



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

Assessment of SEC's System and Network Logs



March 16, 2012
Report No. 500

Assessment and Review Conducted by C5i Federal, Inc.

REDACTED PUBLIC VERSION



OFFICE OF
INSPECTOR GENERAL

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

MEMORANDUM

March 16, 2012

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

From: Noelle Maloney, Acting Inspector General, Office of Inspector General (OIG) *nm*

Subject: *Assessment of SEC's System and Network Logs, Report No. 500*

This memorandum transmits the U.S. Securities and Exchange Commission OIG's final report detailing the results on our assessment of SEC's system and network logs. 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 eight recommendations which if fully implemented should strengthen OIT's controls over the Commission's system and network logs. OIT concurred with all the recommendations. Your written response to the draft report is included in Appendix VI.

Within the next 45 days, please provide the OIG with a written corrective action plan that is designed to address the 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. We appreciate the courtesy and cooperation that you and your staff extended to our audit staff and contractors.

Attachment

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

Assessment of SEC's System and Network Logs

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 Commission's response to the Office of Management and Budget (OMB) Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.¹ The response was completed and submitted to OMB in November 2010 and reported on by the OIG in its report, *2010 Annual FISMA Executive Summary Report*.² As part of its work, C5i conducted an assessment and review of the SEC's continuous monitoring of information technology operations audit logs, and the OIG documented the results of the assessment report *Assessment of SEC's Continuous Monitoring Program*.³ During its assessment of the SEC's continuous monitoring program, C5i found—based on its review of a judgmental sample number of [REDACTED] logs and [REDACTED] server logs—that the SEC Office of Information Technology (OIT) was capturing user identification and log-in/log-out times on [REDACTED]. However, C5i was unable to verify whether all log settings and user activities were being captured for all servers. As a result, on May 17, 2011, the OIG modified its contract with C5i to conduct an in-depth technical assessment of a sample of the [REDACTED] located within the SEC's enterprise network,⁴ to determine whether audit log data were being captured consistent with the requirements of the Federal Information Security Management Act (FISMA), Federal Information Processing Standards (FIPS), and the National Institute of Standards and Technology (NIST) guidelines.

Objectives. The overall objective of this review was to independently evaluate and report on how the Commission has implemented information security requirements for audit log management, including the generation, review, protection, and retention of audit logs. An additional objective was to review system and network logs in the SEC enterprise network, access controls to logs, controls over log management and analysis, data log collection, and log storage.

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

² OIG, *2010 Annual FISMA Executive Summary Report*, Report No. 489 (Mar. 3, 2011).

³ OIG, *Assessment of SEC's Continuous Monitoring Program*, Report No. 497 (Aug. 11, 2011).

⁴The sample includes SEC's operations center, headquarters and the regional offices.

Results. C5i's technical assessment of SEC's system and network logs found that audit log events were not captured for all [REDACTED] servers. C5i's review consisted of comparing server logs collected by the OIG in February 2011 with logs that were collected in June 2011, as well as reviewing additional servers that were located in the SEC's Enterprise network. Specifically, [REDACTED] servers in C5i's judgmental sample did not log auditable events because the server's logging capacity had been exceeded. Also, there is no mechanism in place to alert OIT's Servers and Storage Branch or OIT's Security Branch when servers have reached their capacity and stopped performing logging functions. C5i found that the OIT Servers and Storage Branch did not actively monitor server logs and did not have an alerting mechanism to provide notification of when a sever was no longer logging events. Although OIT's Security Branch monitors logs, an alerting mechanism does not exist. Both the OIT Servers and Storage Branch and the OIT Security Branch were unaware that the three servers were not logging events.

C5i also found that OIT's policies and procedures for audit log capture and management were outdated and do not clearly define required components such as roles and responsibilities. C5i reviewed five formal, documented policies and procedures specific to audit log capture and management. C5i found that only one of these policies was current and the other policies had not been reviewed or updated based on the "anticipated review date" identified in each policy. In addition, C5i found that OIT does not have documented policies and procedures for application database log management. Further, our review of log capture and log management (including capacity planning and identification of roles and responsibilities of persons involved in log management) found that OIT does not have documented policies and procedures for reviewing server logs to ensure that log capacity has not been exceeded or for alerting OIT officials when the capacity is exceeded. In previously-issued reports the OIG found that OIT's security policies and procedures were outdated but none of the policies and procedures were related specifically to logs. OIT is aware that the vast majority of their policies and procedures are outdated and has taken action to address this matter.

Additionally, C5i found [REDACTED] servers identified as decommissioned were still actively connected to the SEC's Enterprise networks and were still accessible. Further, C5i found that one of the servers had stopped performing logging functions. Decommissioned servers remained accessible on the SEC network and, of those examined, one was not capturing logs.

Also, C5i found that logs are not generated consistently for application databases because the audit trail functionality that is built into the database is not always available, which has resulted in OIT not being able to capture logs for all auditable events. OIT informed C5i that resources have now been dedicated to address this matter.

Lastly, OIT's Servers and Storage Branch and OIT's Security Branch do not have an alerting mechanism to notify appropriate personnel when [REDACTED] are full or have stop performing logging functions. Although OIT does not have an alerting mechanism to notify it when logs are no longer performing logging functions, OIT informed C5i that the office plans to deploy a tool that will provide OIT with this capability in the near future.

Summary of Recommendations. We recommend OIT take the following actions to enhance the SEC's system and network logs.

- (1) OIT should identify capacity requirements for all servers, ensure sufficient capacity is available for the storage of audit records, configure auditing to reduce the likelihood that capacity will be exceeded, and implement an alerting mechanism to alert and notify appropriate office/divisions when log storage capacity is reached.
- (2) When updating its policies and procedures, OIT should include log management language that
 - Identifies the roles and responsibilities of staff who are involved in log management,
 - requires server logs to be periodically reviewed to check whether log capacity has been exceeded, and
 - requires appropriate OIT officials be notified when audit logging functions are suspended when log storage capacity has reached its limit.
- (3) OIT should review and update all logging policies and procedures consistent with the policy's review interval requirements and retain evidence of its reviews and any updates to the policy.
- (4) OIT should ensure that all servers connected to the Commission's enterprise network are configured to have logging enabled.
- (5) OIT should update Server Decommission Guidelines and include language to fully document each action that should be performed when decommissioning a server. OIT should also develop a server decommissioning checklist to be included in the Server Decommission Guidelines.
- (6) OIT should conduct a review of application database log management and generation procedures to ensure audit events are being captured and retained, consistent with OIT policies and procedures and National Institute of Standards and Technology guidelines.

- (7) OIT should implement a mechanism to notify OIT's Server and Storage Branch, or OIT's Security Branch when [REDACTED] stop performing [REDACTED] functions.
- (8) OIT should implement its plan to develop a computer script that determines whether [REDACTED] are producing [REDACTED]

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

TABLE OF CONTENTS

Executive Summary	ii
Table of Contents	vi
Background and Objectives	1
Background	1
Objectives	2
Findings and Recommendations	3
Finding 1: Audit Log Events Are Not Being Captured for All [REDACTED] [REDACTED] Servers	3
Recommendation 1	9
Finding 2: OIT Audit Logging Policies and Procedures for SEC Network Servers Should be Revised and Reviewed According to Its Current Policy	10
Recommendation 2	12
Recommendation 3	12
Finding 3: Decommissioned Servers Remain Active on the SEC Network	13
Recommendation 4	14
Recommendation 5	14
Finding 4: Application Database Logs Are Not Generated	15
Recommendation 6	15
Finding 5: OIT Does Not Have a Monitoring and Alerting Mechanism for [REDACTED] Failure	16
Recommendation 7	17
Recommendation 8	17
Appendices	
Appendix I. Abbreviations	18
Appendix II. Scope and Methodology	19
Appendix III. Criteria	22
Appendix IV. Screenshots	23
Appendix V. List of Recommendations	28
Appendix VI. Management's Comments	30
Appendix VII. OIG Response to Management's Comments	33

Tables

Table 1. Servers Eliminated from Initial Judgmental Sample 4
Table 2. Sampled Servers Not Capturing Logs 5
Table 3. Servers Eliminated from Additional Judgmental Sample Used in
Log Comparison 6
Table 4. Server From Additional Judgmental Sample Not Performing
Logging Functions 7

Figures

Figure 1. [REDACTED] Log, October 17, 2011 23
Figure 2. [REDACTED], Verified
June 18, 2011 23
Figure 3. [REDACTED], Verified
June 18, 2011 24
Figure 4. [REDACTED] Verified
June 18, 2011 25
Figure 5. [REDACTED] Verified June 18, 2011 26
Figure 6. [REDACTED] Verified June 18, 2011 27

Background and Objectives

Background

Overview. In August 2010, the U.S. Securities and Exchange Commission (SEC or Commission) Office of Inspector General (OIG) contracted with C5i Federal, Inc. (C5i) to assist with the completion and coordination of OIG's input to the Commission's response to Office of Management and Budget (OMB) Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.⁵ The response was completed and submitted to OMB in November 2010 and reported on by the OIG in the report *2010 Annual FISMA Executive Summary Report*.⁶ As part of its work, C5i conducted an assessment and review of the SEC's continuous monitoring of information technology operations audit logs, and the results of the assessment were documented by the OIG in the report *Assessment of SEC's Continuous Monitoring Program*.⁷

During its assessment of the SEC's continuous monitoring program, C5i found—based on its review of a judgmental sample number of [REDACTED] logs and [REDACTED] server logs—that the SEC Office of Information Technology (OIT) was capturing user identification and log-in/log-out times on [REDACTED]. However, without conducting a more in-depth analysis, C5i was unable to verify whether all log settings and user activities were being captured for all servers. To assist the OIG in conducting an in-depth assessment of logs, on February 2, 2011, at the OIG's request, OIT collected and provided a hard drive with audit log records from all OIT [REDACTED] that were generated from January 4, 2010 to January 30, 2011.

Because OIG was unable to verify log settings and user activities in the log records OIT provided on February 2, 2011, OIG modified its contract with C5i on May 17, 2011, to include a detailed technical assessment on a sample number of the [REDACTED] that are located within the SEC's enterprise network, to determine whether audit log data was being captured consistent with the requirements of the Federal Information Security Management Act (FISMA), Federal Information Processing Standards (FIPS), and the National Institute of Standards and Technology (NIST) guidelines. In addition, the modification to the contract included a comparison of the network logs OIG collected on June 24, 2011, covering the period February

⁵ Office of Management and Budget, Memorandum 10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf.

⁶ OIG, *2010 Annual FISMA Executive Summary Report*, Report No. 489 (Mar. 3, 2011).

⁷ OIG, *Assessment of SEC's Continuous Monitoring Program*, Report No. 497 (Aug. 11, 2011).

⁸The sample includes SEC's operations center, headquarters and the regional offices.

4, 2010 through June 20, 2011, with the system and network logs OIT collected and provided to OIG on February 2, 2011, a review of segregated duties among OIT staff who access SEC enterprise network logs, access controls to logs, controls over log management and analysis, log collection, and log storage.

Objectives

The overall objective of this review was to independently evaluate and report on how the Commission has implemented information security requirements for audit log management, including the generation, review, protection, and retention of audit logs. An additional objective was to review system and network logs in the SEC enterprise network, access controls to logs, controls over log management and analysis, data log collection, and log storage.

Findings and Recommendations

Finding 1: Audit Log Events Are Not Being Captured for All [REDACTED] Servers

Three of 56 servers in the judgmental sample did not log auditable events because the server's logging capacity had been exceeded. There is no mechanism in place to alert OIT's Servers and Storage Branch or OIT's Security Branch when servers have reached their capacity and have stopped performing logging functions.

In connection with this review, C5i conducted a technical assessment of [REDACTED] located in the SEC's enterprise network. In addition, C5i compared SEC enterprise network logs, including systems and application logs, collected in February 2011 to the logs that were collected in June 2011.

FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems (FIPS Publication 200), states that organizations must:

- (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.¹⁰

The OIT Server and Storage Branch provided C5i with a list of [REDACTED] servers representing the various types of servers deployed across the Commission's enterprise network. From this list, C5i identified [REDACTED],¹¹ [REDACTED],¹² [REDACTED]¹³ and [REDACTED], for a

⁹ The sample includes SEC's operations center, headquarters and the regional offices.

¹⁰ FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems (Mar. 9, 2006) p. 2.

¹¹ For the purpose of this report, [REDACTED]

[REDACTED]
For the purpose of this report, [REDACTED]

For the purpose of this report, [REDACTED]

For the purpose of this report, [REDACTED]

total of [REDACTED] items. C5i selected a judgmental sample of [REDACTED] servers from these [REDACTED]. C5i reviewed the servers to assess their log generation and retention, server log capacity, and log monitoring and alerting.

C5i conducted an on-site assessment on Saturday, June 18, 2011, from 6:10 p.m. Eastern Daylight Time (EDT) to 2:15 a.m. EDT on Sunday, June 19, 2011, and on Friday, June 24, 2011, from 10:37 p.m. EDT to 12:47 a.m. EDT on Saturday, June 25, 2011. C5i manually logged onto each server using the administrator-level credentials OIT provided for this assessment. This access level was necessary to properly validate the configuration of event logging and log information being captured.

Elimination of Servers from the Initial Judgmental Sample

C5i attempted to manually log onto each of the [REDACTED] servers identified in its sample and discovered that some servers were not accessible. In three cases, the servers were unresponsive, and in two cases, the server's maximum allowable number of connections had been reached. In addition, two of the servers that C5i was able to access did not allow exporting of their server log configurations. As a result, C5i reduced the number of servers in its judgmental sample [REDACTED]. Table 1 provides details on the seven servers that were removed from the initial sample.

Table 1. Servers Eliminated From Initial Judgmental Sample

System	IP Address	Location	Type of Server	Date and Time of Last Audit Entry	Results
[REDACTED]	[REDACTED]	Atlanta Regional Office	[REDACTED]	6/18/2011 11:50 p.m.	System could not be reached.
[REDACTED]	[REDACTED]	New York Regional Office	[REDACTED]	6/18/2011 12:23 a.m.	System could not be reached.
[REDACTED]	[REDACTED]	Fort Worth Regional Office	[REDACTED]	6/18/2011 12:12 a.m.	Maximum allowable connections had been reached.

¹⁵ See Figure 5. [REDACTED], Verified June 18, 2011, Appendix IV.

System	IP Address	Location	Type of Server	Date and Time of Last Audit Entry	Results
[REDACTED]	[REDACTED]	SEC Operations Center	[REDACTED]	6/18/2011 12:33 a.m.	Maximum allowable connections had been reached.
[REDACTED]	[REDACTED]	Chicago Regional Office	[REDACTED]	6/19/2011 1:26 a.m.	Server log configuration could not be exported.
[REDACTED]	[REDACTED]	San Francisco Regional Office	[REDACTED]	6/18/2011 1:43 a.m.	Server log configuration could not be exported.
[REDACTED]	[REDACTED]	Salt Lake Regional Office	[REDACTED]	6/18/2011 1:16 a.m.	System could not be reached.

Source: OIG-generated

Of the [REDACTED] servers that were accessible [REDACTED] C5i found that [REDACTED] and [REDACTED] did not capture logs because the logs were full. In these cases, C5i received the following warning message: "The security log on the system is full." As shown in Table 2, C5i found that logs for one of the servers had not been captured for nine days.

Table 2. Sampled Servers Not Capturing Logs

System	IP Address	Location	Server Type	Date and Time of Last Audit Entry	No. of Days Without Logging (Prior to 6/18/2011)
[REDACTED]	[REDACTED]	SEC Operations Center	[REDACTED]	6/15/2011 4:57:43 p.m.	3
[REDACTED]	[REDACTED]	SEC Alternate Data Center	[REDACTED]	6/9/2011 5:55:37 p.m.	9

Source: OIG-generated

C5i found that all of the print servers and domain controllers in its 40-server sample were performing audit logging functions and generating audit records for the list of audited events.

¹⁶ See Figure 6. [REDACTED] Verified June 18, 2011, Appendix IV.

¹⁷ See Figure 4. [REDACTED] Verified June 18, 2011, Appendix IV.

¹⁸ See Figure 2. [REDACTED] Verified June 18, 2011, Appendix IV.

Log Comparison

C5i compared server logs the OIG collected in February 2011 with the server logs that were captured in June 2011. From the list of [REDACTED] servers provided by the OIT Servers and Storage Branch, C5i selected the following 18 additional server types in the [REDACTED]

C5i found that [REDACTED] additional servers were not accessible. In one case, C5i found that the system could not be reached; in the other case, C5i was unable to access Audit Policy in the server log configuration. Table 3 provides details on the two eliminated servers.

Table 3. Servers Eliminated From Additional Judgmental Sample Used in Log Comparison

System	IP Address	Location	Type of Server	Date and Time of Last Audit Entry	Results
[REDACTED]	[REDACTED]	SEC Alternate Data Center	[REDACTED]	6/18/2011 10:45 p.m.	Not able to access Audit Policy
[REDACTED]	[REDACTED]	SEC Alternate Data Center	[REDACTED]	6/18/2011 11:50 p.m.	System cannot be reached

Source: OIG-generated

C5i also found that one of the accessible servers was not performing audit logging functions for at least one day, as shown in Table 4, because its log were full.

Table 4. Server From Additional Judgmental Sample Not Performing Logging Functions

System	IP Address	Location	Type of Server	Date and Time of Last Audit Entry	Number of Days without Logging (Prior to 6/16/2011)
[REDACTED]	[REDACTED]	SEC Alternate Data Center	[REDACTED]	6/17/2011 5:38:12 a.m.	At least 1 day

Source: OIG-generated

In summary, C5i found that [REDACTED] accessible servers in its judgmental sample (consisting of [REDACTED] servers and [REDACTED] other servers) had been operating without audit log functions for as long as 9 days.²⁰

Log Generation and Retention

C5i found that for most of the SEC servers in its sample, OIT Servers and Storage Branch generates and retains audit logs. C5i found that OIT Servers and Storage Branch has implemented two automated computer scripts to manage and archive log data.²¹ The first script, which runs every day at [REDACTED]; copies the daily audit logs on each server to a temporary storage folder. A second automated computer script, which runs every Monday at [REDACTED] moves the daily audit logs from the temporary storage folder to a centralized log server for retention and archival purposes. OIT Security Branch extracts the logs from the storage folders that are managed by OIT Servers and Storage Branch and analyzes the data using the [REDACTED]. The three servers that C5i previously identified as having exceeded their log capacity and were not generating logs, were subject to this log extraction and analysis process.

C5i contacted OIT Security Branch to confirm that the three servers were not generating security logs on Saturday, June 18, 2011, from 10:00 p.m. to 11:59 p.m. EDT, when C5i performed its onsite assessment. OIT Security confirmed that logs did not exist for that date and time and provided C5i with a screen shot from [REDACTED] showing the result.²²

¹⁹ See Figure 3. [REDACTED]

²⁰ The audit log function produces audit records that contain sufficient information to establish the type of logged event that has occurred, when (date and time) the event occurred, where (IP Address) the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user or subject associated with the event.

²¹ A script is a program or sequence of instructions that is carried out by a computer without user interaction.

²² See Figure 1, [REDACTED] October 17, 2011, Appendix IV.

Server Log Capacity

NIST SP 800-53 recommends that an organization allocate audit record storage capacity and configure auditing “to reduce the likelihood of such capacity being exceeded.”²³

As noted above, C5i found three servers for which logs were not being generated because log capacity had been reached. C5i manually compared the servers log configuration settings with the [REDACTED] configuration.²⁴ Using the list of [REDACTED] configuration provided by OIT Servers and Storage Branch, C5i confirmed that at the server level, the configuration settings were implemented according to the [REDACTED] settings as defined by OIT.

C5i determined that a maximum log capacity of [REDACTED] had been configured and implemented across the Commission’s network by a [REDACTED]. C5i also found that a log setting, “Do Not overwrite events (clear log manually)” had been configured on servers to prevent overwriting of previously generated logs. Once a log reached capacity, any future logging will not be captured unless and until the OIT Servers and Storage Branch performs a manual check and clears or moves the last-created logs to free up capacity for additional logging.

Monitoring and Alerting

In addition to the requirement that organizations create, protect, and retain information system audit records,²⁵ NIST SP 800-53 recommends that information systems alert designated organization officials in the event of an audit processing failure, such as audit storage capacity being reached or exceeded.²⁶

C5i interviewed staff from OIT’s Servers and Storage Branch and OIT’s Security Branch to determine whether they were aware of the impaired logging issues and whether an alerting mechanism was in place to notify them if a server stops performing logging functions. OIT Servers and Storage Branch informed C5i that it was not actively monitoring the logs and did not have an alerting mechanism in place to receive notifications when a server stops performing required logging functions. C5i also found that although the OIT Security Branch monitors logs using [REDACTED], there is no mechanism in place to notify it when a server has stopped performing required logging functions. Because neither the OIT Servers and Storage Branch, nor the OIT Security Branch has an alerting mechanism in

²³ NIST SP 800-53, Rev. 3, p. F-25.

²⁴ [REDACTED] controls what users can and cannot do on a computer system.

²⁵ FIPS Publication 200, p. 2.

²⁶ NIST SP 800-53, Rev. 3, p. F-26.

place, logging failures could go unnoticed indefinitely until a manual check is performed. C5i discovered that OIT staff first identified this issue in June 2009 and notified both OIT's Service Desk and Customer Care at that time as well as on several occasions thereafter, but to date the problem has not been resolved.

Since the OIT Servers and Storage Branch does not actively monitor logs and does not have an automated alerting mechanism in place to receive notifications when a server stops performing logging functions, OIT may be unaware of audit processing failures for extended periods of time. As a result, OIT's ability to analyze and investigate inappropriate information system activity and ensure that the actions of individual information system users can be traced to those users could be hindered.

The failure to ensure that servers are performing logging functions is inconsistent with FIPS Publication 200 and prevents OIT from actively monitoring, analyzing, investigating, and reporting unlawful, unauthorized, or inappropriate information system activity and from capturing sufficient information to trace back and hold users accountable for their actions on the servers.²⁷

Overall, OIT lacks thorough processes and procedures for ensuring consistent, uninterrupted server logging functions. In particular, OIT lacks adequate capacity planning for server logs and an alerting mechanism for notifying appropriate officials when audit logging functions are suspended because of inadequate capacity or other reasons.

Recommendation 1:

The Office of Information Technology should identify capacity requirements for all servers, ensure sufficient capacity is available for the storage of audit records, configure auditing to reduce the likelihood that capacity will be exceeded, and implement an alerting mechanism to alert and notify appropriate Commission office/divisions when log storage capacity is reached.

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

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

²⁷ FIPS Publication 200, p. 2.

Finding 2: OIT Audit Logging Policies and Procedures for SEC Network Servers Should be Revised and Reviewed According to Its Current Policy

OIT policies and procedures for audit log capture and management are outdated and do not clearly define roles and responsibilities. As a result, OIT's effectiveness at maintaining network security and the critical data that is processed and stored may be hindered.

OIT provided C5i with the following five policies and procedures pertaining to audit log capture and management for the SEC's enterprise network servers:

- Operating Directive (OD) [REDACTED]
- SEC Regulation (SECR) [REDACTED]
- Implementing Instruction [REDACTED]
- Implementing Instruction [REDACTED]
- Operating Procedure (OP) [REDACTED]

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, recommends that organizations develop, disseminate, and review/update, with a frequency defined by the organization, the following:

- a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.²⁸

C5i reviewed OIT's documented policies and procedures pertaining to audit log capture and management to determine whether the polices

²⁸ NIST SP 800-53, Rev. 3, p. F-3.

- had been reviewed in accordance with the frequency specified,
- clearly defined roles and responsibilities,
- contained provisions for segregation of duties among OIT staff accessing the SEC enterprise network,
- included controls for accessing logs,
- provided for management and analysis of logs,
- called for collection of adequate data, and
- provided for sufficient log storage capability.

C5i found that only [REDACTED] appeared to be current, while the other four policies, all of which cited an “anticipated review date” of one year from their approval date, have not been reviewed or updated based on the effective date(s).

C5i’s review of OIT’s policies and procedures related to application database log management confirmed that OIT does not have documented policies and procedures for application database log management. In addition, C5i found that OIT has not defined the roles and responsibilities of individuals who are expected to be involved in log management, as recommended by NIST SP 800-92, which states that “[a]s part of the log management planning process, an organization should define the roles and responsibilities of individuals and teams who are expected to be involved in log management.”²⁹

Further, C5i found that OIT does not have policies and procedures requiring the review of server logs to ensure that log capacity has not been exceeded or for alerting and notify appropriate officials when audit logging functions are suspended due to log storage capacity being reached.³⁰

Consistent with the OIG’s *2011 Annual FISMA Executive Summary Report*, OIT has recently dedicated resources to review and update its policies and procedures to ensure they are consistent with OIT’s current business practices. In addition, OIT informed C5i of its deployment of a new automated tool, Qualys, which provides on-demand vulnerability management and compliance solutions. Among other things, Qualys automates security audits to help ensure that the organization is in compliance with applicable regulations and internal security policies.

²⁹ NIST SP 800-92, p. 4-10.

³⁰ C5i’s current finding that OIT policies are outdated and nonexistent is similar to Finding 1 in the OIG report *2011 Annual FISMA Executive Summary*, issued February 2, 2012. The report found that the policies and procedures specific to the eight Federal Information Security Management Act control areas reviewed were outdated and nonexistent. However, this report did not include a review of OIT’s policies and procedures pertaining to the capture of audit logs, log management, or management of the SEC’s enterprise network servers. Additionally, in response to recommendation 6 in OIG report *Assessment of SEC’s Continuous Monitoring Program*, issued August 11, 2011, OIT agreed that its policies and procedures need to be updated to reflect its desired log management practices and separation of duties needs to be documented.

Because OIT did not review and update policies and procedures pertaining to audit log capture and management at prescribed intervals and did not provide clearly defined roles and responsibilities for audit log functions, OIT's ability to effectively maintain network security and protect critical data may be limited.

Recommendation 2:

When updating its policies and procedures, the Office of Information Technology (OIT) should include log management language that

- identifies the roles and responsibilities of staff who are involved in log management,
- requires server logs to be periodically reviewed to check whether log capacity has been exceeded, and
- requires appropriate OIT officials be notified when audit logging functions are suspended when log storage capacity has reached its limit.

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

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

Recommendation 3:

The Office of Information Technology should review and update all logging policies and procedures consistent with the policy's review interval requirements and retain evidence of its reviews and any updates to the policy.

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

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

Finding 3: Decommissioned Servers Remain Active on the SEC Network

Decommissioned servers remained accessible on the SEC network and, of those examined, one was not capturing logs. In addition, OIT's Server Decommission Guidelines should include a checklist to ensure that all required decommissioning activities are implemented.

From the [REDACTED] servers in our sample, we identified [REDACTED] decommissioned servers. All [REDACTED] of the decommissioned servers were file servers. C5i then examined a judgmental sample of [REDACTED] decommissioned file servers to determine whether OIT had executed the required actions related to risk management for systems removed from operation, as specified in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, including updating organizational tracking and management systems to indicate the specific information system components being removed from service.³¹

C5i found that the four decommissioned servers in our sample were still actively connected to SEC's enterprise network and were accessible. Further, C5i found that one of the servers had stopped performing audit logging functions. Therefore, any activity on that server was not being recorded, which is not consistent to FIPS Publication 200, which states that organizations must "ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions."³² Maintaining active logging-disabled servers on the SEC enterprise network could lead to undetected security breaches and data compromise because OIT cannot actively monitor, analyze, investigate, or report unlawful, unauthorized, or inappropriate activity on such servers.

C5i reviewed OIT Servers and Storage Branch's Server Decommission Guidelines. The guideline pertains to the procedure for decommissioning servers, to determine whether OIT had implemented an information system decommissioning strategy that "executes required actions when a system is removed from service," as called for in NIST SP 800-37, including ensuring that "all security controls addressing information system removal and decommissioning (e.g., media sanitization, configuration management and control) are implemented."³³ Our review found that OIT's Server Decommission Guidelines do not include a documented decommissioning strategy, such as a

³¹ NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Rev. 1 (February 2010), p. 41.

³² FIPS 200, p. 2.

³³ NIST SP 800-37, Rev. 1, p. 41.

checklist that clearly documents each action that should be performed when a server is removed from service. Without a fully documented decommissioning strategy that includes a checklist, OIT cannot readily ensure that all security controls for decommissioning have been consistently implemented.

Recommendation 4:

The Office of Information Technology should ensure that all servers connected to the Commission's enterprise network are configured to have logging enabled.

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 5:

The Office of Information Technology (OIT) should update its Server Decommission Guidelines and include language to fully document each action that should be performed when decommissioning a server. OIT should also develop a server decommissioning checklist to be included in the Server Decommission Guidelines.

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

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

Finding 4: Application Database Logs Are Not Generated

OIT's application database logs are not being generated for auditable events.

According to NIST SP 800-53, information systems should provide audit record generation capability for the list of auditable events, allow designated personnel to select which auditable events are to be audited by specific components of the system, and generate audit records for the list of audited events.³⁴

OIT staff informed C5i that the events captured in application database logs are inconsistent because native database logging—the audit trail functionality built into a database management system—has not been turned on for most database applications. As a result, not all auditable events are captured. In addition, OIT did not identify and select auditable events to be audited for the application database servers. Most database administrators and system owners developed their own audit logging functionality and disabled native database logging because it was resource-intensive and impeded the applications' ability to perform optimally. As a result, OIT is unable to generate audit records for all auditable events. Without native database application logging or secondary systems that provide the same level of detail, OIT is unable to retain audit records to provide support for investigations of security incidents and to meet regulatory and organizational information retention requirements.³⁵

OIT is aware of the issues surrounding application database logging and has designated a staff member to specifically focus on addressing these issues.

Recommendation 6:

The Office of Information Technology (OIT) should conduct a review of application database log management and generation procedures to ensure auditable events are being captured and retained, consistent with OIT policies and procedures and National Institute of Standards and Technology guidelines.

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

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

³⁴ NIST SP 800-53, Rev. 3, p. F-30.

³⁵ NIST SP 800-53, Rev. 3, p. F-30.

Finding 5: OIT Does Not Have a Monitoring and Alerting Mechanism for [REDACTED] Failure

There is no monitoring and alerting mechanism in place to notify OIT's Servers and Storage Branch or the OIT Security Branch if a [REDACTED] stops performing [REDACTED] functions.

[REDACTED] is a standard for logging computer data in a [REDACTED] files contain event information, including panic conditions, data corruption, hardware errors, warnings, and tracking information. [REDACTED] files can be used for computer system management, security events, auditing events, system information analysis, and debugging messages. According to NIST SP 800-53, a control should be in place that “[a]llerts designated organization officials in the event of an audit processing failure.”³⁷

C5i conducted an assessment to review data log collection and controls over log management and analysis and to ensure that log storage is being performed consistently within OIT's [REDACTED]. C5i's interviews with staff in OIT's Servers and Storage Branch and the OIT Security Branch, found that neither Branch has an alerting mechanism in place to notify it if a [REDACTED] server stops performing [REDACTED] functions. The OIT Servers and Storage Branch and the OIT Security Branch also informed C5i that OIT is in the process of replacing an information system tool called [REDACTED]. As part of its deployment of [REDACTED], the OIT Security Branch plans to develop a computer script that would assess each server to determine if the server is producing [REDACTED] and if the configuration on each server is correct.

If a server stops performing logging functions the activity on that server will not be recorded, compromising the organization's ability to manage the computer system, detect and address security events, establish an audit trail of events, analyze or investigate events, or protect against individuals falsely denying having performed particular actions.

³⁶ A Panic condition is an emergency level of a problem in [REDACTED] – e.g., warning, error, emergency.

³⁷ NIST SP 800-53, Rev. 3, AU-5, Response to Audit Processing Failures, p. F-26.

Recommendation 7:

The Office of Information Technology (OIT) should implement a mechanism to notify OIT's Servers and Storage Branch, or OIT's Security Branch when [REDACTED] performing [REDACTED] functions.

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

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

Recommendation 8:

The Office of Information Technology should implement its plan to develop a computer script that determines whether [REDACTED] are producing [REDACTED]

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

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

Abbreviations

EDT	Eastern Daylight Time
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
OD	Operating Directive
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OP	Operating Procedure
SEC or Commission	U.S. Securities and Exchange Commission
SECR	SEC Regulation
SP	Special Publications

Scope and Methodology

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

Scope. The assessment covered the period from January 2010 to August 2011. The review consisted of detailed technical assessment samplings of [REDACTED] located within the SEC's enterprise network located at the SEC's operations center, headquarters and regional offices. Further, the assessment included a comparison and analysis of audit log records, obtained on an external hard drive, from all OIT [REDACTED] that were generated between January 4, 2010, and October 23, 2010, with audit log records generated by the same servers [REDACTED] between January 29, 2011, and June 23, 2011, to identify changes in controls and logging requirements. The log analysis included determining whether the servers were performing audit logging functions; determining whether critical auditable security event types were being logged, including: privilege escalation attempts, password guessing attempts, user session activity, changes to user permissions and user accounts, log-in/out, modifications to information systems or application software, and system startup/shutdown; and comparing the actual logs with the [REDACTED] audit logging settings for consistency.

Methodology. To meet the overall objectives to assess the various types of servers deployed at the Commission and located within the enterprise network, 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 relevant to completing this assessment. C5i reviewed pertinent data log records and supporting documentation (policies, procedures, roles and responsibilities) to address the review objectives. C5i's review of policies and procedures also included discussions with SEC officials and covered the areas identified in the scope.

In addition, C5i obtained a detailed list of [REDACTED] servers representing the various types of servers deployed at the Commission and located within the enterprise network. The assessment consisted of reviewing a judgmental sample of [REDACTED]

³⁸ The data was collected by OIT and saved on to the hard drive. OIT certified that the data was not modified or manipulated.

██████████ located within the network, including regional offices. Further, the assessment reviewed logs on all servers ██████████ for segregation of duties among OIT staff accessing SEC enterprise network logs, access controls to those logs, controls over log management and analysis, log data collection, and log storage. Also, the assessment included a comparison and analysis of audit log records to identify changes in controls and logging requirements and to determine whether the servers were performing audit logging functions; determine whether critical auditable security event types were being logged, including privilege escalation attempts, password guessing attempts, user session activity, changes to user permissions and user accounts, log-in/out, modifications to information systems or application software, and system startup/shutdown; and comparing the actual logs with ██████████ audit logging settings for consistency.

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

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 as noted in the discussion of scope. C5i relied on information requested and supplied by OIT and interviews with OIT personnel to understand OIT's management controls pertaining to policies, roles and responsibilities, and procedures.

User of Computer-Processed Data. C5i reviewed the following computer-processed data (i.e., system logs and network logs) that OIT staff members provided to us:

- system and network Logs,
- event log automation script procedure,
- screenshots of ██████████ security log settings,
- log migration scripts, and
- list of ██████████ settings.

C5i believes that the information that was retrieved from the SEC's systems, as well as the requested network logs and documents provided to us, was sufficient, reliable, and adequate to use in meeting our stated objectives.

C5i assessed the reliability of OIT's computer configuration settings as it pertained to our review of log generation, log capture, log management and storage.

Prior OIG Coverage.

- OIG Report No. 501, *2011 Annual FISMA Executive Summary Report*, February 2, 2012, contained 13 recommendations to strengthen the SEC's controls over information security. All of the report's recommendations are open.
- OIG Report No. 489, *2010 Annual FISMA Executive Summary Report*, March 3, 2011, contained eight recommendations to strengthen the Commission's security posture. All of the report's recommendations are closed, with the exception of recommendation 5, which pertains to the logical access integration of the HSPD-12 card.
- OIG Report No. 476, *Evaluation of the SEC Encryption Program*, March 26, 2010, contained three recommendations to strengthen IT management controls for safeguarding the Commission's information. All of the report's recommendations are closed.
- OIG Report No. 497, *Assessment of SEC's Continuous Monitoring Program*, August 11, 2011, contained 13 recommendations to strengthen the Commission's security posture. All of the report's recommendations remain open.

Judgmental Sampling. C5i obtained from OIT a detailed list of [REDACTED] representing the various types of servers deployed at the Commission and located within the enterprise network. From the list of [REDACTED], C5i identified a judgmental sample of [REDACTED] servers consisting of [REDACTED] located within the SEC's enterprise network, including regional offices. C5i further targeted a population of [REDACTED] servers, of which [REDACTED] were accessible [REDACTED] percent of the total sampled servers). The servers were reviewed onsite at the SEC Operations Center in [REDACTED], on June 18, 2011 and June 24, 2011.

Criteria

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

NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Revision 1, February 2010. Provides guidance for applying the Risk Management Framework to federal information systems.

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

NIST SP 800-92, *Guide to Computer Security Log Management*, September 2006. Provides guidance on the generation, review, and retention of computer logs and log data.

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.

Screenshots

Figure 1. [REDACTED]



Source: OIG-generated

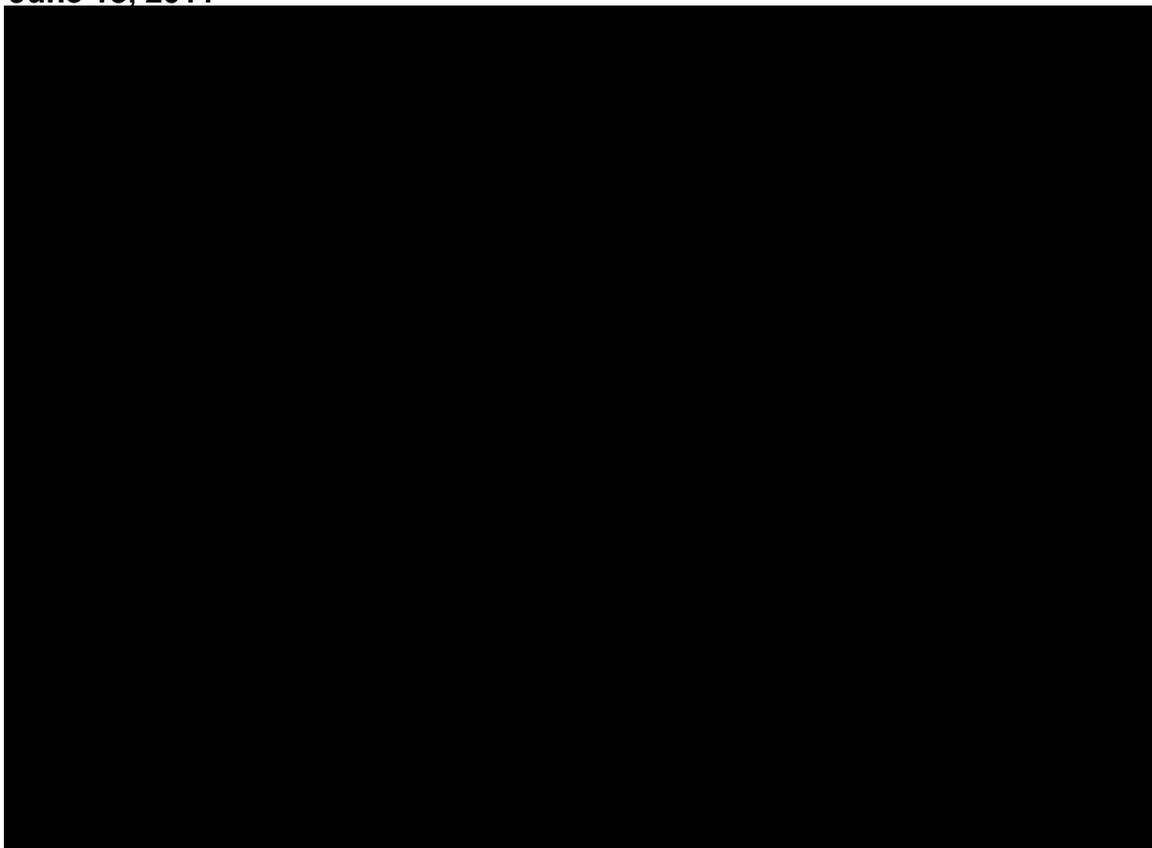
Figure 2. [REDACTED]



Source: OIG-generated

Figure 3. [REDACTED]
June 18, 2011

Verified

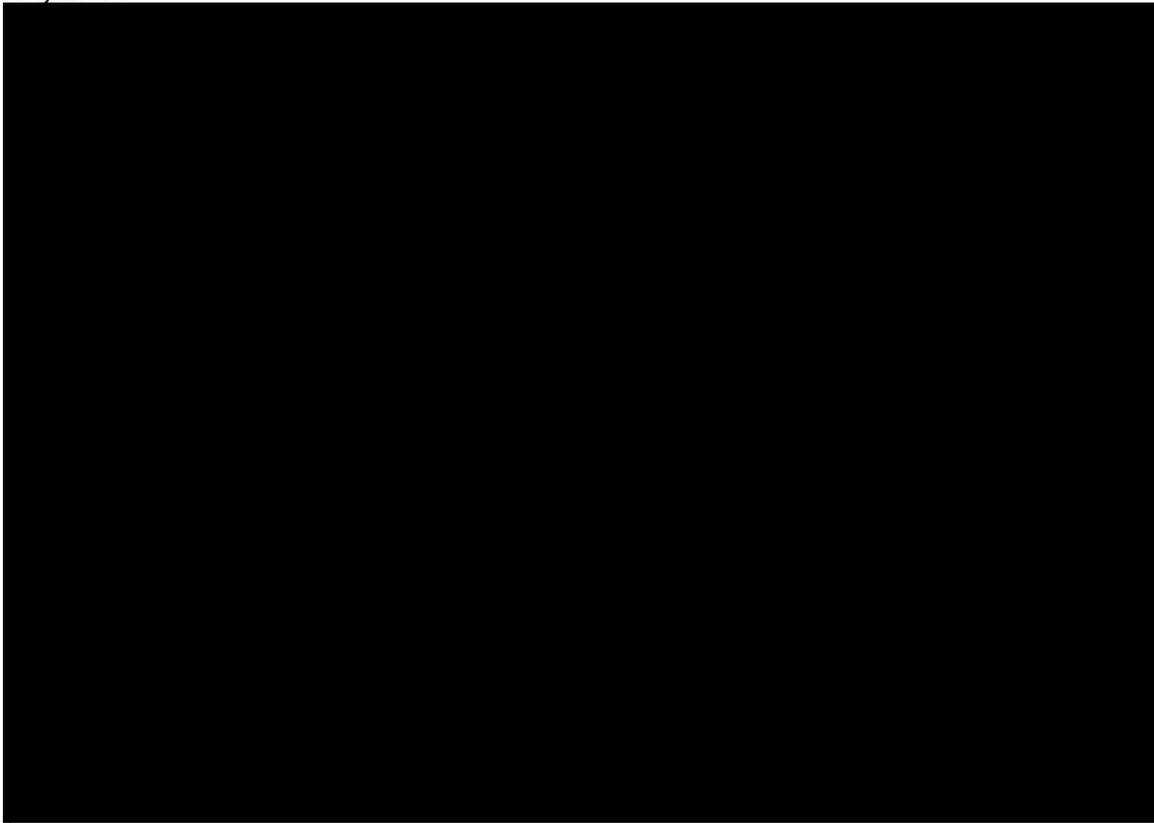


Source: OIG-generated

Figure 4.
18, 2011



Verified June



Source: OIG-generated

Figure 5. [REDACTED]
Verified June 18, 2011



Source: OIG-generated

Figure 6. [REDACTED],
Verified June 18, 2011



Source: OIG-generated

List of Recommendations

Recommendation 1:

The Office of Information Technology should identify capacity requirements for all servers, ensure sufficient capacity is available for the storage of audit records, configure auditing to reduce the likelihood that capacity will be exceeded, and implement an alerting mechanism to alert and notify appropriate Commission office/divisions when log storage capacity is reached.

Recommendation 2:

When updating its policies and procedures, the Office of Information Technology (OIT) should include log management language that

- identifies the roles and responsibilities of staff who are involved in log management,
- requires server logs to be periodically reviewed to check whether log capacity has been exceeded, and
- requires appropriate OIT officials be notified when audit logging functions are suspended when log storage capacity has reached its limit.

Recommendation 3:

The Office of Information Technology should review and update all logging policies and procedures consistent with the policy's review interval requirements and retain evidence of its reviews and any updates to the policy.

Recommendation 4:

The Office of Information Technology should ensure that all servers connected to the Commission's enterprise network are configured to have logging enabled.

Recommendation 5:

The Office of Information Technology (OIT) should update its Server Decommission Guidelines and include language to fully document each action that should be performed when decommissioning a server. OIT should also develop a server decommissioning checklist to be included in the Server Decommission Guidelines.

Recommendation 6:

The Office of Information Technology (OIT) should conduct a review of application database log management and generation procedures to ensure auditable events are being captured and retained, consistent with OIT policies and procedures and National Institute of Standards and Technology guidelines.

Recommendation 7:

The Office of Information Technology (OIT) should implement a mechanism to notify OIT's Servers and Storage Branch, or OIT's Security Branch when [REDACTED] stop performing [REDACTED] functions.

Recommendation 8:

The Office of Information Technology should implement its plan to develop a computer script that determines whether [REDACTED] are producing [REDACTED]

Management's Comments

MEMORANDUM

TO: Jacqueline Wilson, Assistant Inspector General for Audits, Office of Inspector General (OIG)

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

RE: *Assessment of SEC's System and Network Logs*, Report No. 500

DATE: March 15, 2012

This memorandum is in response to the Office of Inspector General's (OIG) Draft Report No. 500 entitled, *Assessment of SEC's System and Network Logs*. Thank you for the opportunity to review and respond to this report.

OIG Recommendation 1:

OIT should identify capacity requirements for all servers, ensure sufficient capacity is available for the storage of audit records, configure auditing to reduce the likelihood that capacity will be exceeded, and implement an alerting mechanism to alert and notify appropriate office/divisions when log storage capacity is reached.

OIT concurs with this recommendation. OIT will use existing system monitoring tools to explicitly alert on log size approaching and/or reaching capacity.

OIG Recommendation 2:

When updating its policies and procedures, the Office of Information Technology (OIT) should include log management language that

- identifies the roles and responsibilities of staff who are involved in log management,
- requires server logs to be periodically reviewed to check whether log capacity has been exceeded, and
- requires appropriate OIT officials be notified when audit logging functions are suspended when log storage capacity has reached its limit.

OIT concurs with this recommendation. OIT will revise their log management policy to take into account the recommended language. OIT is currently reviewing and updating their logging policies and procedures as part of an IT policy review project.

OIG Recommendation 3:

The Office of Information Technology should review and update all logging policies and procedures consistent with the policy's review interval requirements and retain evidence of its reviews and any updates to the policy.

OIT concurs with this recommendation. OIT is currently reviewing and updating their logging policies and procedures as part of an IT policy review project.

OIG Recommendation 4:

The Office of Information Technology should ensure that all servers connected to the Commission's enterprise network are configured to have logging enabled.

OIT concurs with this recommendation. OIT is currently reviewing and updating their logging policies and procedures as part of an IT policy review project. Included in this will be language to define what types of hosts most or should perform logging, as per NIST Special Publication (SP) 800-92, section 4.2.

OIG Recommendation 5:

The Office of Information Technology (OIT) should update its Server Decommission Guidelines and include language to fully document each action that should be performed when decommissioning a server. OIT should also develop a server decommissioning checklist to be included in the Server Decommission Guidelines.

OIT concurs with this recommendation. OIT is currently reviewing and updating their policies, procedures and guidelines as part of an IT policy review project.

OIG Recommendation 6:

The Office of Information Technology (OIT) should conduct a review of application database log management and generation procedures to ensure auditable events are being captured and retained, consistent with OIT policies and procedures and National Institute of Standards and Technology guidelines.

OIT concurs with this recommendation. OIT is currently reviewing and updating their policies, procedures and guidelines as part of an IT policy review project.

OIG Recommendation 7:

The Office of Information Technology (OIT) should implement a mechanism to notify OIT's Servers and Storage Branch, or OIT's Security Branch when [REDACTED] stop performing [REDACTED] functions.

OIT concurs with this recommendation. OIT will leverage existing tools to monitor the status of [REDACTED] processes and alert the appropriate personnel if the process terminates.

OIG Recommendation 8:

The Office of Information Technology should implement its plan to develop a computer script that determines whether [REDACTED] are producing [REDACTED]

OIT concurs with this recommendation. OIT will leverage existing tools to monitor the status of [REDACTED] processes and determine if logging is actively occurring or has ceased.

OIG Response to Management's Comments

We are pleased that OIT concurred with the report's eight recommendations. We are also encouraged that OIT has indicated that they will initiate actions to address the findings described in the report. We believe that OIT's proposed actions are responsive to the report's findings and recommendations and their implementation of the recommendations will further aid in strengthening OIT's controls over the SEC's system and network logs.

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