) 24-04.09 *IT Security Business Continuity Management Program*; and
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30; *Risk Management Guide for Information Technology Systems*, July 2002.

⁶⁸ Federal Continuity Directive 1 (FCD 1), *Federal Executive Branch Continuity Program and Requirements*, February 2008, p. 1.

C5i verified that the agency has developed and performed an overall Business Impact Assessment (BIA) process. BIAs must be completed for all systems currently designated by the SEC as applications reportable under FISMA. In addition, BIAs must be completed for any new applications, which will be reportable under FISMA, and during the system's design phase. The BIA for the "Tips, Complaints, and Referrals Repository" system, dated March 12, 2010 was reviewed.

The specific Federal government and SEC requirements requiring and defining the performance of BIAs are contained in the policy and procedural references: SEC Implementing Instruction *24-04.09.01 (02.0)*, *System Business Impact Analysis*, and NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

C5i found that the SEC performs the development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures. It was confirmed that contingency planning and disaster recovery exercises were performed in April and November 2010, which included the fail-over test results. An "Exercise After Action" report is prepared once the exercise is completed to include full documentation of the outcome of each phase of the exercise and includes "lessons learned" for issues or problems that occurred.

The SEC continues the performance of regular ongoing testing and exercising of its continuity/disaster recovery plans to determine their effectiveness and to maintain current plans. C5i has verified that the Critical systems have alternate processing sites and the training, testing, and exercises have been developed.

Response. Concerning questions 10.a.1 through 10.a.7, C5i found that the SEC has an entity-wide disaster recovery program that includes documented policies and procedures in compliance with federal guidance. Testing of the plan is conducted twice per year with results documented. We provided our response to question 10 as shown in Table 9 below.

Table 9: OIG Response to Question 10

ID	Questions from OMB Questionnaire	Response
10.a	The Agency established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	Yes
10.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.	
10.a.2	The agency has performed an overall Business Impact Assessment.	
10.a.3	Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.	
10.a.4	Testing of system specific contingency plans.	
10.a.5	The documented business continuity and disaster recovery plans are ready for implementation.	
10.a.6	Development of training, testing, and exercises (TT&E) approaches.	
10.a.7	Performance of regular ongoing testing or exercising of continuity/disaster recovery plans to determine effectiveness and to maintain current plans.	

Source: OMB FISMA Web Portal

Section 10: Status Agency Program to Oversee Contractor Systems

Background. Outside contractors play an integral role in the federal government operations, as well as in commercial enterprises. Contractors can provide a wide range of services 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 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.

Results of Assessment. C5i found that the SEC ensures that contractors or other entities of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. Interviews were conducted with several persons responsible for managing and administering the SEC's information systems security program, and a review of policies and procedures provided by OIT to verify compliance. C5i also determined that the SEC has implemented appropriate policies 24-1.2 *Introduction of New Technology Into the Agency*, 24-1.6 *Enterprise Architecture*, OD 24-03.01 *Process and Product Assurance Management*, OD 24-03.01.01 *Process and Product Assurance Management: Quality Management* to perform oversight and evaluation of contractor information systems.

C5i found that there are detailed procedures developed, documented, and effectively implemented to reduce risks from outsourced services by contractors of the agency, or other organization(s) on behalf of the agency, that explicitly address the need for effective security controls at the service provider.

The SEC performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency, or other organization(s) on behalf of the agency, meet the requirements of FISMA, OMB, and NIST guidelines, as well as National Security Policy. Further, OIT maintains an inventory (Excel spreadsheet) of major information systems, including systems operated by contractors on the agencies behalf. The system inventory was reviewed and is well documented with the name of the system, system owner, and whether or not the system is SEC operated or operated by a contractor on behalf of the commission. The SEC authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve the information system interconnection agreements, Security Plans and procedures to verify reduction of risk of introducing a security flaw or breach to the organization.

These agreements are comprehensive and include detailed information regarding the purpose of the connection, the responsibilities of each party, a description of the systems or networks to be interconnected, procedures for responding to security incidents, disaster and contingency plans, funding considerations, and numerous administrative details. As part of our review, we examined Memoranda of Understanding (MOU's) and an Interconnection Security Agreement (ISA) between the SEC and DOJ, Department of Interior, and other government and contractor entities, that meet the requirements of NIST guidelines and OMB's FISMA requirements.

Response. In response to question 11, C5i found that the SEC has established and maintains a program to oversee systems operated on its behalf by contractors. Concerning questions 11.a.1 through 11.a.6, C5i found that the SEC has established and is maintaining a program to oversee systems operated on its behalf by contractors and/or other entities. There are documented policies and procedures that comply with NIST, FISMA, and OMB guidance. Based on information provided by OIT, but not verified by C5i through testing, an inventory of systems is maintained and kept up to date by OIT. All interfaces are identified and MOU's and ISA's are in place. We provided our response to question 11 as shown in Table 9 below.

Table 10: OIG Response to Question 11

ID	Questions from OMB Questionnaire	Response
11.a	The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:	Yes
11.a.1	Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities and that the Agency obtains sufficient assurance that security controls of systems operated by contractors or others on its behalf are effectively implemented and comply with federal and agency guidelines.	
11.a.2	A complete inventory of systems operated on the Agency's behalf by contractors or other entities.	
11.a.3	The inventory identifies interfaces between these systems and Agency-operated systems.	
11.a.4	The agency requires agreements (MOUs, Interconnect Service Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.	
11.a.5	The inventory, including interfaces, is updated at least annually.	
11.a.6	Systems that are owned or operated by contractors or entities are subject to and generally meet NIST and OMB's FISMA requirements.	

Source: OMB FISMA Web Portal

MEMORANDUM

TO: H. David Kotz, 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 Report, *2010 Annual FISMA Executive Summary Report, Report No. 489*

DATE: February 25, 2011

This memorandum is in response to the Office of Inspector General's (OIG) Draft Report No. 489 entitled, *2010 Annual FISMA Executive Summary Report*. Thank you for the opportunity to review and respond to this report.

OIG Recommendations:

The draft report had eight recommendations:

Recommendation 1: *The Office of Information Technology should identify all exceptions to the Federal Desktop Core Configuration standards and submit them to National Institute of Standards and Technology within 90 days of the issuance date of this report.*

OIT concurs with this recommendation and has initiated actions to address within 90 day.

Recommendation 2: *The Office of Information Technology should ensure justifications for deviations to Federal Desktop Core Configurations requirements are fully and adequately documented.*

OIT concurs with this recommendation and has initiated actions to address.

Recommendation 3: *The Office of Information Technology (OIT) should:*

- a. Perform a thorough review and identify the universe of all Commission user accounts.*
- b. Once the universe has been identified, OIT should then identify all "active" and "inactive" user accounts and determine whether any accounts should be disabled.*
- c. Then take immediate action to disable the accounts of employees and contractors who no longer work at the Commission.*

OIT concurs with this recommendation and has initiated actions to address.

Recommendation 4: *The Office of Information Technology should review their policies and procedures for disabling accounts to ensure they are well-documented and thorough, and provide training to appropriate staff regarding account termination procedures.*

OIT concurs with this recommendation and has initiated actions to address.

Recommendation 5: *The Office of Information Technology should complete the logical access integration of the HSPD-12 card no later than December 2011, as reported to the Office of Management Budget on December 31, 2010.*

OIT concurs with this recommendation and will take the most cost-effective measures to implement logical access control utilizing the HSPD-12 cards. If the financial situation dictates, we may revise the date committed to OMB.

Recommendation 6: *The Office of Information Technology should conduct a full review and identify the universe of all users with elevated privileges.*

OIT concurs with this recommendation and has initiated actions to address.

Recommendation 7: *Based on the review results from recommendation 6, the Office of Information Technology should enforce or develop procedures to ensure:*

- a. *Only users whose job function require permanent elevated access have the needed privileges;*
- b. *Business justification are fully documented; and*
- c. *Elevated privileges are only issued for the finite amount of time needed to complete assigned task.*

OIT concurs with this recommendation and has initiated actions to address.

Recommendation 8: *The Office of Information Technology should maintain an accurate and current list of all users that have elevated privileges.*

OIT concurs with this recommendation and has initiated actions to address.

OIG Response to Management's Comments

We are pleased that OIT concurred with the report's recommendation and has initiated actions to address the issues described in the report. We believe that full implementation of these recommendations will act to strengthen the SEC's information security systems.

Screenshots

Figure 1: SEC Administrative Notice, Issued 11/23/2010



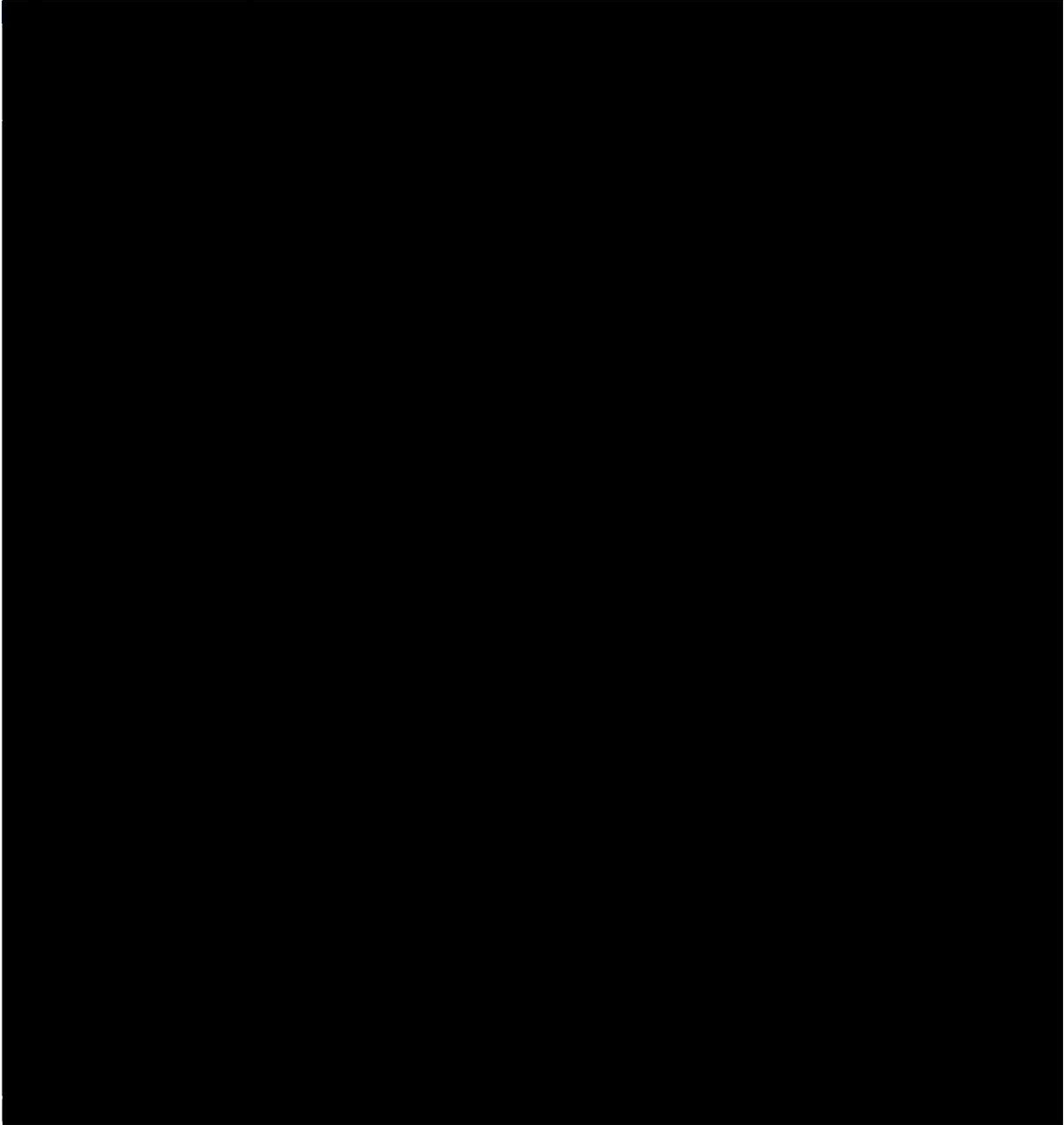
Source: SEC Email from OIT

Figure 2: CSAM Home Page



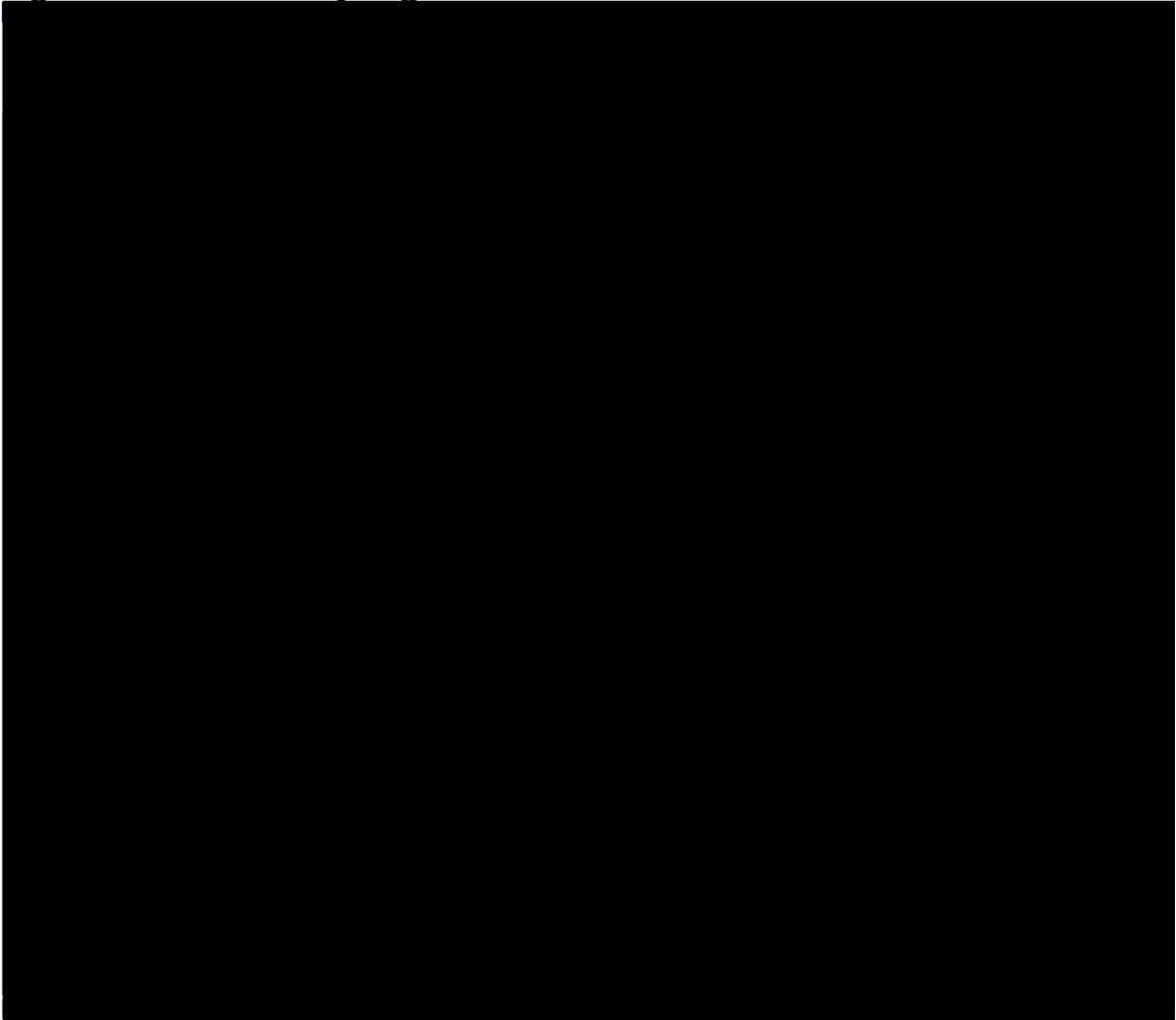
Source: Generated by CSAM

Figure 3: Inventory of GAO POA&Ms



Source: Generated by CSAM

Figure 4: POA&M Entry Page



Source: Generated by CSAM

Figure 5: POA&M Page



Source: Generated by CSAM

Figure 6: Incident Escalation Flow Chart



Source: SEC Incident Response Handbook

Audit Requests and Ideas

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

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

Tel. #: 202-551-6061

Fax #: 202-772-9265

Email: oig@sec.gov

Hotline

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

Phone: 877.442.0854

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