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

Assessment of SEC's Continuous Monitoring Program

August 11, 2011
Report No. 497

Assessment and Review Conducted by C5i Federal, Inc.

REDACTED PUBLIC VERSION

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

August 11, 2011

To: Thomas Bayer, Chief Information Officer, Office of Information Technology (OIT)
Jayne L. Seidman, Acting Associate Chief Operating Officer, Office of Administrative Services (OAS)
Cristin Fair, Acting Associate Executive Director, Office of Human Resources (OHR)

From: H. David Kotz, Inspector General, Office of Inspector General (OIG)

Subject: *Assessment of SEC's Continuous Monitoring Program,*
Report No. 497

This memorandum transmits the U.S. Securities and Exchange Commission OIG's final report detailing the results on our review of the Commission's continuous monitoring program. This review was conducted as part of our continuous effort to assess management of the Commission's programs and operations and as a part of our annual audit plan.

The final report contains 13 recommendations which if fully implemented will strengthen OIT's continuous monitoring program. We are pleased OIT concurred with the 12 recommendations addressed to its office, OAS concurred with the 3 recommendations addressed to its office, and OHR concurred with the recommendation addressed to its office. Your written responses to the draft report are included in Appendix VII.

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

Should you have any questions regarding this report, please do not hesitate to contact me or Anthony Barnes at x15331. We appreciate the courtesy and cooperation that you and your staff extended to our staff and contractors during this review.

Attachment

cc: James R. Burns, Deputy Chief of Staff, Office of the Chairman
Luis A. Aguilar, Commissioner
Troy A. Paredes, Commissioner
Elisse B. Walter, Commissioner
Jeff Heslop, Chief Operating Officer, Executive Director, Office of Chief of Operations
Todd Scharf, Chief Information Security Officer, Office of Information Technology
Judith Blake, Acting Audit Liaison, Office of Administrative Services

Assessment of SEC's Continuous Monitoring Program

Executive Summary

Background. 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 OIG's input to the Office of Management and Budget (OMB) Memorandum M-10-15, fiscal year 2010 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management[1] and to perform two separate reviews—one on the SEC's continuous monitoring program and the other on the inclusion of language addressing privacy act requirements in SEC contracts.[2] Specifically, this review was conducted to assess the Commission's continuous monitoring program. C5i did not conduct detailed control tests because doing so was not within the scope of its work.

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 operating environments with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring includes, but is not limited to, the following components, which are specified in National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* (NIST 800-53):[3]

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identity and Authentication
- Incident Response
- Maintenance
- Media Protection

[1] *2010 Annual FISMA Executive Summary Report,* Report No. 489 (Mar. 3 2011).
[2] *Review of SEC Contracts for Inclusion of Language Addressing Privacy Act Requirements*, Report No. 496
[3] National Institute of Standards and Technology (NIST), *Recommended Security Controls for Federal Information Systems and Organizations,* Special Publication 800-53, Revision 3, Annex 3, pages 2-7, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity

C5i used the guidance from NIST, OMB, and FISMA, and industry best practices in our review and to support our conclusions and recommendations.

C5i reviewed the findings from previously issued OIG reports, conducted interviews with SEC Office of Information Technology (OIT) staff, and reviewed support documentation and the Commission's policies and procedures. As detailed in this report, we found the following additional areas need improvement:

- Access Control
- Audit and Accountability
- Configuration Management
- Contingency Planning
- Identity and Authentication
- Planning
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity

Because of previous work C5i conducted on the OIG's annual FISMA reporting to OMB,[4] C5i was aware of areas where they should focus its assessment of the SEC's continuous monitoring program.

Objectives. The overall objective was to review the SEC's continuous monitoring program and further assess current policies and procedures and their compliance with NIST, FISMA, and OMB guidance.

Results. C5i's review consisted of conducting in-depth interviews with OIT staff whose areas of responsibility included, but were not limited to, disaster recovery/continuity of operations, account management (activation and termination of user accounts), help desk, network operations (patching, software updates, log management), and asset inventory. We conducted interviews from November 2010 to December 2010. During this timeframe, we also conducted follow-up interviews with SEC employees to fully understand the Commission's continuous monitoring program. In addition, we reviewed documentation provided to us such as the results of OIT's disaster recovery tests and asset

[4] *2010 Annual FISMA Executive Summary Report*, Report No. 489, March 3, 2011.

inventory databases, and performed tests to verify whether OIT's documented procedures were being followed for functions such as password resets.
C5i met with staff from the OIT Server and Storage Group to fully understand how the SEC's network servers are managed and monitored. These servers include [redacted] which are the essential components that make up the SEC's network. We spoke with staff responsible for the various servers to understand the configuration of new servers, the deployment of new servers on the SEC's network, the retiring of old equipment, the monitoring of activities on the servers (logs), backup procedures used to retain and store historical information in the event of a system failure, and the process to "rebuild" network data. Our review found some areas of concern in OIT's policies and procedures surrounding log management and retention, and backup retention.

Currently, the OIT Server and Storage Group captures and retains logs for its networks and systems but has no documented policies and procedures pertaining to this function. Without fully defined and documented roles and responsibilities and procedures detailing the types of logs to be captured and retained, we cannot fully determine whether the Commission is capturing system and network logs in a manner that would provide all the necessary information in the event of a security event investigation.

We also reviewed the SEC's backup retention policies and procedures. We found that the SEC performs [redacted] on critical files [redacted] on every server. [redacted] and stored for [redacted] are then reused. We also found that OIT has documented policies and procedures outlining the roles and responsibilities for backing up data. Although NIST does not specify a retention period for backup data, industry best practices call for a [redacted] retention period. We are recommending the Commission lengthen its retention period from [redacted] and update its policies and procedures accordingly. During this review, we also found that [redacted] stored [redacted] in a [redacted] facility.

As part of our review of the backup policies and procedures at the Commission, C5i reviewed the Commission's disaster recovery plans and its most recent results of the disaster recovery tests that were performed. As documented in the 2010 FISMA assessment report,[5] the SEC has established and maintains an agency -wide continuity of operations plan (COOP) and disaster recovery program consistent with the requirements of NIST, FISMA, OMB and the provisions of the February 2008 Federal Continuity Directive,[6] which state that continuity plans and programs should be developed and have well-documented

[5] *2010 Annual FISMA Executive Summary Report*, Report No. 489 (Mar. 3, 2011).
[6] Federal Continuity Directive, *Federal Executive Branch Continuity Program and Requirement* (February 2008).

policies and procedures.[7] However, in reviewing the disaster recovery test results, C5i found that not all the tests produced successful results. For example, some applications exceeded the maximum allowable time to come back online, and communication and coordination was not as strong as needed. C5i did find there were improvements from the bi-annual April and November tests in 2010 to the retest performed in January 2011. However, we are still concerned about the SEC's full failover and restore capabilities. Due to the issues encountered in the disaster recovery exercises, C5i is concerned that in the event of a major disaster, a fully successful failover and recovery cannot be completed.

During a previous assessment,[8] we found many issues with OIT's patching policies and procedures, specifically, ineffective patch management. During this assessment, C5i found that the Commission had made great strides in improving the deployment of patches to its systems and ensuring that the systems were up to date with current security remediation issued by vendors. However, C5i also found that the environment used to test patches before deployment to the Commission's production systems was not identically configured to the test environment due to differences in hardware and software. Using a test environment that does not accurately reflect the current production environment can produce inaccurate results and can result in failure of patches or other remediation to work correctly when deployed into production, which can lead to adverse effects on the production network and degradation of network performance. We are recommending that the Commission configure its testing and production environments identically to ensure that the results of pre-deployment tests of patches are full and conclusive.

During the 2010 FISMA assessment, C5i found the SEC's network password policy is not Federal Desktop Core Configuration compliant with respect to password complexity and the frequency which passwords are required to be changed.[9] Our review found that the SEC password policy is not consistently applied to all network users. C5i found five contractors who had never been prompted to change their passwords and had their then-current passwords for more than [redacted] in violation of the SEC's password policy that requires passwords to be changed [redacted] [10] C5i also found that the SEC password policy requirements for complexity, as documented in SEC Implementing Instruction, II 24-04.06.01 (01.1), Identification and Authentication, July 9, 2008, are inconsistent with the Group Policy requirements implemented in Active Directory on the SEC network in that the Group Policy requirements require [redacted]

[7] 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*.

[8] *Assessment of SEC's Privacy Program*, Report No. 485 (Sept. 29, 2010).

[9] *2010 Annual FISMA Executive Summary Report*, Report No. 489 (Mar. 3, 2011).

[10] SEC Implementing Instruction II 24-04.06.01 (01.1), Identification and Authentication (July 9, 2008).

Further, C5i tested procedures for requesting password changes through the SEC help desk and performed four separate tests to determine whether help desk technicians were following the proper procedures to fully verify callers' identity before resetting their network password. C5i found many inconsistencies. For example, some technicians requested information such as [redacted] and others did not. Although OIT Policy 41-07-007-001.0, Technical Assistance Center/Customer Care Center Password Reset Procedures for Remote and LAN Accounts, specifies the information that technicians are to verify before they reset a password, C5i found that technicians are not consistently following these procedures. In addition, the policy should be updated to include the new requirement to verify the [redacted]

Furthermore, C5i conducted two additional tests to verify whether or not the password structure documented in SEC II 24-04.06.01 (01.1), Identification and Authentication was being fully enforced. We found that although a [redacted] is [redacted] in the [redacted] the requirement [redacted] being [redacted] by the [redacted].

When an SEC help desk technician resets a password, the technician provides the caller with a [redacted] such as [redacted] or [redacted] but when the caller logs into the SEC network for the first time with the [redacted]. This, coupled with inconsistent application of the requirement that [redacted] be [redacted] could allow individuals to [redacted] We recommend that OIT investigate using a random password generator that would generate a complex password for users requesting a password reset, which would (1) provide more secure temporary passwords and (2) spur users to change their password on their first log-on attempt after the reset. OIT should also investigate the implementation of a prompt that directs users to change their help-desk-issued [redacted] on their [redacted] on to help ensure that [redacted] are used only [redacted].[11]

As reported in the OIG's 2010 FISMA Assessment,[12] C5i found that 14 network accounts had not been properly terminated when users had separated from or been terminated by the Commission. Our review of the procedures used to activate and terminate network accounts found that although the procedures are documented, there is no "cross-reference" or audit performed by OIT, Office of Human Resources, and Office of Administrative Services (OAS) to ensure all terminations have been received and processed in a timely manner. C5i also

[11] As of June 8, 2011 one contractor's passwords had expired reflecting that OIT is taking steps to remediate this issue. The password was changed to a randomly generated password. Three of the contractors are no longer working at the SEC, and the other test subject has not yet been affected by the change in procedure

[12] *2010 Annual FISMA Executive Summary Report*, Report No. 489 (Mar. 3, 2011).

found that while OIT has a policy for contractor's entry and exit that specifies steps for issuing badges, setting up and terminating accounts, equipment issuance and so on, the policy does not apply Commission-wide. At the time of our review OAS was developing a policy to be implemented throughout the Commission, but it had not been completed or approved. C5i also found that the OAS policy under development lacked some of the detail that was included in OIT's policy such as roles and responsibilities and checklists. C5i is recommending that OAS and OIT work together on Commission-wide policy and finalize and implement this policy. Training for all staff involved with contractors such as Contracting Officers, Contracting, Officer's Technical Representatives, and Contractor Points of Contact, should also be developed and rolled out to ensure the policy is effectively and thoroughly communicated.

Summary of Recommendations. Our review determined that numerous improvements were required to enhance the SEC's continuous monitoring program. Specifically, we recommended the following:

(1) OIT should review the Commission's Microsoft Active Directory settings and make the necessary changes to ensure that OIT password policy requirements, as documented in the Implementing Instruction, are strictly enforced for both on-site and remote users and that the documented password structure set forth in OIT policy is strictly enforced.

(2) OIT's help desk should begin using a random password generator to create temporary passwords and require users to [redacted] on their [redacted].

(3) OIT should implement training for [redacted] personnel to ensure that [redacted] technicians consistently verify users' information in accordance with OIT policy when they receive requests to change user accounts and passwords.

(4) OIT should ensure that security controls configurations that are applied in the production environment are identical with those applied in the testing environment.

(5) OIT should develop and implement written procedures to ensure configuration consistency in the Commission's production and testing environments. These procedures should detail the software and hardware components in both environments and specify the actions required to maintain consistent environments.

(6) OIT should complete and finalize written server and storage log management policies and procedures that fully document roles and responsibilities for log capture, management, retention and separation of duties.

(7) OIT should require that the [redacted] and the [redacted] have consistent, appropriately installed application and system configuration files to ensure the ability to successfully failover and/or restore in the event of a disaster.

(8) OIT should fully document and communicate the criteria used to determine the success or failure of an application during the Disaster Recovery tests to ensure consistent reporting of results and alleviate confusion.

(9) OIT should analyze the level of criticality of the Commission's data being [redacted] and the needs and wants of its customers, and establish an appropriate backup retention period based on the results of that analysis and that meets the requirements of the Commission.

(10) OIT should ensure that [redacted] from the Commission's [redacted] are sent to an [redacted].

(11) OAS should work with the OIT to develop and implement a comprehensive Commission–wide policy for the Entry and Exit of Contractors.

(12) After the OAS contractor entry and exit policy, Contractor Personnel Employment Entrance and Exit Procedures, has been finalized and approved, OAS should provide training and communicate with responsible parties, such as Contracting Officers, Contracting Officer's Technical Representatives, and Inspection and Acceptance Officials, regarding their roles and responsibilities and proper procedures with respect to contractor entry into and exit from the Commission.

(13) OHR, OIT, OAS, and the contracting office should perform, at a minimum, a [redacted] of separated/terminated employees and contractors to ensure that OIT has received all account termination notices and has deactivated the appropriate accounts in a timely manner.

TABLE OF CONTENTS

Appendices

Tables

Figures

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 completing and coordinating the OIG's input to the Commission's response to Office of Management and Budget (OMB) Memorandum M-10-15, fiscal year (FY) 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.[13] This memorandum provides the instructions and templates for meeting the FY 2010 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA).[14] The SEC OIG also contracted with C5i to review the SEC's continuous monitoring program and the handling of SEC personally identifiable information (PII) by third-party contractors.[15]

This report presents the results of C5i's review of the SEC's continuous monitoring program. 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 business processes. C5i did not conduct detailed control tests, as they were not within the scope of its work.

According to National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* (NIST 800-53), continuous monitoring includes, but is not limited to the following components:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identity and Authentication

[13] OMB Memorandum M-10-15, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (Apr. 21, 2010). http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf.

[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] OIG, *Review of Third-Party Contractor's Handling of SEC Personally Identifiable Information*, Report No. 496.

- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity[16]

Objective

To review the SEC's continuous monitoring program and further assess the SEC's current policies and procedures and its compliance with the NIST, FISMA, and OMB guidance.

[16] National Institute of Standards and Technology (NIST), *Recommended Security Controls for Federal Information Systems and Organizations,* Special Publication 800-53, Revision 3, Annex 3, pp. 2-7, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

Findings and Recommendations

Finding 1: OIT Is Not Fully Enforcing the Requirements of Its Implementing Instruction for User Account Identification and Authentication

> OIT's Implementing Instruction 24-04.06.01(01.1), Identification and Authentication for all network user accounts is not being fully enforced. As a result, OIT's practices are in violation of Implementing Instruction 24-04.06.01 (01.1) and NIST 800-53.

Passwords are an essential component in protecting an organization's computer networks and the information they contain. When a network account is initially setup at the Commission, users are assigned a user name and a temporary password that must be changed when the user logs onto the network for the first time. The user is prompted to change the password and the password is to be changed at regular intervals according to OIT Implementing Instruction 24-04.06.01(01.1), Identification and Authentication, which states the following:

> With the exception of initial passwords, user-selected passwords are required. [redacted] expire every [redacted] which [redacted] The information system must have an automated mechanism to ensure that users and administrators change their passwords at an interval not greater than the timeframes established by this policy. The information system provides the user, via a popup alert on login, with a [redacted] of [redacted].[17]

In the Microsoft Active Directory Network environment, OIT uses the built in Microsoft feature called Group Policy which provides the centralized management and configuration of operating systems, applications and users' settings. Microsoft Group Policy is a set of rules that controls the working environment of user accounts and computer accounts, essentially controlling what users can and cannot do in Microsoft environments. Microsoft's default Group Policy password structure requires that passwords contain characters from three of the following five categories:

[17] OIT Implementing Instruction 24-04.06.01 (01.1), Identification and Authentication (July 9, 2008).

- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.[18]

According to OIT's Implementing Instruction for Identification and Authentication, system and application passwords must be at least eight characters long, contain at least one number, and include at least one special character (i.e., a non-alphabetic or non-numeric symbol). They should also be complex or difficult to guess and should not contain full dictionary words.[19]

C5i determined that the instruction is written to apply to all users who access SEC systems, whether onsite or remotely, and conforms with NIST 800-53, Security Control IA-5 Authenticator Management,[20] although it does not comply with Federal Desktop Core Configuration standards for password length and change intervals, as noted in the OIG's *2010 Annual FISMA Executive Summary Report*.[21] While the instruction conforms to NIST 800-53, OIT is not implementing the instruction in a manner that complies with NIST 800-53 standards.

NIST 800-53 standards require that passwords have defined "lifetime restrictions," i.e., how frequently passwords need to be changed.[22] Further, the Implementing Instruction provides the requirement that user passwords be changed every 120 days and that the user is prompted 14 days prior to the expiration of their current password to make the change.[23] However, C5i identified discrepancies with password change prompting personnel who remotely access SEC systems via the virtual private network, Citrix, or Outlook Web Access. C5i's judgmental sample found five cases where contractors who [redacted] SEC [redacted] were not [redacted] to [redacted] and had [redacted] for [redacted]. Two of the five contractors received their passwords in [redacted] and the other three received their passwords in [redacted]

[18] http://technet.microsoft.com/en-us/library/cc786468%28WS.10%29.aspx.
[19] Id., p. 3.
[20] NIST 800-53, p. F-57, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.
[21] OIG, *2010 Annual FISMA Executive Summary Report*, Report No. 489 (Mar. 6, 2011).
[22] NIST 800-53, p. F-57, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.
[23] OIT Implementing Instruction 24-04.06.01 (01.1), Identification and Authentication (July 9, 2008).

However, none of them have been [redacted] [24] Although a [redacted] solution is in place for the initial authorization of remote users, the Microsoft Windows Active Directory password changes are not enforced and the cases C5i identified violate OIT Implementing Instruction 24-04.06.01 (01.1) and NIST 800-53.[25]

Recommendation 1:

The Office of Information Technology (OIT) should review the Commission's Microsoft Active Directory settings and make the necessary changes to ensure that OIT password policy requirements, as documented in the Implementing Instruction, are strictly enforced for both on-site and remote users and that the documented password structure set forth in OIT policy is strictly enforced.

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

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

Recommendation 2:

The Office of Information Technology help desk should begin using a random password generator to create temporary passwords and require users to [redacted] on their [redacted]

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

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

[24] As of June 8, 2011 one of the contractor's passwords expired reflecting that OIT is taking steps to remediate this issue. The password was changed to a randomly generated password. Three of the contractors are no longer working at the SEC, and the other test subject has not yet been affected by the change in procedure.

[25] NIST 800-53, p. F-58, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

Finding 2: OIT's Help Desk Password and PIN Reset Verification Procedures Need Improvement

> OIT help desk does not always apply consistent procedures when users call to request a password reset.

When an SEC user requests a user password or personal identification number (PIN) reset from [redacted] responding technicians do not always use consistent verification procedures. By not always properly and fully verifying the [redacted] to the [redacted] OIT personnel are violating documented OIT procedures and can increase the risk that a malicious party may inadvertently gain access to SEC's systems.

According to OIT Policy 41-07-007-001.0, [redacted] Password Reset Procedures for [redacted] (OIT Policy 41-07-007-001.0), the following user information must be verified before a password or PIN reset is processed:

[redacted]

During interviews with OIT staff, C5i found that in certain cases before [redacted] technicians process a user password or PIN reset, they verified the [redacted] by [redacted] asking for the user's [redacted], the [redacted] of the [redacted] and the [redacted], which according to OIT Policy 41-07-007-001.0 is not sufficient.

To test [redacted] compliance with OIT's documented user password and PIN reset policy, a C5i contractor who had just received his SEC network credentials attempted to log onto his account at the SEC Operations Center (OPC) in Alexandria, Virginia. When the contractor's temporary password did not work he used the [redacted] to call the [redacted] for assistance. The technician asked for the person's [redacted] and the password was reset. To determine whether this behavior was an anomaly, C5i conducted [redacted] additional tests of whether the OIT help desk obtained the information required by OIT Policy 41-07-007-001.0 from individuals requesting password and PIN resets, as described below.[27]

[26] OIT Help Desk, (202) 551- 4357, Option 2.

[27] In all tests, the contractors used their true identities and did not represent themselves as someone else.

Test 1: On January 21, 2011, a C5i contractor working for SEC called the [redacted] from [redacted] and requested his password be reset. The [redacted] technician asked for the person's [redacted] the [redacted] and whether he was an [redacted] or a [redacted] The technician did not reset the password because the call did not come from a [redacted] The technician said that he did not have the authority to make the change and referred the contractor to an OIT information technology (IT) specialist who could help reset the password. While OIT Policy 41-07-007-001.0 does not specifically require referral to an IT specialist in this type of situation, C5i found that the [redacted] technician's verification of the caller's identity was more thorough than in the initial test case described above.

Tests 2 and 3: On January 27, 2011, two C5i contractors contacted the [redacted] and requested their passwords be reset. The calls were made from the [redacted] location in [redacted] from the desk of an [redacted] and from a [redacted] telephone. The technicians verified both callers' identities by obtaining their [redacted], and the [redacted], then reset the passwords. The technicians did not, however, obtain all the required information that was needed to verify the callers' identify, as described in OIT Policy 41-07-007-001.0.

Test 4: On January 28, 2011, a C5i contractor called the [redacted] from a [redacted] and requested his password be reset. The technician only verified the caller's [redacted] and then reset the password, which violates OIT Policy 41-07-007-001.0.[28]

On their next logins, which occurred onsite at [redacted] location, [redacted], and [redacted], the four contractors who performed the tests described above were not [redacted] the [redacted] passwords they were given by [redacted] staff. As of February 7, 2011, the four contractors [redacted]. Although the [redacted] conform to OIT Implementing Instruction 24-04.06.01 (01.1) (i.e., they have a minimum of [redacted] characters and contain a [redacted]), all four contractors contend that the structure of the [redacted] is not sophisticated and could [redacted] be compromised. The four contractors did not share their passwords with anyone and only confirmed that they were [redacted]

[28] OIT was not notified of the results of these tests prior to the issuance of this report as this was not a requirement of the assessment.

Further, to test compliance with OIT Implementing Instruction 24-04.06.01 (01.1), for password characteristics and structure, C5i conducted the following two additional tests:

> ***Test 5***: On February 7, 2011, while [redacted] at the [redacted] offices, one of the four contractors who had received a [redacted] password from the [redacted] technician changed the [redacted] password to further test compliance with OIT Implementation Instruction 24-04.06.01 (01.1). The contractor purposely did not include [redacted] as required by the Implementing Instruction, and the new password was successfully changed without the required [redacted]
>
> ***Test 6***: To confirm that the result of test 5 was not an anomaly, two additional contractors and an SEC employee changed their [redacted] on February 7, 2011, and February 8, 2011, respectively. First, they attempted to change their [redacted] using only [redacted] and [redacted] or [redacted], but the system rejected [redacted]. They then used a [redacted] but no [redacted] and that password change was accepted.

C5i's review found that the SEC's network systems are not always enforcing the SEC's documented, required [redacted], as evidenced by the ability of SEC contractors and employees to [redacted] without using [redacted] as required by OIT Implementing Instruction 24-04.06.01 (01.1). The SEC's network systems are set to comply with [redacted], which has less complex requirements than the [redacted] This deficiency must be addressed to ensure full compliance with the SEC's [redacted] The failure to enforce Implementing Instruction 24-04.04.01 (01.1) most stringent requirements increases the risk that user accounts and critical SEC data could be compromised.

C5i also determined from the results of the tests described above that OIT [redacted] personnel did not consistently verify [redacted] in accordance with OIT Policy 41-07-007-001.0. By not properly and fully verifying the [redacted] OIT personnel are violating documented OIT policy and increasing the risk that they might inadvertently help a malicious party gain access to SEC systems.

Recommendation 3:

The Office of Information Technology (OIT) should implement training for [redacted] personnel to ensure that [redacted] technicians consistently verify users' information in accordance with OIT policy when they receive requests to change user accounts and passwords.

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

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

Finding 3: OIT's Test and Production Environments Are Not Identically Configured

OIT's test and production environments are not identically configured. As a result, OIT may be unable to fully assess and determine if updates to applications and software tested in the test environment that are deployed into the production environment will operate and function as intended and prevent unintended negative impacts to the existing production environment.

A testing environment is created for the purpose of testing application and software upgrades, new applications, security patches, configuration modifications, and the like, that are to be deployed throughout an organization to confirm that they function properly and have no negative impact on the existing production environment. A production environment consists of the hardware and software used day-to-day to conduct the organization's business. The setup of software and hardware components consists of physical and logical and other needed software components.

Testing is an essential component of IT staff practices in any organization. The testing environment is used by testers to load and test new applications, system or application patches, system updates, and software products prior to their implementation in production systems. In the testing environment tests are conducted to identify and remediate any issues that emerge (e.g., software incompatibility) and thereby prevent them from occurring in the production environment, and to ensure that production systems are capable of handling new applications, patches, system updates, and software products.

As stated in NIST SP800-123, *Guide to General Server Security*, “Administrators should generally not apply patches to production servers without first testing them on another identically configured server because patches can inadvertently cause unexpected problems with proper server operation.”[29]

Testing new software and security patches in an environment that is not identically configured can provide false-positive results which incorrectly indicate that a deployment will be successful. If, for example, a patch were deployed into production without first being tested in an identically configured environment, the patch could have a severe negative effect on an organization’s network or applications, such as locking out users from system files or causing the system to crash. The more closely the test environment configuration reflects the production environment—through the use of duplicate hardware and software components and version numbers—the more likely it is that the performance obtained in the testing environment will reflect the performance obtained in the production environment. Ideally, once any upgrade or change has been properly tested, the results demonstrate the desired functionality, and the testing has been deemed sufficiently reliable, the upgrade or change can be deployed to the production environment and made available to users without having unintended, negative effects on the network or applications.

Through interviews with OIT staff, C5i discovered that OIT’s testing and production environment is not identically configured. C5i determined that the differences have occurred because major applications or software in the testing environment (1) do not have the correct configuration files, (2) are not the correct version, and (3) are not being set up to simulate the production environment. Based on a sample report of 10 applications from OIT’s testing and production environments provided by OIT, C5i determined that the [redacted] are not the same version in the test environment as in production as follows:

(1) The [redacted] is currently using [redacted] in the test environment while running [redacted] in the production environment.
(2) The [redacted] is currently using [redacted] in the test environment while running [redacted] in the production environment.
(3) The [redacted] is currently running [redacted] in the test environment while running [redacted] in the production environment.

[29] NIST SP 800-123, *Guide to General Server Security*, July 2008, http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf, Page 4-2

Different application versions may have different configuration files, and inconsistent configuration files may cause issues with applications, such as affecting the ability to view and create reports.

According to OIT staff, the differences in the application versions occurred because newer versions of the applications were being tested in the test environment before being deployed to the production environment. However, the updated test environment is the same environment that OIT uses to test patches. Testing a patch in this updated environment may therefore not accurately predict whether the patch will adversely affect the existing, un-updated production environment.

Although there are currently no specific OIT policies or procedures that require it to implement or maintain identical environments, OIT's testing of patches in an environment that is not identical to the production environment could incorrectly indicate that patches could be successfully deployed to the SEC production environment when in fact they could have adverse effects on SEC production systems. Testing procedures for patches are detailed in OIT Implementing Instruction 24-05.04.03, Patch Management, which states the following:

> Patches and configuration modifications are initially tested on non-production systems to account for any unintended remediation consequences. The non-production testing environment, within budget constraints, needs to accurately represent the production configuration.[30]

One of the main goals of the IT staff within an organization is to ensure that production systems run smoothly and efficiently. To achieve this goal, system modifications or additions need to be tested in a test environment that is configured identically as the production environment before they are deployed throughout the organization.

Recommendation 4:

The Office of Information Technology should ensure that security controls configurations that are applied in the production environment are identical with those applied in the testing environment.

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

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

[30] OIT Implementing Instruction 24-05.04.03, Patch Management (Dec. 28, 2005).

Recommendation 5:

The Office of Information Technology should develop and implement written procedures to ensure configuration consistency in the Commission's production and testing environments. These procedures should detail the software and hardware components in both environments and specify the actions required to maintain consistent environments.

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

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

Finding 4: Policies and Procedures for Computer [redacted], Management, and [redacted] Have Not Been Fully Implemented, and Duties Are Not Segregated

> OIT currently does not have policies and procedures pertaining to log management and has not applied the concept of separation of duties to log management. As a result, logs may not be effectively capturing important information, and staff are not fully aware of their roles and responsibilities with respect to the logging function.

A computer log is a file that contains events that are logged by the operating system's components. Logs can be configured to track information about user activity such as access, or to contain specific user information, such as the time pattern of a user's log-in. When an organization enables its logs, it can then use security tools to examine the logs to detect abnormal patterns, such as user log-ins at unusual times, which could suggest that an intruder has gained access to an organization's network, server, or system.

Logs are the primary tool used by system administrators to detect and investigate attempted and unauthorized network or computer system access activity and to troubleshoot user system problems. Since logs can track user activity, ensuring that logs are enabled can deter users from misusing the organization's network and make it possible to detect unauthorized access attempts to the organization's network, server, or system by hackers or intruders. Because most system threats are internal to an organization, logs can also aid in identifying the parties that are involved in security incidents. When an organization's logs are active and enabled, the organization should be able to obtain substantial information that will help it conduct an audit, and trace events that can identify the root cause of problems.

Computerized data logging is the process of recording events with an automated computer program to provide an audit trail that can be used to understand the activity of the system and to diagnose problems. Logs can be generated by such sources as the organization's system, server, and domain controller. The OIT Servers and Storage group is responsible for administering nd managing hundre of logs for th EC's [redacted] The OIT Servers and Storage group has enabled logging for all Exchange servers, Print servers, File servers, Domain Controllers, and system-generated logs. NIST SP 800-92 *Guide to Computer Security Log Management* states:

> Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems.[37]

The specifics of the type of information an organization chooses to capture in its logs (log configuration/rules), the log retention period (*i.e.,* how long the logs are retained), system administrator roles and responsibilities, and how often logs should be reviewed are key components in establishing an organization's log management policies and procedures. Quantified, established policies and procedures give management the ability to guide operations without constant intervention because they provide guidance regarding day-to-day activities to system administrators, system owners, and system users.

[31] A Microsoft Exchange server is a widely used method of creating a messaging collaborative environment.

[redacted]

NIST, *Guide to Computer Security Log Management,* Special Publication 800-92, pp. ES-1, http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf, September 2006.

OIT Log Retention, Capture, and Management Policies and Procedures. C5i found that OIT does not have formal written policies and procedures pertaining to log retention, log capture, and log management. NIST 800-92 requires agencies to establish and maintain log management activities as follows:

> To establish and maintain successful log management activities, an organization should develop standard processes for performing log management. As part of the planning process, an organization should define its logging requirements and goals. Based on those, an organization should then develop policies that clearly define mandatory requirements and suggested recommendations for log management activities, including log generation, transmission, storage, analysis, and disposal. An organization should also ensure that related policies and procedures incorporate and support log management requirements and recommendations. The organization's management should provide the necessary support for the efforts involving log management planning, policy, and procedures development.
>
> After an organization defines its requirements and goals for the log management process, it should then prioritize the requirements and goals based on the organization's perceived reduction of risk and the expected time and resources needed to perform log management functions. An organization should also define roles and responsibilities for log management for key personnel throughout the organization, including establishing log management duties at both the individual system level and the log management infrastructure level.[38]

NIST 800-53, Control AU-1 Audit and Accountability Policies and Procedures*,* provides the following guidance regarding the need for documented and implemented policies and procedures for audits (logs):

> The organization develops, disseminates, and reviews/updates (*Assignment: organization-defined frequency)*:
>
> a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance; and

[38] NIST, *Guide to Computer Security Log Management,* Special Publication 800-92, pp. ES-1–ES-2, http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf, September 2006.

b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.[39]

C5i's interviews with OIT Server and Storage group [redacted] staff found that although they generate logs, OIT does not have any written log management policies and procedures. According to OIT staff, OIT is in the process of drafting policy, but the draft policy was not available for C5i's review. Therefore, C5i was unable to assess its adequacy and compliance with NIST 800-53 and NIST 800-92.

C5i judgmentally sampled real-time and historical event logs, [redacted] to verify the activities that were being documented (see screenshots in Appendix V). C5i worked with members of the OIT Server and Storage group to capture screenshots of activities as the logs were generated. To verify the capture of logs, C5i requested logs for a judgmental number of dates.[40] OIT then accessed the logs for these dates and provided C5i with screenshots. Based on our review of the screenshots, we confirmed that user ID and log-in/log-out times are all captured for the [redacted] To fully verify all settings, a further in-depth analysis would have to be done to understand the level of information captured for user activities on [redacted] and systems. Authorized access can be abused (e.g., files or logs altered without authorization), which is why event log analysis is critical to ensure appropriate access and the use of network resources. Logs should be configured to provide sufficient information to verify user activity. Equally important to ensuring that data is being logged is establishing the storage and retention period for logs when an incident occurs. Incidents can go unnoticed for a long period; therefore, retaining data for a sufficient period is necessary if administrators and an organization are to be able to detect the causes of security-related incidents. NIST 800-92[41] recommends that security, application, and system logs be retained for 1 to 3 months for "moderate systems"[42] and 3 to 12 months for "high systems."[43] Additionally, NIST 800-53 has the following specific control for audit record retention:

[39] NIST 800-53, p. F-24. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

[40] We requested and were provided event logs for June 21, 2006, December 18, 2006, January 17, 2011, January 20, 2011, and Active Directory logs for December 7, 2009, December 14, 2009, December 21, 2009, December 28, 2009, January 1, 2010, January 11, 2010, January 18, 2010, January 26, 2010, February 15, 2010, March 14, 2010, April 12, 2010, April 19, 2010, April 26, 2010, May 30 - 31, 2010, June 1 - 3, 2010, June 30, 2010, October 23, 2010, and December 16, 2010.

[41] NIST 800-92, pp. 4-3 and ES-1, http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf.

[42] A moderate system is one whose confidentiality, integrity, and availability are considered to be at a moderate level—compromise of the system's confidentiality, integrity, or availability would not cause grave damage to an organization.

[43] A high system is one whose confidentiality, integrity, and availability are considered to be critical—compromise of the system's confidentiality, integrity, or availability cause grave damage to an organization and its ability to conduct business.

AU-11 AUDIT RECORD RETENTION

> **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.
>
> **Supplemental Guidance**: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. The National Archives and Records Administration (NARA) General Records Schedules (GRS) provide federal policy on record retention.[44]

Based on interviews C5i conducted with OIT, we found that [redacted] [redacted] of storage is allocated for each server [redacted] for logging; as soon as this threshold is met, an automated script transfers all the logs from each of the servers to a centralized server for storing. The job of the centralized server is to maintain logs from the [redacted] [redacted]’ of available storage. If the logs captured in the centralized server start to approach the [redacted], the OIT Server and Storage group is responsible for increasing storage capacity to maintain the high volume of logs. This process is compliant with the NIST 800-53 control for audit storage.[48] Currently, the OIT Server and Storage group retains logs for one year. These logs are stored on-site at the SEC Operations Center, in Alexandria, Virginia, and are replicated at the Alternate Data Center (ADC), in Ashburn, Virginia.

Certain staff in the Server and Storage group have been granted administrator-level access for the task of verifying and reviewing audit records and event logs for [redacted]

[44] NIST 800-53, p. F-30, http://csrc.nist.gov/publications/ nistpubs/800-53-Rev3/sp800-53-rev3- [redacted]

[47] Unit of measurement of computer memory equivalent to one trillion bytes or 1,000 gigabytes of information.

[48] NIST 800-53, p. F-24, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

[redacted] However, C5i found that a key security principle—separation of duties—is not applied to OIT log management activities, performed by the Server and Storage group. With separation of duties, more than one person is needed to complete a task. The goal of separation of duties is to promote integrity, prevent fraud, reduce potential damage from the actions of one person and the implementation of an appropriate level of checks and balances on an individual's activities.

Separation of duties is a requirement of NIST 800-53, which states the following:

Control: Access Control, AC-5 Separation of Duties

The organization:

a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
b. Documents separation of duties; and
c. Implements separation of duties through assigned information system access authorizations.

Supplemental Guidance. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., systems management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrators account for different roles.[49]

NIST 800-92 emphasizes the separation of duties with respect to log management as a means of preventing log tampering and manipulation. C5i found that administrators, who have access to system, [redacted] may also have the authority of altering, modifying, and deleting logs. Consistent with the principle of separation of duties from NIST 800-53, an individual with administrator access to configure the logs should not be the same person to generate or review the logs. Prevention of log tampering or altering is essential to ensure the integrity of the logs and without separation of duties, the reliability of SEC log information is difficult to ensure.

Additionally, without fully documented and implemented policies and procedures, SEC OIT may not be effectively and thoroughly collecting important information with respect to Network and Systems log functions.

[49] NIST 800-53, pp. F8-F9, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

Recommendation 6:

The Office of Information Technology should complete and finalize written server and storage log management policies and procedures that fully document the roles and responsibilities for log capture, management, retention and separation of duties.

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

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

Finding 5: OIT's [redacted] and [redacted] Disaster Recovery Tests Were Not Fully Successful Because Some Internal Applications Did Not Failover

> OIT is unable to failover all of its internal applications, which could hinder its ability to fully and swiftly perform mission-critical functions if a disaster or significant disruptions occur.

Disaster recovery (DR) is the process of re-establishing an organization's operations in the event of a disaster or other significant event, such as a tornado, hurricane, snowstorm, or fire. The process includes, but is not limited to, re-activating the organization's information systems, communicating with employees, establishing alternate work locations for employees, and identifying employees needed roles and responsibilities. NIST 800-53 provides guidance to organizations covering contingency planning policy and procedures, contingency plans, contingency training, contingency plan testing and exercises, alternate storage sites, telecommunications service, information service backup, and information system recovery and reconstitution.[50] NIST has also developed and issued NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems,*[51] which details several aspects of the planning process for developing a comprehensive DR plan and program, including the information system

[50] NIST, *Recommended Security Controls for Federal Information Systems and Organizations,* Special Publication 800-53, Rev 3 (August 2009), app. F-CP, Contingency Planning, page F-47, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

[51] NIST, *Contingency Planning Guide for Federal Information Systems,* Special Publication 800-34, Revision 1 (May 2010), p. 18, http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.

contingency planning process, information system contingency plan development, and technical contingency planning considerations.[52]

A DR plan is an information system–focused plan that is designed to restore the operability of a target system, application, or computer facility infrastructure at an alternate site. It applies to major disruptions in an organization's services or operations for an extended period of time. The DR plan may be supported by other information system contingency plans, which are organized, coordinated procedures that are to be activated to address the recovery of affected systems. However, the DR plan only addresses information system disruptions that require the relocation to an alternate site.

To assess a DR plan's effectiveness, it must be tested to ensure it provides the SEC's senior-level management confidence in the Commission's ability to restore its systems, applications, and other computing resources, in the event of a disaster or a significant event, such as a system disruption.

As documented in the OIG's *2010 Annual FISMA Assessment Report*,[53] the SEC has established and maintains an agency-wide business continuity of operations plan/DR program that is consistent with NIST, FISMA, and OMB requirements and Federal Continuity Directive 1 (FCD1), which states that continuity plans and programs should be developed and have well-documented policies and procedures.[54] We did not test the SEC's continuity/disaster recovery plans; but merely reviewed the two specific DR tests conducted on [redacted] and [redacted] and the [redacted] re-test, and confirmed that the SEC has policies and procedures[55] for DR that comply with FCD1, as well as NIST, FISMA, and OMB requirements.

As part of the DR process, the system owners for specific SEC systems and applications are involved in testing the SEC's DR plan [redacted] to ensure the full functionality of the plan and failover of systems and to document problems that may need attention or remediation. The system owners and other OIT staff (i.e., Central Operations, Information Security, etc.) are responsible for the details of each test.

[52] NIST, *Contingency Planning Guide for Federal Information Systems,* Special Publication 800-34, Rev 1 (May 2010), pp. vi-vii, http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.

[53] OIG, *2010 Annual FISMA Assessment Report*, Report No. 489 (Mar. 6, 2011).

[54] Federal Continuity Directive 1, Federal Executive Branch Continuity Program and Requirements (February 2008).

[55] 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.

[56] Failover is the capability to switch over automatically to a redundant or standby computer server, system, or network upon the failure or abnormal termination of the previously active application, server, system, or network. Failover happens without human intervention and generally without warning, unlike switchover.

On [redacted] SEC personnel performed the [redacted] of [redacted] DR plan tests for calendar year 2010. The test involved the failover of [redacted] are listed below in Table 2, along with the reasons for their lack of successfully failing over.

Table 1. Internal Applications that Did not Failover

[redacted]	Reason
[redacted]	Application database [redacted]. Per OIT, this is considered a mission-critical application.
[redacted]	Login was successful but reports [redacted] run due to [redacted] issues.[58]
[redacted]	Login was successful but reports [redacted] [redacted] to [redacted] issues.
[redacted]	Login was successful, but USA Staffing was not available at the [redacted]

Source: OIG-generated data.

On [redacted] the SEC system owners and the Disaster Recovery Group conducted the [redacted] DR test and selected [redacted] internal applications to test (see Appendix IV for a list of the applications). During this test, all but one internal application—[redacted]—successfully failed over and back. [redacted] did not fail over successfully because an incorrect version of the application had been installed at the [redacted]. The [redacted] application has been defined as mission-critical. The [redacted] applications that did not fail over successfully in the [redacted] test failed over successfully in the [redacted] test, demonstrating improvement in OIT's testing and remediation of the previously found issues. The [redacted] est was conducted specifically for the internal system with [redacted], and did not include the External Applications because they are not operated using [redacted] Table 2 provides a comparison of the results from the [redacted] DR tests.

[57] The [redacted] function enables the user to view a summary of [redacted] or previously executed [redacted] for a specific [redacted] for specific [redacted]
http://wapps.sec.gov/oitintranet/oit_request/oit_learn/Bluesheet%205.0/Script%202A%20-%20How%20to%20Perform%20an%20Equity%20Cleared%20Search_Revised%20.pdf

[58] [redacted] is a web-based reporting environment where reports can be created, generated, edited, and shared with other users. It also provides the capability for e-mail distribution of reports.

[59] [redacted] is used by SEC staff in determining and handling cases where disgorgements and penalties are to be dispersed to investors. OIT provided C5i with a list of mission critical applications which identified the [redacted] application, among others.

Table 2. Comparison of [redacted] With Results of [redacted]

	Test Date	Tested	Passed/ Restored	Failed	Percentage Passed/ Restored
Internal Applications	[redacted]	40	36	4	90%
	[redacted]	32	31	1	97%
External Applications	[redacted]	12	12	0	100%
	[redacted]	n/a	n/a	n/a	n/a

Source: OIG-generated data.

Although the SEC experienced a more favorable DR test result in [redacted] the [redacted] application still did not fail over successfully because different versions of the application are operating at [redacted] and at [redacted] which prevented the system owners from accessing the application.

On [redacted] OIT conducted a retest of applications previously tested in the [redacted] DR test. The retest consisted of [redacted] internal applications. In this retest, according to a spreadsheet provided by OIT that described the failover test results of all the applications, [redacted] internal, mission-critical applications [redacted][60] and one non-mission critical internal application, [redacted] did not fail over successfully as a result of the reporting functions not operating as expected due to problems with the report server. Although the reporting function did not operate as expected, the core applications did operate as expected. Table 2 shows the results of the [redacted] [redacted] and the [redacted].

Table 3. Comparison of [redacted] With Results of [redacted]

	Test Date	Tested	Passed/ Restored	Failed	Percentage Passed/ Restored
Internal Applications	[redacted]	32	31	1	97%
	[redacted]	42	39	3	93%

Source: OIG-generated data.

Our comparison of the [redacted] and [redacted] and [redacted] test results provided by OIT indicate that different criteria was used by the DR team to determine the pass or fail of an application. In addition, we found that there is no documentation that specifies the criteria to be used by the DR team to determine the pass or fail of an application in the test. As a result, there is confusion about the success or failure of the application test and the documented result which can lead to a misinterpretation of OIT's DR test results. For example, the spreadsheets provided to C5i indicate that in the [redacted], the [redacted] application has a failover status of "Fail" due to "IQ Issues" – the reports function

[redacted] [redacted]

not operating properly. However, based on C5i's conversations with OIT personnel, applications are considered successfully tested, i.e., passed, if the end user of the system is able to perform their basic functions after the system has been recovered.

The main objective of a DR test is to verify an organization's ability to restore applications and systems in accordance with a specific recovery time objective. Based on the results of the [redacted] C5i determined that if a disaster or other significant event were to occur, some SEC applications and systems would likely be inaccessible to users and negatively affect the SEC's normal business operations.

Recommendation 7:

The Office of Information Technology should require that the [redacted] and the [redacted] have consistent, appropriately installed application and system configuration files to ensure the ability to successfully failover and/or restore in the event of a disaster.

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

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

Recommendation 8:

The Office of Information Technology should fully document and communicate the criteria used to determine the success or failure of an application during the Disaster Recovery tests to ensure consistent reporting of results and alleviate confusion.

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

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

Finding 6: OIT Has Not Sufficiently Conducted an Analysis to Determine Whether its Information System Backup Retention Period Is Sufficient

> Given the criticality of Commission data, the SEC's information system backup retention period of [redacted] may not be sufficient. In the event of a full system failure, the only data that could be restored would be from the previous [redacted], resulting in potential data loss that would negatively affect the Commission's business operations. OIT has not conducted a recent analysis to determine whether the [redacted] period is sufficient.

Information system backup consists of copying an organization's data, files, or the contents of a hard drive or a server to preserve critical business data and other needed information so that they can be restored in the event of a data loss event (e.g., hardware or software failure, natural disaster, file corruption, theft, or fire). An information system backup retention period is the length of time an organization can go back to perform a "restore" with minimal or no loss of data. Organizations have a variety of options for backing up their information systems including tapes, zip drives, flash drives, CDs, DVDs, removable drives, remote servers, and network connections. OIT currently uses Digital Linear Tapes, a magnetic tape storage technology, to back up the Commission's information systems. However, OIT has informed us that by the end of calendar year 2011, the office will replace tapes with storage disks.

NIST Backup and Retention Policy. NIST has not issued specific guidance on backup retention periods. According to NIST 800-34, "[b]ackup and retention schedules should be based on the criticality of the data being processed and the frequency that the data is modified."[61] NIST 800-92 also states that "…more stringent requirements for performing log preservation in support of investigations (e.g., internal investigations, computer security incident handling) should override the standard organization-established values for log retention as applicable."

OIT's Backup and Retention Policies and Procedures. According to SECR 23-2a, Safeguarding Non-Public Information, and SEC Administrative Regulation (SECR) 24-2.6, Enterprise Backup of Electronic Data, all backup tapes processed at the SEC offices and divisions are considered sensitive because they contain privacy-related information, such as PII, and critical and sensitive financial data. SEC Operating Procedure (OP) 24-05.02.04.07, Safeguarding Procedures for Non-Public Backup Media, requires that all backup media,

[61] NIST 800-34, p. 57, http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf, May 2010.

including tapes, be appropriately marked to identify their content as SEC sensitive data.[62]

SECR 24-2.6, Enterprise Backup of Electronic Data*,* states the following:

a) All critical files are backed up on a nightly basis;

b) A full backup of each server that houses user and/or application data shall be performed weekly. After [redacted] the tapes are returned to OPC. Upon return of the tapes, they shall be recycled into the backup rotation. Regional and district offices shall send their full backup tapes to the designated SEC backup specialist on the first full workday after the backup was performed. If the full backup was not successful, another full backup must be taken as soon as possible, but not later than [redacted] and

c) On the days that a full backup is not performed, an incremental backup shall be performed.[63]

C5i interviewed personnel responsible for performing OIT's backups to obtain a better understanding of how often OIT conducts backups, the length of time OIT maintains the backups, the criticality of the data being backed up, and where backup tapes were stored, as well as to ascertain whether OIT's current backup policies and procedures meet the NIST 800-34 standard.[64]

C5i found that [redacted] are performed at [redacted] and individual SEC regional offices, which retain a copy of the [redacted] and [redacted] and [redacted]. Tapes are retained and are available for 30 days after the backup date. Once [redacted] has passed, the tapes are then shipped from the regional office and from [redacted] and all [redacted] of the tapes are recycled (reused) for future backups. For example, a backup tape made [redacted] ago would be available if needed, but a tape made [redacted] ago would already have been recycled and the data would no longer be available.

Data Replication. To further prevent data loss, OIT replicates[65] data in real time between [redacted] and [redacted] The SEC has [redacted] telecommunication links to circuits between [redacted] and [redacted] These circuits are fully active and provide telecommunication connectivity over the [redacted] links such that if one circuit were

[62] OP 24-05.02.04.07, Safeguarding Procedures for Non-Public Backup Media (Mar. 14, 2007).

[63] SECR 24-2.6, Enterprise Backup of Electronic Data (May 15, 2003).

[64] NIST 800-34, http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf, May 2010.

[65] Data replication is the process of copying data from one data source to another source while maintaining identical copies of the data that are synchronized. Any changes made to the original content should be posted to the copy of the data at the other location. This will enable two or more copies of data to be available.

to fail, there would still be connectivity on the [redacted] circuits. If [redacted] circuits were lost, a backup circuit from [redacted] that is routed through [redacted] would provide telecommunication connectivity. If the replication process itself had an issue, replication would be suspended until the link was back up. For all storage systems being replicated, connectivity would then resume without data loss, but the replication would have to catch up.

Analysis of Retention Period. C5i inquired from OIT as to its basis for determining that its information backup retention period should be [redacted] OIT informed us that it has not recently conducted an analysis to determine if the [redacted] is sufficient. OIT also has indicated that it has not reached out to its customers to determine if any customers would request or even require a longer backup retention period. Based upon the criticality of data, we believe that it is important to conduct a thorough analysis to determine whether a [redacted] retention period is sufficient.

Recommendation 9:

The Office of Information Technology should analyze the level of criticality of the Commission data being [redacted] and the needs and wants of its customers, and establish an appropriate backup retention period based on the results of that analysis and that meets the requirements of the Commission.

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

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

Finding 7: All SEC [redacted] are Not [redacted]

Currently, the [redacted] for the Regional Offices are stored at the [redacted] However, the [redacted] for the [redacted] are stored onsite and not at a secure off-site facility.

As outlined above in Finding 6, SEC OIT has documented policies and procedures for performing backup of critical SEC data which are compliant with NIST guidance. However, during our interviews, C5i was informed that OIT

stores [redacted] for the SEC's 11 regional offices[66] and [redacted] but the [redacted] for the [redacted] are stored [redacted].
We further found that OIT has a contract with an off-site storage vendor that allows OIT to send tapes to the vendor twice a week. However, OIT staff informed C5i that tapes had not been shipped to the off-site storage vendor since March 2008.

NIST 800-34 *Contingency Planning Guide for Federal Information Systems* provides the following guidance:

> It is good business practice to store backed-up data offsite. Commercial data storage facilities are specially designed to archive media and protect data from threatening elements. If using offsite storage, data is backed up at the organization's facility and then labeled, packed, and transported to the storage facility. If the data is required for recovery or testing purposes, the organization contacts the storage facility requesting specific data to be transported to the organization or to an alternate facility. Commercial storage facilities often offer media transportation and response and recovery services. When selecting an offsite storage facility and vendor, the following criteria should be considered:
>
> - Geographic area: distance from the organization and the probability of the storage site being affected by the same disaster as the organization's primary site;
> - Accessibility: length of time necessary to retrieve the data from storage and the storage facility's operating hours;
> - Security: security capabilities of the shipping method, storage facility, and personnel; all must meet the data's security requirements;
> - Environment: structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention, and power management controls); and
> - Cost: cost of shipping, operational fees, and disaster response/recovery services.[67]

Thus, OIT is storing [redacted] in violation of NIST guidance, and even though OIT has a contract with an off-site vendor that could be utilized to store [redacted] for the [redacted] as per NIST guidance, OIT is not currently using this mechanism to send the [redacted] offsite.

[66] The SEC's 11 regional offices are in Atlanta, Boston, Chicago, Denver, Fort Worth, Miami, Los Angeles, New York, Philadelphia, Salt Lake City, and San Francisco.

[67] NIST SP 800-34 Section 3.4.2, p 21, http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.

Recommendation 10:

The Office of Information Technology should ensure that [redacted] from the Commission's [redacted] are sent to an [redacted]

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

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

Finding 8: OAS's Draft Contractor Entry and Exit Procedures Should be Revised to Include More Comprehensive Procedures

> OAS's draft Commission-wide contractor entrance and exit policies lack the comprehensiveness of current OIT-specific procedures.

OIT's Contractor Entry and Exit Operating Procedures. OIT has developed comprehensive operating procedures for contractor entry and exit, in its Contractor Entry and Exit, OP 24-06.04.01.01(01.2) guidance. Without comprehensive procedures that fully outline specific roles and responsibilities, the Commission risks the improper entry and exit of contractors, which can cause projects to be delayed because of entry issues, contractor accounts to remain active after the contractor's exit, and improper tracking of SEC assets, including laptops and RSA tokens.

Contractors are used throughout the federal government to augment department and agency workforces and to provide professional and management support services. Generally, federal government departments and agencies have processes and procedures to bring contractors on board and to terminate them when their services are no longer needed. In alignment with other federal departments and agencies, OIT has developed Contractor Entry and Exit, OP 24-06.04.01.01(01.2) procedures, which contains its operating procedures for the entry and exit of contractors.[68] OIT's procedures also include two forms to be used for OIT contractor entry and exit. The contractor entry form is used to request hardware and local area network access for an entering contractor and specifies pertinent documentation that the contractor must complete, such as a nondisclosure agreement and an authorization for credit check, in order to be

[68] Contractor Entry and Exit, OP 24-06.04.01.01(01.2) (July 18, 2006).

processed for a badge.[69] The contractor exit form is used to document the return of a departing contractor's badge, equipment, and RSA token, and includes a section on reassigning equipment.[70]

Overall, C5i found OIT's entry and exit procedures for contractors to be comprehensive and sufficient. The entry process for OIT contractors requires completion of a background check and nondisclosure agreement, processing of credentials required to access SEC facilities and network systems, documentation of equipment issued (e.g., laptop, Blackberry), coordination of workspace for contractors working on-site at the SEC, and completion of the Contractor Entry Form. The exit process for OIT contractors includes, but is not limited to, documenting the roles and responsibilities of the staff for terminating accounts, collection of SEC equipment and badges, and reallocation of workspace.

C5i judgmentally selected 6 of 30 OIT Contracting Officer's Technical Representatives (COTR) to interview and determine whether they were aware of current OIT policies and procedures pertaining to contractor entry and exit. C5i found that all 6 were aware of the OIT's contractor entry and exit policies and procedures.

OAS's Draft Contractor Entry and Exit Policy. OAS staff provided C5i with its draft SEC contractor entrance and exit policy, Contractor Personnel Employment Entrance and Exit Procedures, dated November 29, 2010, which covers all SEC contractors, including OIT contractors, and will supersede the operating procedures OIT currently uses to oversee the entry and exit of OIT contractors. OAS was not initially aware that OIT had already developed comprehensive entrance and exit procedures and did not consider or review OIT's procedures in drafting its overarching policies and procedures for the Agency.

C5i's review of OAS's draft policy determined that the OAS policy lacks certain specific details—details that are included in OIT's operating procedures. We further determined that the OAS draft policy is insufficient. Specifically, C5i found that the OAS draft procedures lack full coverage of the roles and responsibilities of administrative officers, COTRs, and contractor points of contact and did not contain references to other pertinent or applicable policies and procedures. Without comprehensive procedures that fully outline the contractors specific roles and responsibilities, the Commission risks the improper entry and exit of contractors, which can cause projects to be delayed because of entry issues, contractor accounts to remain active after the contractor's exit, and the improper tracking of SEC assets, such as laptops and RSA tokens.

[69] OP 24-06.04.01.02.T01.

[70] OP 24-06.04.01.02.T02.

Recommendation 11:

The Office of Administrative Services should work with the Office of Information Technology to develop and implement a comprehensive Commission–wide policy for the Entry and Exit of Contractors.

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

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

Recommendation 12:

After the Office of Administrative Services (OAS) contractor entry and exit policy, Contractor Personnel Employment Entrance and Exit Procedures, has been finalized and approved, OAS should provide training and communicate with responsible parties, such as Contracting Officers, Contracting Officer's Technical Representatives, and Inspection and Acceptance Officials, regarding their roles and responsibilities and proper procedures with respect to contractor entry into and exit from the Commission.

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

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

Finding 9: SEC Lacks Procedures to Ensure Timely Termination of Network Accounts

No cross-referencing procedures exist at the Commission to ensure the timely termination of network accounts for separated or terminated users. Without such procedures, the accounts of terminated employees and contractors could remain active, allowing unauthorized and potentially malicious users to gain access to sensitive SEC data or systems.

According to NIST 800-53, organizations should manage information system accounts, and should deactivate temporary accounts that are no longer required and deactivate accounts of terminated or transferred users, and review accounts.[71]

As C5i reported in OIG's *2010 Annual FISMA Executive Summary Report,* C5i found network accounts for employees who had separated from the Commission that had not been disabled in a timely manner.[72] Specifically, the accounts for 14 employees remained active after their last day of employment at the SEC.

Through additional subsequent interviews with OIT personnel and further assessment of the procedures surrounding account terminations, C5i found that although there is a process in place for terminating the accounts of separated employees and contractors, no verification procedures currently exist to ensure that accounts have been terminated.

C5i found that the same process is used for account termination and account creation. In both situations, OIT OP 24-05.01.02.T01, Request for Account Creation, Modification, Termination, or Transfer*,* is used. The IT Specialist or administrative contact for the relevant organization is responsible for completing the form and submitting it to the OIT Technical Assistance Center–Local Area Network Account Management Group, which is to enable or disable the account on the employee's separation date, as documented on the form. In the event of an involuntary termination, the Technical Assistance Center and OIT Security are immediately notified of the termination and the account is terminated.

Through additional interviews with OIT personnel and further assessment of OIT's account termination procedures, C5i found that although OIT is following its internal account termination process, there are no procedures to verify that all termination forms have been received and processed. Further, C5i found that there are no formal procedures or system for cross-referencing OIT user account termination records with Office of Human Resources, OAS, or Contracting Officer/COTR/Inspection and Acceptance Official records of employee and contractor terminations.

Without a process to ensure that all SEC employee and contractor termination forms have been received and processed by OIT, the SEC is unable to maintain an accurate and complete user account inventory and disable accounts in a timely manner. As a result, the accounts of terminated employees and contractors could remain active, permitting unauthorized and potentially malicious users access to sensitive SEC data or systems.

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

[72] OIG, *2010 Annual FISMA Executive Summary Report*, Report No. 489 (Mar. 6, 2011).

Recommendation 13:

The Office of Human Resources, Office of Information Technology (OIT), Office of Administrative Services, and the contracting office should perform, at a minimum, a [redacted] of separated/terminated employees and contractors to ensure that OIT has received all account termination notices and has deactivated the appropriate accounts in a timely manner.

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

OIG Analysis. We are pleased that OHR, OIT and OAS concurred with this recommendation.

Abbreviations

ADC	Alternate Data Center
BDRA	Broker Dealer Risk Assessment
BLUE	Bluesheet Management Systems
CATS	Case Activity Tracking System
CMDB	Configuration Management Database
COOP	Continuity Of Operations Plan
COTR	Contracting Officer's Technical Representative
DR	Disaster Recovery
EAUA	External Application User Authentication
FACTS	Filing Activity Tracking System
FDC1	Federal Continuity Directive 1
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IT	Information Technology
NIST	National Institute of Standards and Technology
NRSI	Name Relationship Search Index
NSAR	Investment Company Semi-Annual Report
OAS	Office of Administrative Services
OHR	Office of Human Resources
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OPC	SEC Operations Center, Alexandria, Virginia
PII	Personally Identifiable Information
PTS	Property Tracking System
SDCAT	Secure Data Collection Analysis Tool
SEC or Commission	U.S. Securities and Exchange Commission

Scope and Methodology

Scope. C5i obtained information from OIT and OAS pertaining to the SEC's Continuous Monitoring Program. In addition, C5i interviewed staff members from all areas of OIT—End User Technology, Security, Server Group, Disaster Recovery Participants, Policy Development—to fully understand the roles and responsibilities of each organization and verify compliance with policies and procedures.

C5i conducted its assessment from November 2010 through January 2011. The scope of C5i's work consisted of reviewing the following areas defined by NIST 800-53:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identity and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity[73]

C5i used the guidance from NIST 800-53; other NIST, OMB, and FISMA guidance; and industry best practices in C5i's evaluation and to support its conclusions and recommendations.

Based on the results of our recent annual FISMA assessment,[74] C5i was aware of areas on which it wanted to focus as well as processes and procedures that needed to be strengthened or improved. In addition to reviewing the findings

[73] NIST 800-53, pp. 2-7, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf (accessed on Jan. 29, 2011).

[74] OIG, *2010 Annual FISMA Executive Summary Report*, Report No. 489 (Mar. 6, 2011).

from recent reports,[75] C5i interviewed OIT personnel, reviewed documents provided, and reviewed SEC policies and procedures to find other areas in need of improvement. Those areas were as follows:

- Access Control
- Audit and Accountability
- Configuration Management
- Contingency Planning
- Identity and Authentication
- Planning
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity

The review included an evaluation of the major security components for FISMA 2010 in order to provide recommended OIG responses to the OMB online questionnaire (i.e., information security and privacy items). C5i also completed all data collection instruments related to FISMA 2010 and

- performed the necessary evaluation procedures to answer those questions in OMB Memorandum 10-15,
- compiled an executive summary for the SEC's OIG, and
- performed a detailed security evaluation of two of the SEC's major security components.

The scope also included a review of

- test results from disaster recovery exercises,
- asset management/tracking database,
- screen captures of logs, and
- all SEC policies and procedures pertinent to the required areas.

Methodology. To meet the overall objectives of the assessment of the SEC's continuous monitoring program, C5i conducted interviews with key personnel, made independent observations, and examined documentation provided by SEC officials. Key personnel included system owners, business line managers, OIT representatives, and OIG personnel. These interviews were further held to determine issues that were germane to completing this assessment. C5i reviewed pertinent records and supporting documentation (policies, procedures, roles and responsibilities) to address the evaluation objective. C5i's review of policies and procedures also included discussions with SEC officials and covered the areas identified in the scope.

[75] OIG, *Assessment of SEC's Privacy Program,* Report No. 485 (Sep. 29, 2010), and OIG, *2010 Annual FISMA Executive Summary Report*, Report No. 489 (Mar. 6, 2011).

C5i staff members were provided with Certification and Accreditation packages, including plan of action and milestones, incident response documentation, pertinent SEC policies and procedures, DR plans, and after-action reports, for review and evaluation to ensure compliance with FISMA, NIST, and OMB guidance. C5i also reviewed an extensive collection of system data, policies, procedures, and other documentation relating to the systems and issues identified above. C5i relied on its analysis of all the information provided from various sources, including testimonial evidence, prior review coverage, and all documentation provided.

Management Controls. Consistent with the objectives of the review, C5i did not assess OIT's management control structure or its internal controls. C5i evaluated existing controls at the Commission specific to the assessment which are detailed above in the scope. C5i relied on information requested and supplied by OIT and interviews with OIT personnel to thoroughly understand OIT's management controls pertaining to policies, methods of operation, and procedures.

Use of Computer-Processed Data. C5i did not assess the reliability of OIT's computers because it did not pertain to C5i's review objectives. Further, C5i did not perform any tests on the general or application controls over OIT's automated systems, as this was not within the scope of the review. C5i believes that the information that was retrieved from SEC's systems, as well as the requested documents provided to us, was sufficient, reliable, and adequate to use in meeting C5i's stated objectives. C5i reviewed the following computer-processed data (i.e., Excel spreadsheets and MS Project plans) that OIT staff members provided to us:

- DR test scripts, test results, and after-action report,
- compliance workbook detailing the status of Certification and Accreditation of SEC systems,
- screenshots of system logs
- list of OIT COTR's, and
- differences between the SEC production environment and the OIT test environment.

Prior OIG Coverage. The following four prior OIG reports are relevant to this review:

- OIG Report No. 489, *2010 Annual FISMA Executive Summary Report*, issued on March 3, 2011, which contained eight recommendation to strengthen the commission's security posture.

- OIG Report No. 485, *Assessment of the SEC's Privacy Program*, issued on September 29, 2010, which contained 20 recommendations to strengthen and improve the Commission's security posture for protecting personally identifiable information.

- OIG Report No. 476, *Evaluation of the SEC Encryption Program*, issued on March 26, 2010, which contained three recommendations to strengthen the IT management controls for safeguarding the Commission's information.

- OIG Report No. 475, *Evaluation of the SEC Privacy Program*, issued on March 26, 2010, which contained one recommendation to manage and operate the privacy program with appropriate internal controls, privacy controls, and oversight.

Judgmental Sampling. C5i identified a population (universe) of five SEC contractors, employed by C5i, assigned to this assessment to test the adherence of help desk staff to the procedures for password reset requests. Each test was performed via telephone—three from SEC offices, one from C5i offices, and one from a personal cell phone.

C5i personnel sat with OIT personnel to perform a review of logs to verify historical data. The C5i technician judgmentally requested logs for ad hoc dates, which were retrieved for the technician in real time.

Criteria and Guidance

OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (April 21, 2010). Provides instructions for meeting agency FY 2010 reporting requirements under the Federal Information Security Management Act of 2002 (Title III, Pub. L. No. 107-347). It also includes reporting instructions for agency privacy management programs.

NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems,* (May 2010). Provides guidance on developing and implementing a Contingency Plan for information systems.

NIST SP 800-40, Version 2.0, *Creating a Patch and Vulnerability Management Vulnerability* (November 2005). This document provides guidance for establishing and maintaining an effective patch and vulnerability management program.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* Special Publication 800-53, Revision 3 (Updated May 1, 2010). Provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.

NIST SP 800-86, *Guide to Integrating Forensic Techniques Into Incident Response* (August 2006). Provides detailed information on establishing a forensic capability, including the development of policies and procedures. Its 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 800-92, *Guide to Computer Security Log Management* (September 2006). Provides guidance on the generation, review and retention of computer logs and log data.

NIST SP 800-123, *Guide to General Server Security* (July 2008). Provides guidance for the securing servers deployed on a network.

Federal Information Security Management Act of 2002, (Title III, Pub. L. No. 107-347, Dec. 17, 2002). Requires each federal agency 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.

E-Government Act of 2002, (Pub. L. No. 107-347) (Dec. 17, 2002). The purpose of this act is 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 (February 2004). 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 (March 2006). Outlines the minimum security requirements for the security of federal information systems.

SEC Policies:

- OIT-00047-001.0, Disaster Recovery Planning Procedures (February 4, 2003)
- OIT 24-04.09, IT Security Business Continuity Management Program (December 12, 2005)
- SEC Implementing Instruction 24-04.09.01 (02.0), System Business Impact Analysis (December 12, 2005)
- OIT-00003-001.0, Disaster Recovery Planning Policy (August 6, 2002)
- SEC Implementing Instruction II 24-04.06.01 (01.1), Identification and Authentication (July 9, 2008)
- OIT 00015.002.0, Asset Management Procedure (July 8, 2003)
- OIT-00062-003.0, Procedure for Documenting Permanent and Temporary IT Asset Transactions (March 18, 2003)
- OIT 41-07-007-001.0, Password Reset Procedures for Remote and LAN Accounts (April 16, 2002)
- OIT Implementing Instruction 24-05.04.03, Patch Management (December 28, 2005)
- OIT 24-05.02.04.07, Safeguarding Procedures for Non-Public Backup Media (March 14, 2007)
- SECR 24-2.6, Enterprise Backup of Electronic Data (May 15, 2003)
- OD-24-05.09 (01.0), IT Asset Management Program (July 30, 2009)
- OIT-00062-003.0, Procedure for Documenting Permanent and Temporary IT Asset Transactions (March 18, 2003)
- OP 24-06.04.01.01(01.2), Contractor Entry and Exit (July 18, 2006)
- Draft OAS Policy, Contractor Personnel Employment Entrance and Exit Procedures
- OP 24-06.04.01.02.T01, Contractor Entry Form (March 27, 2007)

- OP 24-06.04.01.02.T02, Contractor Exit Form (July 18, 2006)
- OIT OP 24-05.01.02.T01, Request for Account Creation, Modification, Termination, or Transfer (May 23, 2006)

Appendix IV

[redacted] for External and Internal Applications

Table 4. [redacted] [redacted], [redacted]

External Applications
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

Source: OIG-generated.

Table 5. Internal Applications [redacted] During [redacted]

Internal Applications	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		
[redacted]			[redacted]
[redacted]	[redacted]		[redacted]
[redacted]			[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Internal Applications	[redacted]	[redacted]	[redacted]
[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		[redacted]
[redacted]			[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Source: OIG-generated.

.

Screenshots

Figure 1. Event Logs: [redacted]

[redacted]

Source: Generated by OIT, [redacted]

Figure 2. Event Logs: Historical Archives [redacted]

[redacted]

Source: Generated by OIT, [redacted]

Figure 3. Event Logs: Historical Archives [redacted]

[redacted]

Source: Generated by OIT, [redacted]

Figure 4. Active Directory Logs: [redacted]

[redacted]

Source: Generated by OIT, [redacted]

Figure 5. Active Directory Logs: [redacted]

[redacted]

Source: Generated by OIT, [redacted]

Figure 6. Active Directory Logs: [redacted]

[redacted]

Source: Generated by OIT, [redacted]

Figure 7. Active Directory Logs: [redacted]

[redacted]

Source: Generated by OIT, [redacted]

Figure 8. ADC [redacted] [redacted]

[redacted]

Source: Generated by OIT, [redacted]

Figure 9. ADC [redacted] [redacted]

[redacted]

Source: Generated by OIT, [redacted]

Figure 10. OPC [redacted] [redacted]

[redacted]

Source: Generated by OIT, [redacted]

List of Recommendations

Recommendation 1:

The Office of Information Technology (OIT) should review the Commission's Microsoft Active Directory settings and make the necessary changes to ensure that OIT password policy requirements, as documented in the Implementing Instruction, are strictly enforced for both on-site and remote users and that the documented password structure set forth in OIT policy is strictly enforced.

Recommendation 2:

The Office of Information Technology help desk should begin using a random password generator to create temporary passwords and require users to [redacted] on their [redacted]

Recommendation 3:

The Office of Information Technology (OIT) should implement training for [redacted] personnel to ensure that [redacted] technicians consistently verify users' information in accordance with OIT policy when they receive requests to change user accounts and passwords.

Recommendation 4:

The Office of Information Technology should ensure that security controls configurations that are applied in the production environment are identical with those applied in the testing environment.

Recommendation 5:

The Office of Information Technology should develop and implement written procedures to ensure consistency in the Commission's production and testing environments. These procedures should detail the software and hardware components in both environments and specify the actions required to maintain consistent environments.

Recommendation 6:

The Office of Information Technology should complete and finalize written server and storage log management policies and procedures that fully document the roles and responsibilities for log capture, management, retention and separation of duties.

Recommendation 7:

The Office of Information Technology should require that the [redacted] and the [redacted] have consistent, appropriately installed application and system configuration files to ensure the ability to successfully failover and/or restore in the event of a disaster.

Recommendation 8:

The Office of Information Technology should fully document and communicate the criteria used to determine the success or failure of an application during the Disaster Recovery tests to ensure consistent reporting of results and alleviate confusion.

Recommendation 9:

The Office of Information Technology should analyze the level of criticality of the Commission data being [redacted], and the needs and wants of its customers, and establish an appropriate backup retention period based on the results of that analysis and that meets the requirements of the Commission.

Recommendation 10:

The Office of Information Technology should ensure that [redacted] from the Commission's [redacted] are sent to an [redacted]

Recommendation 11:

The Office of Administrative Services should work with the Office of Information Technology to develop and implement a comprehensive Commission–wide policy for the Entry and Exit of Contractors.

Recommendation 12:

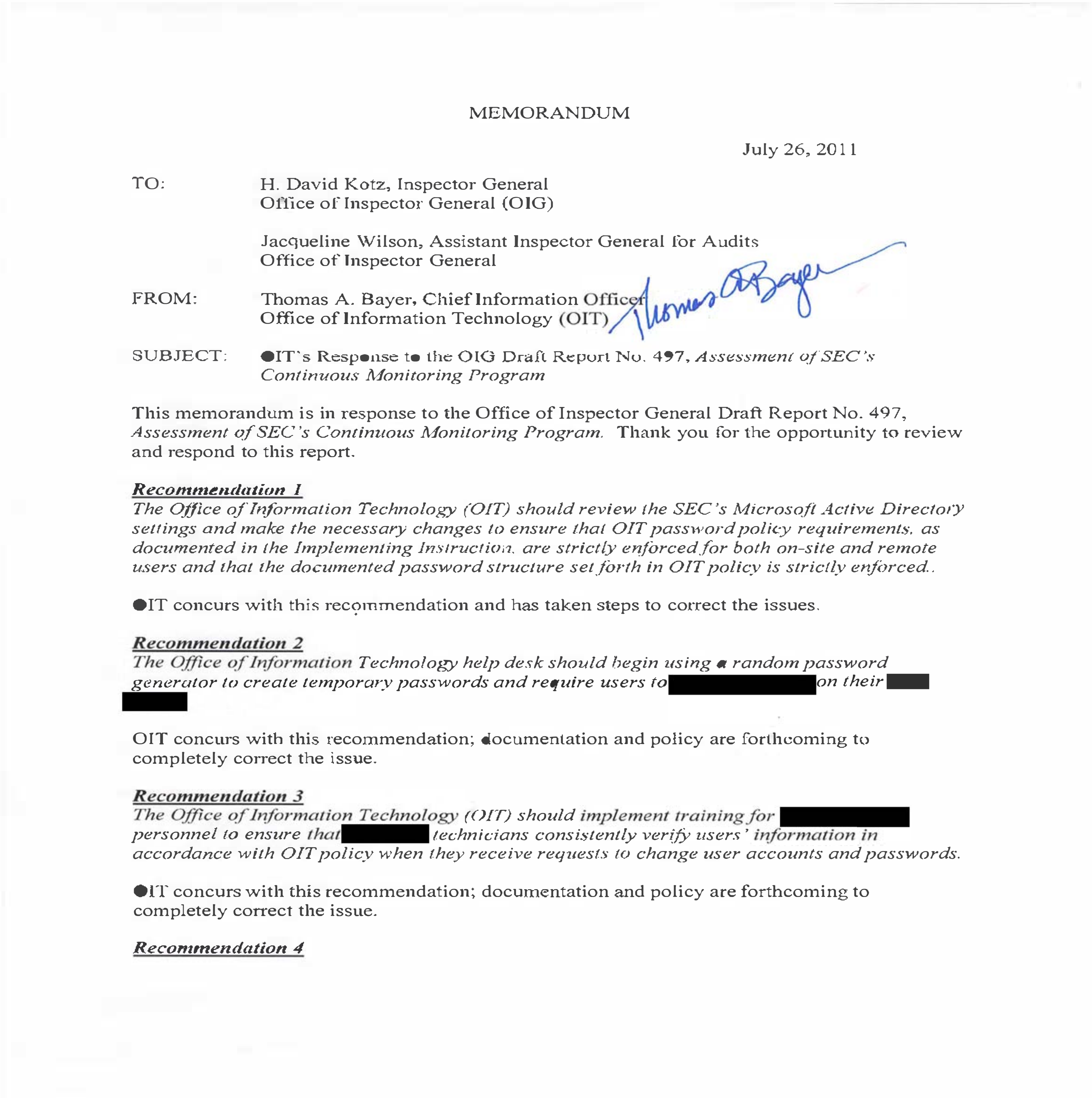
After the Office of Administrative Services (OAS) contractor entry and exit policy, Contractor Personnel Employment Entrance and Exit Procedures, has been finalized and approved, OAS should provide training and communicate with responsible parties, such as Contracting Officers, Contracting Officer's Technical Representatives, and Inspection and Acceptance Officials, regarding their roles and responsibilities and proper procedures with respect to contractor entry into and exit from the Commission.

Recommendation 13:

The Office of Human Resources, Office of Information Technology (OIT), Office of Administrative Services, and the contracting office should perform, at a minimum, a [redacted] of separated/terminated employees and contractors to ensure that OIT has received all account termination notices and has deactivated the appropriate accounts in a timely manner.

Appendix VII

Management's Comments



MEMORANDUM

July 26, 2011

TO: H. David Kotz, Inspector General
Office of Inspector General (OIG)

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

FROM: Thomas A. Bayer, Chief Information Officer
Office of Information Technology (OIT)

Thomas A Bayer

SUBJECT: ●IT's Resp●nse t● the OIG Draft Report No. 497, *Assessment of SEC's Continuous Monitoring Program*

This memorandum is in response to the Office of Inspector General Draft Report No. 497, *Assessment of SEC's Continuous Monitoring Program*. Thank you for the opportunity to review and respond to this report.

Recommendation 1
The Office of Information Technology (OIT) should review the SEC's Microsoft Active Directory settings and make the necessary changes to ensure that OIT password policy requirements, as documented in the Implementing Instruction, are strictly enforced for both on-site and remote users and that the documented password structure set forth in OIT policy is strictly enforced..

●IT concurs with this recommendation and has taken steps to correct the issues.

Recommendation 2
The Office of Information Technology help desk should begin using ● random password generator to create temporary passwords and re●uire users to [redacted] *on their* [redacted]

OIT concurs with this recommendation; documentation and policy are forthcoming to completely correct the issue.

Recommendation 3
The Office of Information Technology (OIT) should implement training for [redacted] *personnel to ensure that* [redacted] *technicians consistently verify users' information in accordance with OIT policy when they receive requests to change user accounts and passwords.*

●IT concurs with this recommendation; documentation and policy are forthcoming to completely correct the issue.

Recommendation 4

The Office of Information Technology should ensure that security controls configurations that are applied in the production environment are identical with those applied in the testing environment.

OIT concurs with this recommendation.

Recommendation 5
The Office of Information Technology should develop and implement written procedures to ensure configuration consistency in the Commission's production and testing environments. These procedures should detail the software and hardware components in both environments and specify the actions required to maintain consistent environments.

OIT concurs with this recommendation.

Recommendation 6
The Office of Information Technology should complete and finalize written server and storage log management policies and procedures that fully document roles and responsibilities for log capture, management, retention and separation of duties.

OIT concurs with this recommendation.

Currently, all SEC systems send their system security logs to an independent OIT Security log aggregation system. OIT Security staff and contractors have the ability to programmatically review and alert on security events independent of the event source. The OIT Security event aggregation system enforces the separation of incompatible duties. OIT agrees that documentation needs to be updated to reflect our desired log management practices and separation of duties within our Servers and Storage Branch.

Recommendation 7
The Office of Information Technology *should require that the* [redacted] *and the* [redacted] *have consistent, appropriately installed application and system configuration files to ensure the ability to successfully failover and/or restore in the event of a disaster.*

OIT concurs with this recommendation and has taken steps to develop and implement procedures that will routinely verify system failover configuration

Recommendation 8
The Office of Information Technology should fully document and communicate the criteria used to determine the success or failure of an application during the DR tests to ensure consistent reporting of results and alleviate confusion.

OIT concurs with this recommendation and has taken the actions to comply with the recommendation.

Recommendation 9

The Office of Information Technology should analyze the level of criticality of SEC data being [redacted] *and the needs and wants of its customers, and establish an appropriate backup retention period based on the results of that analysis and that meets the requirements of the Commission.*

OIT concurs with this recommendation and has developed investment plan to comply with this recommendation.

Recommendation 10
The Office of Information Technology should ensure that [redacted] *from the SEC* [redacted] *are sent to an* [redacted].

OIT concurs with this recommendation.

Recommendation 11
The Office of Administrative Services should work with the Office of Information Technology to develop and implement a comprehensive Commission--wide policy for the Entry and Exit of Contractors.

OIT concurs with this recommendation and will provide assistance to OAS to implement this Commission-wide policy.

Recommendation 13
The Office of Human Resources, Office of Information Technology (OIT), Office of Administrative Services, and the contracting office should perform, at a minimum, a [redacted] *of separated/terminated employees and contractors to ensure that OIT has received all account termination notices and has deactivated the appropriate accounts in a timely manner.*

OIT concurs with this recommendation.

Appendix VII

MEMORANDUM

To: H. David Kotz
Inspector General
Office of Inspector General

From: Jayne L. Seidman
Acting Associate Executive Director
Office of Administrative Services

Jayne Seidman

Date: August 8, 2011

Subject: Response to Draft Report #497, "Assessment of SEC's Continuous Monitoring Program"

I appreciate the opportunity to review and provide formal comments on the OIG's draft report.

Recommendation 11: OAS should work with the OIT to develop and implement a comprehensive Commission--wide policy for the Entry and Exit of Contractors.

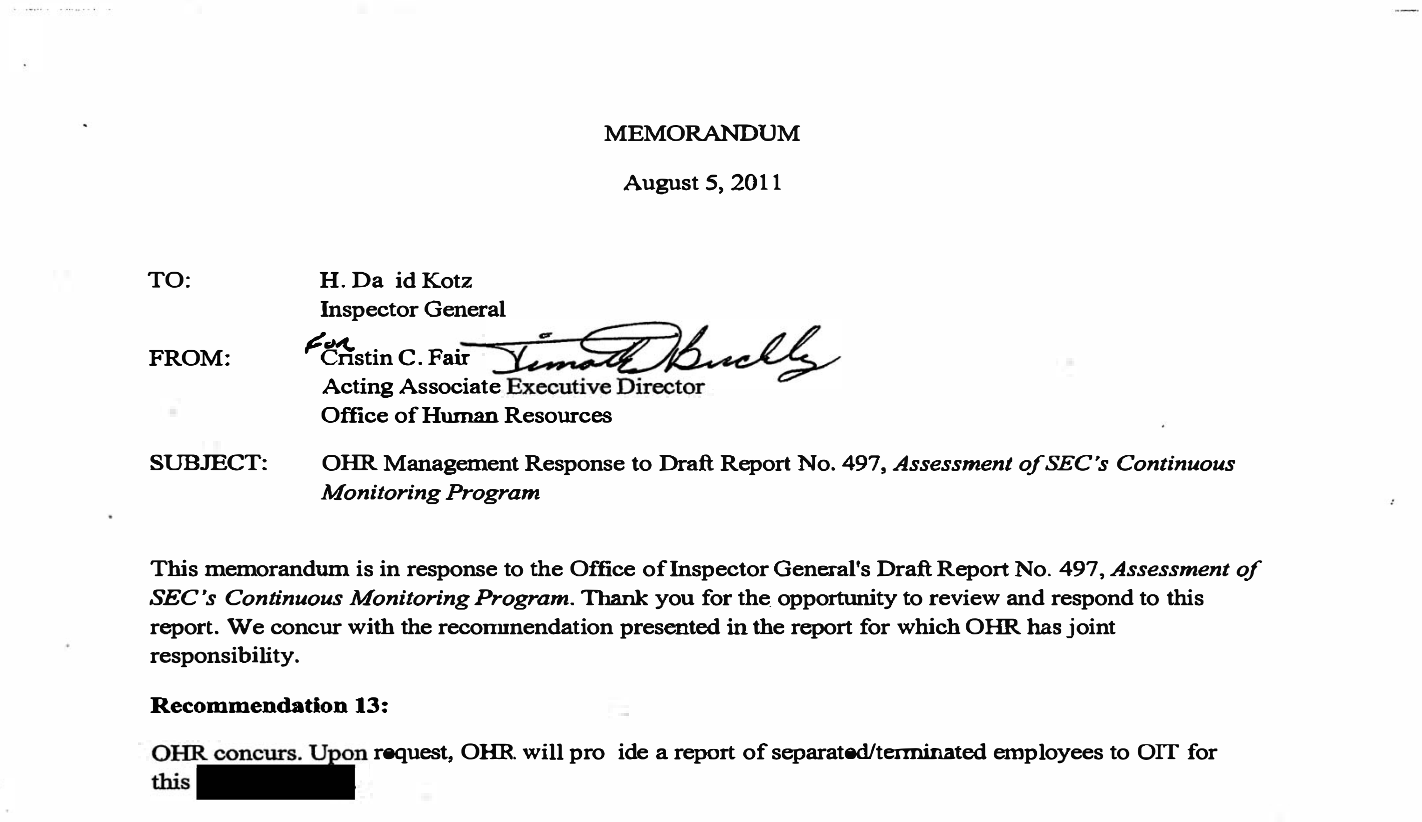
OAS concurs. OAS will implement an agency-wide policy for entry and exit of contractors. The policy will establish the roles and responsibilities of administrative officers, COTRs, and contractor points of contact, and include references to other pertinent policies and procedures.

Recommendation 12: After the OAS contractor entry and exit policy, Contractor Personnel Employment Entrance and Exit Procedures, has been finalized and approved, OAS should provide training and communicate with responsible parties, such as Contracting Officers, Contracting Officer's Technical Representatives, and Inspection and Acceptance Officials, regarding their roles and responsibilities and proper procedures with respect to contractor entry into and exit from the Commission.

OAS concurs. OAS will facilitate training on the agency-wide policy on entry and exit of contractor employees, and communicate with responsible parties regarding their roles and responsibilities and proper procedures.

Recommendation 13: OHR, OIT, OAS, and the contracting office should perform, at a minimum, a [redacted] of separated/terminated employees and contractors to ensure that OIT has received all account termination notices and has deactivated the appropriate accounts in a timely manner.

OAS concurs with respect to contractor staff. OAS will support OIT's audit for the specific roles identified and assigned to OAS in the policy.



MEMORANDUM

August 5, 2011

TO: H. Da id Kotz
Inspector General

FROM: For Cristin C. Fair Timothy Buckley
Acting Associate Executive Director
Office of Human Resources

SUBJECT: OHR Management Response to Draft Report No. 497, *Assessment of SEC's Continuous Monitoring Program*

This memorandum is in response to the Office of Inspector General's Draft Report No. 497, *Assessment of SEC's Continuous Monitoring Program*. Thank you for the opportunity to review and respond to this report. We concur with the recommendation presented in the report for which OHR has joint responsibility.

Recommendation 13:

OHR concurs. Upon request, OHR will pro ide a report of separated/terminated employees to OIT for this [redacted].

OIG Response to Management's Comments

We are pleased that OIT, OAS, OHR concurred with all 13 recommendations addressed to their respective offices. We are also encouraged that OIT, OAS, and OHR indicated they will work together to implement the recommendations that were addressed jointly to their offices.

OIT indicated that it has already taken steps to implement several of the recommendations. Further, OAS has indicated that it will implement an agency-wide policy for entry and exit of contractors, facilitate training on the agency-wide policy for entry and exit of contractors after the policy has been finalized and approved, and will provide support to OIT for the [redacted] of separated/terminated employees and contractors. Additionally, OHR indicated it will provide a report of separated/terminated employees to OIT for the [redacted] as well. We believe OIT, OAS, and OHR's proposed actions are responsive to the report's findings and recommendations.

We believe the swift implementation of all these important recommendations will significantly improve the SEC's continuous monitoring program, which is vital to helping the SEC track the security state of its information systems in a highly dynamic operating environment with changing threats, vulnerabilities, technologies, and missions and business processes.

Audit Requests and Ideas

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

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

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

Hotline

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

Telephone: 877.442.0854

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