



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

---

# Review of the SEC's Continuity of Operations Program



April 23, 2012  
Report No. 502

Review Conducted by TWM Associates, Inc.

**REDACTED PUBLIC VERSION**




OFFICE OF  
INSPECTOR GENERAL

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

**MEMORANDUM**

April 23, 2012

**To:** Jeffrey Heslop, Chief Operating Officer, Office of the Chief Operating Officer  
Barry Walters, Director/Chief FOIA Officer, Office of FOIA, Records Management and Security  
Thomas A. Bayer, Director/Chief Information Officer, Office of Information Technology

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

**Subject:** *Review of the SEC's Continuity of Operations Program, Report No. 502*

This memorandum transmits the U.S. Securities and Exchange Commission OIG's final report detailing the results on our review of the agency's Continuity of Operations 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 38 recommendations which if fully implemented should strengthen the SEC's Continuity of Operations Program. We are pleased your offices provided a joint response and concurred with the respective recommendations in our report that were addressed to each office. Your responses to the formal draft report have been 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 report's 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 the Acting Deputy Inspector General, Jacqueline Wilson at 1-6326.

We appreciate the courtesy and cooperation that you and your staff extended to our contractor during this review.

Attachment

cc: James Burns, Deputy Chief of Staff, Office of the Chairman  
Luis A. Aguilar, Commissioner  
Troy A. Paredes, Commissioner  
Elisse Walter, Commissioner  
Daniel Gallagher, Commissioner  
Lacey Dingman, Director, Office of Human Resources

# Review of the SEC's Continuity of Operations Program

---

## Executive Summary

**Background.** The U.S. Securities and Exchange Commission (SEC or Commission) Office of Inspector General (OIG) contracted the professional services of TWM Associates, Inc. (TWM) to conduct a review of the SEC's Continuity of Operations Program (COOP).

A Continuity of Operations Program (COOP), including the Business Continuity Planning (BCP) and Disaster Recovery Plan (DRP), are essential to an organization maintaining its critical operations when unforeseen disruptions or interruptions occur that may affect the organization's normal operations. All federal agencies are required to have viable programs and plans in place to ensure they are able to continue to perform critical functions during an emergency. An agency's COOP plan focuses on restoring the organization's Mission Essential Functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. Additional functions, or those performed at a field office level, may be addressed by the BCP. "Minor threats or disruptions that do not require relocation to an alternate site are typically not addressed in a COOP plan."<sup>1</sup> Standard elements of a COOP plan include: program plans and procedures; continuity communications; risk management; vital records management; budgeting and acquisition of resources; human capital; essential functions; test, training, and exercise; order of succession; devolution; delegation of authority; reconstitution; and continuity facilities. COOP plans are specific types of plans that should not be confused with BCPs, DRPs, or Information System Contingency Plans (ISCP).

The Office of the Chief Operating Officer, Chief Operating Officer (COO) assumed overall responsibility for overseeing the SEC's agency-wide COOP in 2011, when the former Executive Director left the SEC and these duties were transferred to the COO. Specifically, the Office of Freedom of Information Act, Records Management, and Security's (OFRMS), which reports to the COO, Office of Security Services (OSS), has been responsible for developing and managing the SEC's COOP since July 2011.

The SEC's regional offices and Office of Information Technology (OIT) also play supporting roles in the COOP process. Regional office directors are responsible for updating their COOP plan supplements. OIT has various functions

---

<sup>1</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 8, section 2.2.2.

complementary to COOP processes and is responsible for developing and managing the technology processes for the SEC's business continuity management structure. OIT is also responsible for the SEC's DRP and must be able to recover its full main infrastructure in the event of a disaster. Further, the responsibilities associated with the DRP are overseen by the Commission's Chief Information Officer.

The SEC has a COOP and some related COOP policies and procedures and the SEC periodically conducts testing of the COOP plan. In addition, there is an overall OIT contingency plan (e.g., the ISCP for the general support system) and individual Headquarters division and office COOP plan documents. Further, DRPs and business impact analysis (BIA) are prepared for individual systems, and each regional office has a DRP for its office infrastructure that complements the Headquarters' base DRP for regional offices.

Further, the SEC's COOP plan identifies essential personnel, vital records, lines of succession and other required information. The SEC has identified [REDACTED] essential personnel under its COOP plan and it has established relocation sites for [REDACTED]

[REDACTED] The overall Commission COOP plan document was updated April 2008 and April 2010, and the most recent version is a draft dated October 2011. SEC's Headquarters divisions/office's COOP plans and the regional office's COOP supplements have various dates, some of which are outdated.

In addition to its 2010 COOP plan, the SEC has a separate pandemic influenza preparedness plan (pandemic plan), which incorporates the COOP plan. The SEC's pandemic plan focuses on protecting the health of SEC employees, while maintaining agency operations during a pandemic.<sup>2</sup>

**Objectives.** The overall objective of TWM's review was to determine whether the SEC had a viable COOP, BCP, and DRP that sufficiently supported its operations at its Headquarters, Operations Center, and 11 regional offices. Further, the review sought to determine if the Commission is adequately prepared to perform essential functions during business continuity or disaster recovery event resulting from human/natural disasters, national emergency, or technological events which could impact the Commission's ability to continue mission-critical and essential functions. The sub-objectives for the review were to:

---

<sup>2</sup> "A pandemic occurs when a novel strain of influenza virus emerges that has the ability to infect and be passed between humans. Because humans have little immunity to the new virus, a worldwide epidemic, or pandemic can ensue." *National Strategy for Pandemic Influenza Implementation Plan*, May 2006, page 1.

- Evaluate the Commission's pandemic plan to ensure it is formal, documented, well-communicated, has been tested at regular intervals, and meets the objectives of the *National Strategy for Pandemic Influenza: Implementation*;
- Assess the Commission's implementation and testing of its pandemic plan;
- Determine the Commission's plans for protecting its employees and contractors during a pandemic occurrence; and
- Evaluate the Commission's plans for sustaining essential functions during high rates of employee absenteeism.

**Results.** Our review found that while the SEC does have a COOP function and plan (including relocation sites and testing) in place, the program needs to be improved. In particular, the SEC's COOP policies, directives and documents are out-of-date and incomplete, are not comprehensive and are not currently being followed in some respects. However, since assuming agency-wide responsibility for the COOP Program, the COO directed OFRMS/OSS to perform a thorough review of the SEC's entire COOP program. In addition, after the conclusion of our fieldwork for this review we were informed and confirmed that the OSS issued a statement of work to hire a contractor to provide support to the SEC's COOP and to assist in addressing deficiencies OIG identified in this report and OSS's internal COOP assessment.

The SEC's draft COOP plan states that the divisions, offices, and regional offices are required to report any changes to their supplemental plans to the COO. We found, however, that supplemental plans are not being updated and two regional offices did not have supplemental COOP plans. Further, we found that essential personnel information in the COOP supplements has not been properly maintained and were not up-to-date. In addition, while the overall COOP plan referenced key SEC personnel who comprise the vital records information for the regional offices and Headquarters divisions and offices, it was incomplete and outdated.

Our review further identified deficiencies with the DRPs for individual systems, and we found that that the SEC does not prepare BCPs or ISCPs for its information systems. While OIT stated that BCPs and ISCPs are unnecessary because the components of these documents are included in the DRPs and BIAs for these systems, we found that some BCP elements were missing.

Additionally, our review identified instances in which information feeds and power distribution throughout the SEC's network could fail if a disruption were to occur. Specifically, we found that the information data feeds for the SEC's [REDACTED] [REDACTED] are currently available only through connections to the SEC network and that the data would, therefore, be unavailable if the [REDACTED] were incapacitated. We also identified power issues at the [REDACTED]

[REDACTED]

We also uncovered inconsistencies between the categorization of the systems that were reported to Office of Management and Budget under Federal Information Security Management Act (FISMA), and the recovery time objectives established for SEC COOP systems. For FISMA reportable systems with a moderate to low rated availability, the SEC COOP established recovery time objectives may be overly aggressive and could result in unnecessary expense in documentation, testing, and infrastructure.

In addition, we found SEC systems with a recovery time objective of [REDACTED] which was inconsistent with the COOP documentation for these systems and the FISMA availability categorization of the systems.

Further we found that improvements were needed in the processes for recovering data from [REDACTED] and related testing. Specifically, [REDACTED]

[REDACTED] In addition, the current [REDACTED] and data restoration processes are insufficient. The SEC [REDACTED]

Based upon a review of COOP documents including those found [REDACTED] [REDACTED] we identified essential personnel who no longer worked at the SEC, some essential personnel have not been issued remote access devices and/or tested the devices they were issued.<sup>3</sup> Further, some essential personnel that were issued [REDACTED] never logged in or have not logged in remotely within the past year and, therefore, have not effectively tested their ability to log in during an unscheduled event using this remote access method.

We also found that remote access capabilities would be enhanced if remote access to desktop applications could function even if the user's desktop computer was turned off or did not have power. The SEC has a pandemic plan and its remote access capabilities infrastructure appear to be adequate for this purpose.

---

<sup>3</sup> [REDACTED] matters and is designed to provide SEC divisions/offices with the capability to customize their COOP information across a variety of categories. The [REDACTED] Word files, Excel spreadsheets and pdf files that may be accessed and updated by individuals who have access to the site.

The DRPs for several regional offices have not been tested annually, and two regional offices did not include recovery phase testing in their latest disaster recovery test plans. Also seven regional offices did not include reconstitution phase testing in their most recent disaster recovery test plans. Further, we found that the regional offices did not test any element (e.g., a file or data record) from the system's [REDACTED] for systems that had overall moderate rating under FISMA.

SEC division/office heads select essential personnel based on certain written factors and designated [REDACTED] individuals as essential. Though the SEC indicated in its OIT contingency plan that COOP and disaster recovery testing exercise participation satisfies the requirement to ensure a trained workforce is available to support the SEC's mission critical functions during and following a disaster, our review revealed that only [REDACTED] (3.1 percent) of persons identified as essential personnel under the COOP actually attended the exercise. Further, our review found the SEC did not have a sufficient level of participation by regional office essential personnel in its disaster recovery testing to ensure they were adequately trained.

We were informed that equipment at the SEC's devolution sites were out-of-date and could not be used with SEC's network, due to unresolved security issues. Further, the SEC's COOP plan indicates there are [REDACTED] workstations/work areas available at the SEC's Operations Center location, where emergency response personnel are to relocate in the event of an emergency. However, our review found a total of [REDACTED] vacant seats (not vacant offices) in the entire building. Therefore, COOP plan documentation on space availability needs to be revised to reflect current space availability and needs, taking into account the potential for telework and remote access.

The SEC performs DRP testing for each regional office infrastructure and individual system applications. All of the regional office's DRPs state that POA&Ms will be created. Our review found 39.5 percent of the recommendations generated during the regional office DRP testing could not be tracked to any POA&M and was not identified as having been resolved in the updated DRPs (dates ranging from 2010 to 2011). Further, we found that at least two items identified in the annual Headquarters COOP testing that should have been included as POA&M items (submission of filings gap during testing of Testimony Tracking System, and order of startup for production servers on Business Objective 11 system). We also found that eight regional offices have not updated their DRPs to include recommendations that were identified in DRP testing.

The SEC has chosen to eliminate the BCP, indicating that the elements in the BCP are already contained in the DRP and BIAs. As a consequence, the SEC's DRP exercises are primarily viewed as information technology exercises. As



training and exercises cover the same topics, the SEC uses exercises to satisfy its training requirement in an effort to reduce the number of hours that are devoted to these activities. We also found that the SEC used the participation in regional office DRP exercises to satisfy its requirement to train essential personnel both for the COOP plan and DRP. Our testing revealed that between 2008 and 2011, an average of 88 percent of regional office identified essential personnel did not participate in DRP training or exercises. This indicates that the regional offices essential personnel may not have been sufficiently trained in their roles and responsibilities during a disaster recovery event. As a consequence, essential personnel may not be able to perform their responsibilities during the activation of a DRP.

Finally, we found that while OIT personnel regularly participate in DRP exercises, many key essential personnel do not participate in these exercises and have not received the appropriate role-based training for their part in DRP and COOP activities. Instead, in the past these personnel have only received the annual refresher, online training course.

**Recommendations.** Based on the results of our review we made the following recommendations:

- (1) The Office of the Chief Operating Officer should ensure that the OFRMS completes its review of the agency-wide COOP to ensure the Commission's COOP is comprehensive, cohesive, and in compliance with federal guidance.
- (2) OFRMS should revise and update the Commission's continuity of operations program policies and procedures to ensure they are comprehensive, complete, and up-to-date.
- (3) OFRMS and OIT, in conjunction with the program divisions/offices and regional offices, should update, revise and finalize all COOP documents, including the overall Headquarters COOP plan, individual division/office COOP plans, regional office COOP supplements, disaster recovery plans, business continuity plans and business impact analyses, and pandemic plans supplements. OFRMS and OIT should ensure these documents are complete and include all the necessary elements, and that they properly define the Commission's essential functions. In addition, processes should be implemented to ensure annual review and approval of these documents.
- (4) OFRMS, in conjunction with program and regional offices, should ensure that vital records and lines of succession are properly

identified, documented and readily available during continuity events.

- (5) OIT, in conjunction with the primary program information users, should identify [REDACTED] at the alternate locations should [REDACTED] be unavailable. Further, OIT should review the SEC's network and topology to ensure there are [REDACTED]
- (6) OIT should ensure proper power distribution throughout the network [REDACTED]
- (7) OFRMS, in conjunction with the OIT and system owners, should revise the SEC system recovery time objectives to specify more realistic timeframes, based on the ability to transition to the alternate site, and then determine acceptable recovery times. The recovery plan and priority of recovery of the systems should be based on the overall mission of the agency with a focus on real-time monitoring of the markets. Further, the identification of high priority systems should focus on the immediate mission of the agency, and systems documentation should also be reviewed to ensure proper recovery priority is reflected based on the contribution to the SEC's mission and functions.
- (8) For underutilized systems such as the [REDACTED] the Office of Information Technology should consider discontinuing maintenance, retiring the system, or alternatively making more robust use of the system such that additional Commission funds are not wasted on underutilized systems.
- (9) OIT, in conjunction with system owners, should identify the [REDACTED] requirements (e.g., files, data, and system software) for all systems (at minimum, Federal Information Security Management Act reportable systems). OIT should ensure that [REDACTED] requirements are documented, understood by the owner, and published for future reference. Further, OIT should ensure system software licenses and key requirements are included in [REDACTED] documentation, and the location of this information is known to ensure restoration capability at the alternate location site.

- (10) OIT, in conjunction with the regional offices, should document the processes and procedures to be used in the event that a regional office needs to restore its systems at a regional office transition site, and the corresponding effect on the [REDACTED] procedures for other regional offices that may need to use a regional office transition site or alternate method to ensure recoverability.
- (11) OIT should continue its efforts to replace the regional office's tape [REDACTED] systems. Additionally, OIT should define a [REDACTED] and recovery strategy for multi-hosted application restoration for the regional offices. OIT should also document the system specific files and database items, in order to facilitate the ability to restore only necessary items, rather than the entire database, which could take many hours to accomplish and is not in line with the recovery time objectives for individual systems.
- (12) OIT should implement consistent and appropriate [REDACTED] schedules for mission essential and Federal Information System Management Act reportable systems, including daily, weekly, and monthly [REDACTED] processes and procedures, to ensure these systems are recoverable.
- (13) OIT should include in the Disaster Recovery Plan and Business Continuity Plan, testing steps that are designed to ensure the restoration from [REDACTED] that is consistent with the requirements for systems that are rated as moderate, in accordance with the National Institute of Standards and Technology guidance under the Federal Information Systems Management Act.
- (14) OIT should ensure that remote access testing is included as part of all Continuity of Operations Program, disaster recovery and pandemic testing activities, including those performed in the regional offices, to ensure that essential personnel and a sample of the representative users of the system are able to function remotely during an unscheduled event.
- (15) OIT, in consultation with the OFRMS, should require semi-annual testing of remote access devices to ensure up-to-date connectivity and ability for both essential personnel and non-essential personnel to access the Commission's network. In addition, OIT and OFRMS should implement a system notification warning prior to the connectivity testing date and then disable those devices that are not updated.

- (16) OFRMS and OIT should consider implementation of alternate remote access solutions and/or internal directory structure [REDACTED] and Federal Information Security Management Act reportable systems.
- (17) OFRMS and OIT should update the COOP documents and necessary agreements to appropriately reflect authorized telework activities by Commission personnel during unscheduled events under the COOP, disaster recovery and pandemic plans, including equipment that will be used for teleworking in such circumstances.
- (18) OFRMS and OIT should ensure that the agency's disaster recovery testing includes the Commissions mission essential and Federal Information Security Management Act reportable systems and pandemic plan testing is conducted on a regular basis.
- (19) OIT should determine aspects of continuity of operations disaster recovery and business continuity plan testing that should be conducted annually for regional offices and for Federal Information Security Management Act reportable systems based upon their security categorization. OIT should ensure that this testing includes the recovery phase and the reconstitution phase, as well as a restoration from [REDACTED]
- (20) OIT should add elements to contracts and service level agreements for externally hosted systems to provide appropriate methods by which the SEC can obtain assurance that appropriate disaster recovery plan testing is performed on mission essential and Federal Information Security Management Act reportable systems and to ensure the systems are able to function during unscheduled events. Such measures may include SEC participation in the disaster recovery plan testing for the externally hosted systems and/or a review of the results of such testing.
- (21) OIT should include elements of testing from an alternate site in the regional office continuity of operations program, disaster recovery, and business continuity plan testing on a periodic basis to ensure the necessary capability and functionality for regional office activities are in place.

- (22) OFRMS and OIT should include designated essential personnel for systems, divisions/offices, and regional offices in COOP and disaster recovery testing to ensure that a trained workforce is available to support the SEC's mission critical functions following a disaster.
- (23) OIT should ensure that system specific scripts and test scenarios are included in the disaster recovery and business continuity plan testing activities to provide assurance of system functionality at alternate locations.
- (24) OFRMS and OIT should reassess the definition of essential personnel to ensure that this designation includes only personnel whose services are needed during an event to establish mission essential system connectivity and conduct essential activities until normal operations are resumed. OFRMS and OIT should also develop policies and procedures to ensure that elevated communication cards are distributed only to necessary personnel, cards are disabled upon an employee's departure from the agency, and all essential personnel have appropriate elevated communication cards.
- (25) OFRMS, in conjunction with the regional offices, should specify alternate work locations for which the necessary logistics, such as memoranda of agreement, service level agreements, or credit card limits for hotel conference rooms or other locations, are arranged in advance.
- (26) OFRMS should categorize essential personnel according to necessary functions, based on various realistic scenarios (such as Headquarters or Operations Center locations becoming inaccessible or not operational, including traffic conditions that would affect the scenario). Possible categories include personnel required for immediate activities, personnel needed to establish connections at the alternate site, and personnel needed to work remotely at designated alternate sites such as their homes, hotels, or other specified locations.
- (27) OFRMS, as part of its planning efforts, should specify when Commission personnel are to telework after an event and when they must go to the designated alternate locations instead of teleworking.
- (28) OFRMS and OIT should define migration paths from [REDACTED] [REDACTED] should it become inaccessible and specify where the alternate worksite locations for [REDACTED]

- (29) OFRMS and OIT should ensure that the designated Headquarters alternate worksites are ready for use and contain sufficient equipment and technology resources. In addition, COOP plan documentation should be revised to reflect current space availability and needs, taking into account the potential for telework and remote access.
- (30) OFRMS and OIT should ensure that designated alternate worksite locations are visited and tested periodically to ensure ready access and use. Appropriate steps should be taken to ensure that any cards or badges required for entry to alternate worksite locations are kept up to date and have not expired.
- (31) OIT should reinforce the need for SEC personnel and contractors to register in the agency's emergency notification system, which is designated as the primary method of notifying employees during a continuity of operations or pandemic event. OIT should also implement procedures to ensure the removal of personnel from the emergency notification system after they leave the SEC.
- (32) OFRMS and OIT should clearly define in the continuity of operations, disaster recovery, and business continuity plan documentation the alternate worksite or telework locations for both essential and non-essential personnel. This documentation should also clarify whether; when relocating to an alternate site is required, family members may accompany Commission employees and contractors to the relocation site, consistent with federal regulations.
- (33) OFRMS and OIT should ensure that recommendations made as a result of the continuity of operations, disaster recovery, business continuity and pandemic testing are included in a management corrective action plan (CAP) and is maintained in the CAP until it is resolved.
- (34) OIT should ensure that open POA&M items from previous years are evaluated by management and final corrective actions are implemented to close the items.
- (35) OFRMS and OIT should ensure that continuity of operations, disaster recovery, and business continuity plan training occur prior to annual tests exercises or events as recommended by NIST Special Publication 800-84, Guide to Test, Training, and Exercise Programs for Information Technology Plans and Capabilities, in order to ensure that individuals are prepared for their specific roles during a disaster recovery event.

- (36) OFRMS, in conjunction with the OHR, OIT, and the various divisions and offices, should consider, consistent with federal personnel regulations, if there is the ability to cross-train regional office personnel in functions that are performed exclusively at the Commission Headquarters and regional offices and, if so, should define these functions and implement procedures for cross-training personnel for mission essential functions in the case of a COOP or pandemic event.
- (37) OFRMS and OIT, in conjunction with the OAS and OGC, should document that the necessary contractual agreements and/or provisions are in place to ensure the availability of hardware, software, and services that may be required during an emergency. The use of government credit cards to procure such equipment and services should also be considered and documented. If government credit cards are to be used for this purpose, the authorized limits established should be sufficient for such purchases.
- (38) OFRMS and OIT, in conjunction with the regional offices, OAS, OFM, and OGC, should ensure that an appropriate and updated Memoranda of Agreement, Memoranda of Understanding and Service-Level Agreements are executed to provide for alternate work site locations, capabilities, and accommodations that may be necessary to ensure continuity of operations.

OFRMS and OIT fully concurred with all the recommendations in this report that were addressed to their respective offices.

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

# TABLE OF CONTENTS

Executive Summary .....	iii
Table of Contents .....	xv
<b>Background and Objectives</b> .....	1
Background .....	1
Objectives .....	10
<b>Findings and Recommendations</b> .....	11
Finding 1: SEC’s COOP Policies, Procedures and Documents Require Updating, More Cohesiveness, and Inclusion of Missing Elements .....	11
Recommendation 1 .....	18
Recommendation 2 .....	18
Recommendation 3 .....	19
Recommendation 4 .....	19
Finding 2: Network Weaknesses Could Affect the SEC’s Continuity of Operations and Disaster Recovery Plans .....	20
Recommendation 5 .....	21
Recommendation 6 .....	21
Finding 3: The COOP Systems’ Availability Categorization and Utilization Should be Reviewed .....	22
Recommendation 7 .....	24
Recommendation 8 .....	24
Finding 4: Improvements Are Needed in Recovery from [REDACTED] and Related Testing .....	25
Recommendation 9 .....	28
Recommendation 10 .....	29
Recommendation 11 .....	29
Recommendation 12 .....	29
Recommendation 13 .....	30
Finding 5: Remote Access/Telework Testing Was Not Included in the SEC’s DRP and Pandemic Plan Testing .....	30
Recommendation 14 .....	33
Recommendation 15 .....	34
Recommendation 16 .....	34
Recommendation 17 .....	34



Finding 6: COOP and Disaster Recovery Testing Activities Can Be Improved .....	35
Recommendation 18.....	39
Recommendation 19.....	40
Recommendation 20.....	40
Recommendation 21.....	40
Recommendation 22.....	41
Recommendation 23.....	41
Recommendation 24.....	41
 Finding 7: Alternate Work Locations Need to Be Realistic, Maintained in a Ready State, and Communicated to Staff .....	42
Recommendation 25.....	45
Recommendation 26.....	46
Recommendation 27.....	46
Recommendation 28.....	46
Recommendation 29.....	47
Recommendation 30.....	47
Recommendation 31.....	47
Recommendation 32.....	48
 Finding 8: Plans of Action and Milestones (POA&M) Need to Be Complete and Up-to-Date .....	48
Recommendation 33.....	49
Recommendation 34.....	50
 Finding 9: Additional Training and Cross-Training of COOP Personnel is Required.....	50
Recommendation 35.....	52
Recommendation 36.....	53
 Finding 10: Necessary Memoranda of Agreement, Memoranda of Understanding, and Service-Level Agreements Were Not Present or Are Outdated .....	53
Recommendation 37.....	55
Recommendation 38.....	56

## Appendices

Appendix I: Abbreviations.....	57
Appendix II: List of Issues Identified in Review of Disaster Recovery and Continuity of Operations Plans.....	58
Appendix III: List of Issues Identified from Sample Testing of System Disaster Recovery Plan and Business Impact Analysis Documents .....	61
Appendix IV: Scope and Methodology .....	64
Appendix V: Criteria .....	66
Appendix VI: List of Recommendations .....	68
Appendix VII: Management Comments.....	77
Appendix VIII: OIG Response to Management’s Comments.....	86

# Background and Objectives

---

## Background

Based on the Office of Inspector General's (OIG) annual audit plan, the OIG contracted the professional services of TWM Associates, Inc. (TWM) to conduct a review of the SEC's Continuity of Operations Program (COOP).

All federal agencies are required to have viable programs and plans in place to ensure they are able to continue to perform critical functions during an emergency. Specifically, Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements, "provides direction to the Federal executive branch for developing continuity plans and programs" and provides that "[c]ontinuity requirements must be incorporated into the daily operations of all agencies to ensure seamless and immediate continuation of Primary Mission Essential Function (PMEF) capabilities so that critical government functions and services remain available to the Nation's citizens."<sup>4</sup>

FCD 1 states, "In support of this policy, the Federal executive branch has developed and implemented a continuity program which is composed of efforts within individual agencies to ensure that their Mission Essential Functions (MEF) continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies."<sup>5</sup> FCD 1 also states, "All agencies, regardless of their size or location, shall have in place a viable continuity capability to ensure continued performance of their agency's essential functions under all conditions."<sup>6</sup> Federal Continuity Directive 2 (FCD 2), Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process, provides guidance and direction to federal agencies in identifying their MEFs and potential PMEFS, and provides that "[a]n agency should carefully review all of its missions and functions before determining those that are essential."<sup>7</sup>

## Federal Requirements for COOP Plans and Related Documents

An agency's COOP plan focuses on restoring the organization's MEFs at an alternate site and performing those functions for up to 30 days before returning to normal operations. Additional functions, or those performed at a field office level,

---

<sup>4</sup> *Federal Continuity Directive 1 (FCD 1)*, February 2008, pages 1-2.

<sup>5</sup> *Federal Continuity Directive 1 (FCD 1)*, February 2008, page 2.

<sup>6</sup> *Federal Continuity Directive 1 (FCD 1)*, February 2008, page 2.

<sup>7</sup> *Federal Continuity Directive 2 (FCD 2)*, February 2008, page A-1.

may be addressed by a business continuity plan (BCP).<sup>8</sup> “Minor threats or disruptions that do not require relocation to an alternate site are typically not addressed in a COOP plan.”<sup>9</sup> Standard elements of a COOP plan include: program plans and procedures; continuity communications; risk management; vital records management; budgeting and acquisition of resources; human capital; essential functions; test, training, and exercise; order of succession; devolution; delegation of authority; reconstitution; and continuity facilities. COOP plans are specific types of plans that should not be confused with BCPs, Disaster Recovery Plans (DRP), or Information System Contingency Plans (ISCP).<sup>10</sup>

A BCP focuses on sustaining an organization’s mission or business processes (e.g., payroll) during and after a disruption, and may be written for mission or business processes within a single unit or may address the entire organization’s processes. A BCP may be scoped to address only priority functions, and it may be used for long-term recovery in conjunction with an organization’s COOP plan.<sup>11</sup>

A DRP applies to major (usually physical) “disruptions to service that deny access to the primary facility infrastructure for an extended period,” and is an information system-focused plan designed to restore operability at an alternate site after an emergency.<sup>12</sup> A DRP may be supported by multiple ISCPs and may support a BCP or COOP plan by recovering supporting systems for mission or business processes or MEFs at an alternate location. DRPs only address information system disruptions that require relocation.<sup>13</sup>

An ISCP provides procedures for system assessment and recovery following a system disruption and provides key information needed for system recovery. An ISCP differs from a DRP primarily in that ISCP procedures are developed for recovery of a system regardless of its site or location. Once a DRP has successfully transferred a system to an alternate site, “each affected system would then use its respective ISCP to restore, recover, and test systems, and put them into operation.”<sup>14</sup> While COOP plans address national, primary or mission

---

<sup>8</sup> National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 8, section 2.2.2.

<sup>9</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 8, section 2.2.2.

<sup>10</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 8, section 2.2.2.

<sup>11</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 8, section 2.2.1.

<sup>12</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 10, section 2.2.6.

<sup>13</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 10, section 2.2.6.

<sup>14</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 10, section 2.2.7.

essential functions, ISCPs address federal information systems and are mandated by the Federal Information Security Management Act (FISMA).<sup>15</sup> A business impact analysis (BIA) is a key step in the contingency planning process and is intended to correlate the system with the critical mission or business process and services provided and, based on that information, characterize the consequences of a disruption.<sup>16</sup> The three steps typically involved in the BIA process are: (1) determining mission or business processes and recovery criticality; (2) identifying resource requirements; and (3) identifying recovery priorities for system resources.<sup>17</sup>

## SEC COOP Oversight and Responsibilities

The SEC has a COOP and certain related policies and procedures. The Office of the Chief Operating Officer, Chief Operating Officer (COO) currently has responsibility for overseeing the SEC's agency-wide COOP. The COOP was previously overseen by the Office of the Executive Director's former Executive Director. However, effective July 25, 2011, primary responsibility for COOP was transferred to the Office of Freedom of Information Act, Records Management, and Security's (OFRMS), Office of Security Services (OSS), and the OFRMS director reports to the COO.<sup>18</sup> OSS develops and manages the central agency-wide COOP plan which "describes what procedures are taken to sustain SEC's critical mission functions for a period of 30 days in the event of a large scale disaster and disruption."<sup>19</sup>

The COO directed OFRMS/OSS to perform a thorough review of the entire COOP to ensure that it complies with Federal Emergency Management Agency guidance. Subsequent to the exit conference for this review, OSS management informed us that OSS had initiated a self-review of the COOP program in October 2011 and provided us with a brief outline of its review of the SEC's [REDACTED] is an internal [REDACTED] system that is dedicated to continuity assurance and emergency preparedness. The site contains links to authoritative guidance for continuity and emergency matters and is designed to provide SEC divisions/offices with the capability to customize their

---

<sup>15</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 9, section 2.2.7. FISMA, which was enacted as Title III of the E-Government Act of 2002, provides the framework for securing the federal government's information technology and requires agency program officials, chief information officers, privacy officers, and inspector general to conduct annual reviews of the agency's information security and privacy programs and report the results to the Office of Management and Budget (OMB).

<sup>16</sup> NIST SP 800-34 Rev 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 15, section 3.2.

<sup>17</sup> NIST SP 800-34 Rev 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, pages 15-16, section 3.2.

<sup>18</sup> The Chief Operating Officer was appointed Acting Executive Director on May 3, 2011, and the Commission approved rule amendments reflecting the consolidation of the Office of the Chief Operating Officer (OCOO) and Office of the Executive Director in September 2011.

<sup>19</sup> Operating Directive *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, page 4, section 5d.

COOP information across a variety of categories. The site further includes Word files, Excel spreadsheets and pdf files that may be accessed and updated by individuals who have access to the site. We obtained a spreadsheet from the [REDACTED] site that identified SEC personnel who were designated as essential. Subsequent to the end of fieldwork, OFRMS provided OIG with a statement of work seeking a range of tasks to support the SEC's COOP, including assistance in resolving the deficiencies OIG identified in this report, and OSS's internal COOP assessment from potential contract vendors.

In addition to the primary COOP role OSS has, the regional offices and the Office of Information Technology (OIT) play supporting roles in the COOP process. According to the SEC's COOP plan, the regional office directors are responsible for updating the regional office's COOP plan supplements. OIT has various functions complementary to the SEC's COOP processes and is primarily responsible for developing and managing the technology processes for the SEC's business continuity management (BCM) structure.<sup>20</sup> OIT is also responsible for the DRP and must be in a "position to recover its full main infrastructure in the event of a total or partial disaster."<sup>21</sup>

## Description of the SEC's COOP Plan and Related Documents

The SEC's COOP plan consists of an overall high-level Commission COOP plan document. There is also a regional office base COOP plan document and separate individual regional office COOP plan supplements. In addition, there is an overall OIT contingency plan (i.e., the ISCP for the general support system) and individual Headquarters divisions/offices COOP plan documents. Further, DRPs and BIAs are prepared for individual systems, and each regional office has a DRP for its office infrastructure, complementing the base DRP for regional offices.

The SEC's COOP plan identifies essential personnel, vital records, lines of succession and other required information. The SEC identified [REDACTED] essential personnel under its COOP plan and established relocation sites for SEC [REDACTED]

[REDACTED] The overall Commission COOP plan document was updated in April 2008 and April 2010, and the most recent version of the document on the [REDACTED] is a draft document that is dated October 2011. The regional office COOP supplements and individual Headquarters division and office COOP plans have various dates and have not been recently updated.

<sup>20</sup> Operating Directive, *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, page 4, section 5f.

<sup>21</sup> Disaster Recovery Planning Policy, OIT-00003-001.0, August 6, 2002.

In addition to its COOP plan, the SEC has a separate pandemic influenza preparedness plan (pandemic plan), which incorporates by reference the SEC's COOP plan as it may be amended from time to time. The SEC's pandemic plan focuses on protecting the health of SEC employees, while maintaining agency operations during a pandemic.<sup>22</sup>

## Overview of the SEC's Network and Locations

The SEC is an independent regulatory agency and has the statutory responsibility to oversee and regulate the nation's securities markets and participants. The SEC employees and contractors rely extensively on the SEC's network to perform their duties. SEC's network infrastructure includes a general support system for its [REDACTED] (to serve as the [REDACTED] and its 11 regional offices that are located throughout the country.

The SEC network is an integrated client/server system that is comprised of local area networks, a metropolitan area network, and a wide area network. The wide area network provides connectivity to SEC sites throughout the continental United States. OIT owns and operates the SEC's various network subsystems, which are located at various facilities that the SEC leases. The SEC's network provides services to both internal and external customers (e.g., electronic filers), who use the network for their business applications. The SEC's network provides the necessary security services to support these applications.

The SEC's wide area network is a dynamic virtual private network that connects the regional offices with the [REDACTED] and Alternate Data Center. The virtual private network environment uses dynamic technology, which allows the regional offices to connect directly with each other. This solution alleviates the need for all traffic between sites to pass through the Alternate Data Center or [REDACTED] before arriving at the destination site. The metropolitan area network connects the [REDACTED] Alternate Data Center, and Headquarters locations, and contains redundant aspects (i.e., the ability to use multiple paths) to prevent failure in any single location.

The network infrastructure provides the computer environment for all the applications that are used to support the SEC's business functions and mission. Some of these applications are designated as major applications in the SEC's reports to the Office of Management and Budget (OMB) under FISMA. In its

---

<sup>22</sup> "A pandemic occurs when a novel strain of influenza virus emerges that has the ability to infect and be passed between humans. Because humans have little immunity to the new virus, a worldwide epidemic, or pandemic can ensue." *National Strategy for Pandemic Influenza Implementation Plan*, May 2006, page 1.

<sup>23</sup> The SEC's regional offices are located in Atlanta, Boston, Chicago, Denver, Los Angeles, Miami, New York, Philadelphia, Salt Lake, and San Francisco.

Fiscal Year 2011 FISMA report to OMB, the SEC listed a total of [REDACTED] [REDACTED]<sup>24</sup> [REDACTED] at outside entities (both federal and private). The SEC's internally hosted systems are [REDACTED] and the majority of the systems have a [REDACTED] at the [REDACTED]. Additionally, [REDACTED] are run daily, weekly and monthly, based upon schedules for incremental data, full data, and full system [REDACTED].

While the SEC's regional offices have systems that are supported by its network, each regional office has a [REDACTED]. The regional offices still use [REDACTED] as the primary means of recovering critical regional office servers and data. The regional offices' data is also replicated in real time to servers located at designated [REDACTED]. The replication [REDACTED] act as a secondary means of restoring the regional offices' data and are generally used only following a catastrophic event that severely damages or destroys a regional office's network.

## SEC Policies and Procedures Relating to COOP

The SEC's policies and procedures relating to the COOP are currently all OIT policy documents such as: Operating Directive 24-0.09 (02.0), Information Technology (IT) Security Business Continuity Management Program, dated August 23, 2011; Implementing Instruction 24-04.09.01 (02.0), Business Impact Analysis, dated August 22, 2011; Disaster Recovery Planning Policy, OIT-00003-001.0, dated August 6, 2002, and Disaster Recovery Planning Procedures, OIT-00047-001.0, dated February 4, 2003.

According to Operating Directive 24-04.09, "[b]ased on federal requirements, the SEC has developed an agency-wide program that has policies, processes, and procedures to address the information and information system security requirements needed for business continuity in the event of a disruption."<sup>26</sup> The Operating Directive states that the SEC has created a BCM framework of plans to centralize plan development and ensure that all plans are consistent and standardized, address applicable information technology security requirements,

---

<sup>24</sup> SEC FISMA submission to OMB, October 14, 2011. OMB Memorandum for Heads of Executive Departments and Agencies on *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, M-11-33, September 14, 2011, provides that all of an agency's information systems should be included as part of the agency's FISMA report. M-11-33, FY 2011 Frequently Asked Questions on Reporting for the Federal Information Security Management Act and Agency Privacy Management, page 3, Answer to Question 8.

<sup>26</sup> Operating Directive *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, page 3, section 5b.



and identify priorities for training, testing, exercise, and maintenance.<sup>27</sup> The Operating Directive further provides that “[t]he BCM framework is a suite of plans used to prepare its response, recovery, and restoration of business processes in the event of a disruption, and that plans for business continuity are grouped under continuity of operations processes, business processes, and technology processes.”<sup>28</sup> It notes that “[m]any of these plans have dependencies and must, therefore, be synchronized,” and that “[p]lans to recover business processes at high levels are considered to be subsets of the continuity of operations processes.”<sup>29</sup>

Operating Directive 24-04.09, describes the agency’s COOP plan as directing “its focus on supporting the SEC’s executive leadership and essential organizational structure,” and references various supporting plans, such as the BRP, that deal with immediate crisis operations and communications throughout the COOP plan’s activation.<sup>30</sup> The Operating Directive further states that each functional office addresses functional level business processes that directly support the COOP plan in a contingency plan, and notes that examples of functional level business processes include human resources, procurement, public relations, facilities management, and legal and other services based upon the results of the agency-wide BIA.<sup>31</sup> According to the Operating Directive, critical business processes at the organizational unit and regional levels are maintained through BCPs, which serve as a primary input in the COOP plan. It also states that BCPs are managed by the organizational units that own the business processes and/or facilities, under the approval of the COOP plan coordinator.<sup>32</sup>

As noted above, OIT has primary responsibility for developing and managing the SEC’s technology processes for the BCM structure. Operating Directive 24-04.09 provides that each major application and general support system<sup>33</sup> in the SEC has a supporting Information Technology Contingency Plan (ITCP) (also

---

<sup>27</sup> Operating Directive *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, page 3, section 5c.

<sup>28</sup> Operating Directive *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, pages 3-4, section 5c.

<sup>29</sup> Operating Directive *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, pages 3-4, section 5c.

<sup>30</sup> Operating Directive *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, page 4, section 5d.

<sup>31</sup> Operating Directive *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, page 4, section 5d.

<sup>32</sup> Operating Directive *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, page 4, section 5e. Our review did not disclose that any one individual is currently performing the function of the COOP plan coordinator. As noted above, primary COOP responsibility transitioned from the former Office of the Executive Director to the OCOO in 2011 and the agency’s COOP program is under review.

<sup>33</sup> A major application is define as one “that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or unauthorized modification of, the information in the application.” The general support system interconnects “information resources under the same direct management control that share common functionality.” Operating Directive *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, page 2.

referred to as an ISCP) that includes detailed procedures for responding, recovering, and restoring information systems that are damaged or destroyed in the event of a disruption. According to the Operating Directive, the ITCP addresses emergency situations covered in a DRP for an information system.<sup>34</sup>

Operating Directive 24-04.09, further provides that each ITCP is supported by a BIA, and that “[t]he result of the BIA is used to determine overall contingency requirements and priorities.”<sup>35</sup> Implementing Instruction 24-04.09.01, Business Impact Analysis, provides that the BIA is an essential component of the SEC’s BCM program and notes that the “[t]he BIA links specific system components with the critical services they provide, identifying the consequences that disruption of the system’s availability would have on the SEC mission.”<sup>36</sup> The Implementing Instruction describes the four phases of the BIA process: pre-planning and coordination; information collection and research; identification of critical information technology assets; identification of allowable outage and recovery times; and development of recovery priorities; and post BIA activities and maintenance.<sup>37</sup> Under the Implementing Instruction, recovery time objectives for systems are determined based upon the following:

1. whether the availability of the information technology systems in question can be recovered partially or must be totally restored in order for mission-critical processes to continue; and
2. balancing the cost of information system in operability against the cost of the resources required to restore the information system.<sup>38</sup>

In addition, the SEC’s Disaster Recovery Planning Policy, OIT-00003-001.0, is intended to ensure that OIT is in a position to recover its full infrastructure<sup>39</sup> in the event of a disaster. The policy “supports a [REDACTED] strategy of mirroring and critical server rebuilds, as determined by OIT management,” and “sets forth a strategy requiring reallocation and rebuilding of OIT resources in order of criticality.”<sup>40</sup> Further, under this policy, the OIT Disaster Recovery Specialist is required to ensure that disaster recovery related issues are addressed, provide disaster recovery guidance to project management and staff, coordinate and/or

---

<sup>34</sup> Operating Directive *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, pages 4-5, section 5f.

<sup>35</sup> Operating Directive *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, pages 4-5, section 5f.

<sup>36</sup> Implementing Instruction *Business Impact Analysis*, II 24-04.09.01 (02.0) August 22, 2011, pages 2, Section 5a.

<sup>37</sup> Implementing Instruction *Business Impact Analysis*, II 24-04.09.01 (02.0), August 22, 2011, pages 2-4, Section 5c.

<sup>38</sup> Implementing Instruction *Business Impact Analysis*, II 24-04.09.01 (02.0), August 22, 2011, page 3 Section 5c(4).

<sup>39</sup> The term “infrastructure” refers to the underlying technological components that constitute an organization’s enterprise architecture; it includes hardware, operating systems, shared storage, data/voice communications, database, developments of maintenance tools, and application software.

<sup>40</sup> *Disaster Recovery Planning Policy*, OIT-00003-001.0, August 6, 2002, page 1, Section 2.

conduct BIAs, coordinate and validate disaster recovery testing, and ensure that disaster recovery information is maintained in the [REDACTED]

<sup>41</sup>

## Testing Programs for COOP, DRP and Pandemic Plans

FCD 1 requires all agencies to plan, conduct, and document periodic tests, training, and exercises to prepare for continuity emergencies and disasters, identify deficiencies, and demonstrate the viability of their COOPs.<sup>42</sup> Appendix K of FCD 1, "Test, Training, and Exercises (TT&E) Program," lists the following elements that must be included in an agency's testing program:

1. Annual testing of alert, notification, and activation procedures for continuity personnel and quarterly testing of such procedures for continuity personnel at agency headquarters.
2. Annual testing of plans for recovering vital records (both classified and unclassified), critical information systems, services, and data.
3. Annual testing of primary and [REDACTED] infrastructure systems and services (e.g., power, water, fuel) at alternate facilities.
4. Annual testing and exercising of required physical security capabilities at alternate facilities.
5. Testing and validating equipment to ensure the internal and external interoperability and viability of communications systems, through monthly testing of the continuity communications capabilities outlined in Annex H (e.g., secure and non-secure voice and data communications).
6. Annual testing of the capabilities required to perform an agency's MEFs, as identified in the business process analysis (BPA).
7. Conducting annual testing of internal and external interdependencies identified in the agency's continuity plan, with respect to performance of an agency's and other agencies' MEFs.
8. A process for formally documenting and reporting tests and their results.
9. Reporting the test results as directed by the Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA).<sup>43</sup>

In addition, the National Strategy for Pandemic Influenza Implementation Plan, issued by the Homeland Security Council in May 2006, noted as follows:

---

<sup>41</sup> *Disaster Recovery Planning Policy*, OIT-00003-001.0, August 6, 2002, page 2, Section 7b.

<sup>42</sup> *Federal Continuity Directive 1 (FCD 1)*, February 2008, page 10.

<sup>43</sup> *Federal Continuity Directive 1 (FCD 1)*, February 2008, page 62, Annex K, Testing section.

“Testing, training, and exercising of COOP capabilities are essential to assessing, demonstrating, and improving the ability of organizations to execute their COOP plans and programs during an emergency. Pandemic influenza COOP plans should test, train, and exercise sustainable social distancing techniques that reduce person-to-person interactions within the workplace.”<sup>44</sup>

The SEC has annual testing schedules for its COOP and DRP. As part of a government-wide continuity exercise referred to as “Eagle Horizon,” the SEC’s last COOP plan testing was performed on June 23, 2011. Overall DRP testing of selected systems was conducted for the Operations Center in June and November 2011, and quarterly data integrity testing is performed as part of the DRP. Regional office DRP testing is conducted on a staggered schedule over a three-year period. The SEC last conducted a pandemic flu exercise in 2007.

## Objectives

The overall objective of TWM’s review was to determine whether the SEC had a viable COOP, BCP, and DRP that sufficiently supported its operations at its Headquarters, Operations Center, and 11 regional offices. Further, the review sought to determine if the Commission is adequately prepared to perform essential functions during business continuity or disaster recovery event resulting from human/natural disasters, national emergency, or technological events which could impact the Commission’s ability to continue mission-critical and essential functions. The sub-objectives of our review were to:

- Evaluate the Commission’s pandemic plan to ensure it is formal, documented, well-communicated, has been tested at regular intervals, and meets the objectives of the *National Strategy for Pandemic Influenza: Implementation*;
- Assess the Commission’s implementation and testing of its pandemic plan;
- Determine the Commission’s plans for protecting its employees and contractors during a pandemic occurrence; and
- Evaluate the Commission’s plans for sustaining essential functions during high rates of employee absenteeism.

---

<sup>44</sup> *National Strategy for Pandemic Influenza Implementation Plan*, May 2006, page 167.

# Findings and Recommendations

---

## **Finding 1: SEC's COOP Policies, Procedures and Documents Require Updating, More Cohesiveness, and Inclusion of Missing Elements**

SEC's COOP policies and directives are incomplete and outdated. In addition, the SEC's COOP plan and an array of supplemental documents are outdated, have missing elements, and do not correlate with the SEC business needs identified under FISMA. Also, the current overall COOP plan document is a draft.

### **SEC COOP Policies, Directives and Documents Are Out of Date and Incomplete**

While the SEC does have a COOP function and plan (including relocation sites and testing) in place, the program needs overall improvements. In particular, the SEC's COOP policies, directives and documents are: (a) out-of-date and incomplete, (b) not comprehensive; and (c) currently not being followed in some respects.

Currently, the SEC's COOP policies and procedures are limited to OIT-issued policy documents. OIT's policies and procedures that are related to COOP include Operating Directive 24-24.09 (02.0), Information Technology (IT) Security Business Continuity Management Program, dated August 23, 2011; Implementing Instruction 24-04.09.01(02.0), Business Impact Analysis, dated August 22, 2011; Disaster Recovery Planning Policy, OIT-00003-001.0, dated August 6, 2002; and Disaster Recovery Planning Procedures, OIG-00047-001.0, dated February 4, 2003. The Disaster Recovery Planning Policy and Procedures documents are clearly outdated. Moreover, while Operating Directive 24-04.09 was revised in 2011, it is nonetheless outdated in certain respects. For example, it refers to the Office of the Executive Director, which no longer exists. Further, as noted below, it discusses BCPs and ITCPs in detail, even though the SEC decided not to prepare these types of documents for its systems because they believes the necessary elements are already included in the DRPs and BIAs.

The COOP plan documentation in place for the SEC's

are out-of-date. Further, these documents did not have signatures



**Regional Office and Division Lines of Succession Outdated.** The Headquarters COOP plan requires the line of succession to be [REDACTED] for the SEC's divisions, offices and regional offices. Further, each division and office head must establish an intra-office succession roster that is also at [REDACTED] for each critical office position or responsibility and ensure that this roster is effectively communicated within the division/office, to the Office of the Secretary, and other offices as necessary. The information is required to be maintained as part of the divisions/office's critical documents, accessible remotely in electronic form. We found that this required information was out-of-date and is not being properly maintained. The documents were dated 2004 to 2008, and many of the personnel listed in the documents were no longer in the SEC telephone registry and have likely left the agency.

**Division/Office and Regional Office Vital Records Are Not Complete or Up to Date.** The term "vital records" includes "information systems and applications, electronic and hardcopy documents, references, and records needed to support PMEFs and MEFs during a continuity event."<sup>46</sup> Categories of vital records include emergency operating records, and rights and interests records.<sup>47</sup> The SEC has included vital records information in its COOP plan; the overall plan includes an appendix, which is based on the information provided in the individual division/office and regional office COOP supplements.

The SEC divisions/offices and regional offices have included in their COOP supplemental plans, spreadsheets with tabs that list their vital records. Our review of these documents disclosed that they were templates that have incomplete content. Specifically, we found that the spreadsheets for all of the regional offices and 2 of the 5 randomly selected divisions/offices were missing key information. Further, the data listed in the supplement documents does not match the information contained in the OIT contingency plan COOP document. The spreadsheets were dated between 2004 and 2008 and have not been updated since then.

The vital records that were listed referenced both hard copy and electronic documents and drive locations for the data. However, the vital records spreadsheet supplements do not indicate specifically where the information is maintained, who is responsible for collecting it in the event of COOP activation, or how the information is to be accessed if the facility is not accessible. They also do not identify how hardcopy-only data should be recovered or stored.

In addition to the individual division/office and regional office vital records data, the main Headquarters COOP plan included a section on vital records. However, information for six divisions/offices [REDACTED]

<sup>46</sup> *Federal Continuity Directive 1 (FCD 1)*, February 2008, Annex I, page I-1.

<sup>47</sup> *Federal Continuity Directive 1 (FCD 1)*, February 2008, Annex I, page I-1.

[REDACTED] were not specified. In addition, the SEC has not defined a single location where all division/office and regional office vital records requirements should be backed up and verified.

**Headquarters and Operations Center Overall DRPs Are Not Present Within the COOP documentation.** An organization's DRP "applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period."<sup>48</sup> A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. The DRP plan may be supported by multiple information system contingency plans to address recovery of impacted individual systems once the alternate facility has been established.<sup>49</sup> Our review of the SEC's various COOP documents revealed that there is no specific DRP for SEC's Headquarters and the Operations Center. Some DRP items are included in the SEC's overall COOP document and OIT contingency plan; however, these documents are under revision and in draft form.

**Individual System and Regional Office DRPs are Outdated, In Draft Form and/or Incomplete.** During our review, we identified numerous problems with the DRPs for individual systems. Of the [REDACTED] systems reviewed, we found that [REDACTED] hosted systems did not have DRPs, and [REDACTED] hosted systems did not have DRPs.<sup>50</sup> Further, [REDACTED] system DRPs were in draft form, and [REDACTED] DRPs were outdated. Moreover, all the DRPs we reviewed were missing some traditional elements (e.g., risk management, budget and acquisition, order of succession, concurrent processing, recovery period, access control policy and procedures, alternate facilities, alternate site travel logistics, vital records, restoration, personnel and vendor contract lists, relocation of families, service level agreements, and additional notification procedures).

With respect to our review of regional office DRPs (as well as the overall COOP plan document and the OIT contingency plan), a detailed list of issues we identified with those documents is included at Appendix II.

**The SEC Does Not Prepare BCPs or ISCPs for its Information Systems.** BCPs address sustaining an organization's mission or business processes and the information systems that support those mission or business processes during and after a significant disruption. BCPs are often developed at the organization's

---

<sup>48</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 10, section 2.2.6.

<sup>49</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 10, section 2.2.6.

<sup>50</sup> Appendix III includes a list of the [REDACTED] systems for which no DRP had been prepared.



field level or for mission or business processes that are not prioritized as mission essential.<sup>51</sup>

Our review determined that the SEC only prepares DRPs and BIAs for its applications and does not prepare BCPs or ISCPs, even though Operating Directive 24-04.09, requires them to be prepared and indicates that BCPs serve as a primary input in the COOP plan.<sup>52</sup> OIT staff stated that BCPs and ISCPs were not needed because the contents of the BIAs and DRPs included the components of a BCP or ISCP. However, as described below, we found that some BCP elements were missing from the SEC's COOP documents.

**Missing Business Continuity Plan Elements.** Our review found that some BCP elements (e.g., budget and acquisition, concurrent processing) were not addressed in the SEC's DRPs and BIAs.<sup>53</sup> A DRP refers to an information system-focused plan that is designed to restore operability of one or more information systems at an alternate site after a major disruption that usually causes physical damage to the original data center.<sup>54</sup> We determined that the SEC's current DRP and BIAs do not address the aspects of BCPs, thus giving rise to the possibility of failure should an actual event occur.<sup>55</sup> According to OD 24-04.09, BCPs are to be managed by the organizational units that own the business processes and/or facilities, under the approval of the COOP coordinator.<sup>56</sup>

We also found that the SEC's COOP documents lack the critical tie to the SEC's business and mission essential functions. While the SEC prepared BIA documents, these documents do not necessarily reflect what is actually needed for agency activities that must be performed immediately versus activities that are not needed immediately, and support the agency's mission after the fact. Further, the information contained in the SEC's BIAs does not coincide with the reporting under FISMA regarding the availability needs for the agency's systems. One example of a business function that has an immediate requirement is the SEC's [REDACTED], which is a collection of software [REDACTED] [REDACTED].

---

<sup>51</sup> NIST SP 800-34 Rev 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, Appendix C, page C-1.

<sup>52</sup> Operating Directive *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, page 4, section 5e. The policy further indicates that SEC division directors, office heads, and regional directors are responsible for organizational or regional level BCP. Operating Directive 24-04.09 (02.0), *IT Security Business Continuity Management Program*, August 23, 2011, page 6, section 6.4, section 5e.

<sup>53</sup> The BCP elements that we used in reviewing the SEC's DRPs and BIAs were based upon best practices derived from a variety of sources including, among others, NIST 800-34, the Interagency Statement on Pandemic Planning, as well as SEC Operating Directive 24-04.09.

<sup>54</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page C-1, Appendix C, paragraph 3.

<sup>55</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, Appendix C, paragraph 3.

<sup>56</sup> Operating Directive *IT Security Business Continuity Management Program*, OD 24-04.09 (02.0), August 23, 2011, page 4, section 5e.

[REDACTED] This critical real-time function has not been defined in the SEC's BIAs.

TWM examined all system DRPs and BIAs and found the date it was prepared and the date reviewed. We then randomly selected [REDACTED] systems to conduct a detailed review of the documents to determine whether traditional elements were included. We found missing elements including the [REDACTED] where system specific documentation and scripts are located, background information, validation and functionality testing processors, alternate processing procedures, business process specific data input/output diagrams, and software license requirements. A list of the specific issues we identified based upon the documents we reviewed is at Appendix III.

**Business Impact Analysis Missing, Outdated, or Incomplete.** While we determined that a BIA document was present for all internally hosted systems, some of the BIAs were outdated and/or incomplete. In particular, we found that the completed BIAs for [REDACTED] systems are three years and are, therefore, are considered out-of-date. Further, we found that BIAs had not been updated to reflect the fact that the SEC's former district offices are now regional offices. We also found there were no BIAs for the [REDACTED] FISMA-reportable [REDACTED] hosted systems.

Our detailed review of the BIA's for [REDACTED] selected systems revealed that they lacked traditional BIA elements. For example we found the following sections has missing information such as: [REDACTED] were missing the Background section; three were missing the Resources section; one was missing the Process Criticality section; six were missing the Threats and Hazards section; [REDACTED] were missing Cost Balance Point section; [REDACTED] were missing the MEF Impact section; [REDACTED] were missing the Threat Risk Value section; and [REDACTED] were missing the Recovery Priority Objective section. Further, there was no indication that the BIAs had been reviewed or approved, and [REDACTED] system's BIA Data Collection forms did not have a date indicating when the forms were completed.

### **Integration of Pandemic Planning into COOP Documents Is Needed.**

Pandemic influenza "is a global outbreak of disease that occurs when a new influenza virus emerges in human populations and causes serious illness. Because there is little natural immunity, the disease can spread easily from person to person, rapidly moving across the country and around the world."<sup>59</sup>

---

<sup>57</sup> We were informed that management has recently purchased a license for an Internet service option for the [REDACTED] however, this option is not yet operational.

<sup>58</sup> In contrast to the immediate requirement for the [REDACTED] [REDACTED] could be performed manually during an unscheduled event and, therefore, would not have the same recovery needs or timeline as an essential activity requiring immediate attention.

<sup>59</sup> NIST SP 800-34 Rev 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, Appendix D, page D-2. In addition, FCD 1 provides that continuity planning should include "planning for the Review of the SEC's Continuity of Operations Program April 23, 2012 Report No. 502

According to the Contingency Planning Guide for Federal Information Systems, “[c]ommon strategies to protect personnel health during a pandemic outbreak include stricter hygiene precautions and reducing the number of personnel working in close contact with one another through implementation of ‘social distancing.’ Approved telework arrangements facilitate social distancing through working at home while sustaining productivity. Government-run telework sites are also available to federal employees who cannot work from home or the office.”<sup>60</sup>

According to pandemic guidance, a BCP “should address pandemics and provide for a preventive program, a documented strategy scaled to the stages of a pandemic outbreak, a comprehensive framework to ensure the continuance of critical operations, a testing program and an oversight program to ensure that the plan is reviewed and updated.”<sup>61</sup> As noted above, OIT only creates DRPs and BIAs for SEC applications and do not create BCPs. We found that only two of the regional offices’ COOP plan supplements [REDACTED] included any pandemic information.

While the SEC has a pandemic plan in place, the lack of a BCP addressing pandemic events could negatively impact the implementation of the pandemic plan. Further, the overall SEC COOP plan indicates that it includes events related to pandemic, but it does not contain specific information related to pandemic planning or impact on operations. Further, we found that there is no specific mention in the pandemic plan of alternate procedures for credentialing and hiring during a pandemic or how these functions would be accomplished remotely. If the systems required to be accessed remotely were non-operational, credentialing and hiring would have to be accomplished using manual processes until the systems were available and then reconstructed in the electronic system, which might prove to be difficult during a pandemic event.

**Review and Approval Not Indicated on COOP Program Documents.** FCD 1 outlines the requirements to support the continuity program management cycle, noting that “agencies will develop a continuity multiyear strategy and program management plan that provides for the development, maintenance, and the annual review of continuity capabilities.”<sup>62</sup> These requirements include designating and reviewing MEFs and PMEFs, as applicable, and defining both short-term and long-term goals and objectives for plans and procedures.<sup>63</sup>

---

challenges posed by extended events (like a pandemic) that occur in repeated waves.” *Federal Continuity Directive 1 (FCD 1)*, February 2008, Annex A, page A-4

<sup>60</sup> NIST SP 800-34 Rev 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, Appendix D, page D-2. We were informed that in the past, the SEC Executive Director had approved telework for SEC employees during any officially recognized pandemic, with the concurrence of an employee’s supervisor.

<sup>61</sup> Interagency Statement on Pandemic Planning, page 1. (This is joint guidance issued for financial institutions by the Federal Financial Institutions Examination Council agencies.)

<sup>62</sup> *Federal Continuity Directive 1 (FCD1)*, February 2008, page 6.

<sup>63</sup> *Federal Continuity Directive 1 (FCD1)*, February 2008, page 6.

Based upon our review of the DRP and BIA documents for the individual systems, we determined that the documentation did not evidence review and approval at least annually. We also found that the SEC's Pandemic Plan did not indicate the date it was reviewed.

**Recommendation 1:**

The Office of the Chief Operating Officer should ensure that the Office of Freedom of Information Act, Records Management and Security completes its review of the agency-wide continuity of operations program (COOP) to ensure the Commission's COOP is comprehensive, cohesive, and in compliance with federal guidance.

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

**OIG Analysis.** We are pleased that OFRMS concurred with this recommendation.

**Recommendation 2:**

The Office of Freedom of Information Act, Records Management, and Security should revise and update the Commission's continuity of operations program policies and procedures to ensure they are comprehensive, complete, and up-to-date.

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

**OIG Analysis.** We are pleased that OFRMS concurred with this recommendation.

**Recommendation 3:**

The Office of Freedom of Information Act, Records Management, and Security (OFRMS) and Office of Information Technology (OIT), in conjunction with the program divisions/offices and regional offices, should update, revise and finalize all continuity of operations program (COOP) documents, including the overall Headquarters COOP plan, individual division/office COOP plans, regional office COOP supplements, disaster recovery plans, business continuity plans and business impact analyses, and pandemic plans supplements. OFRMS and OIT should ensure these documents are complete and include all the necessary elements, and that they properly define the Commission's essential functions. In addition, processes should be implemented to ensure annual review and approval of these documents.

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

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

**Recommendation 4:**

The Office of Freedom of Information Act, Records Management, and Security, in conjunction with program and regional offices, should ensure that vital records and lines of succession are properly identified, documented and readily available during continuity events.

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

**OIG Analysis.** We are pleased that OFRMS concurred with this recommendation.



[REDACTED]

[REDACTED]

[REDACTED]

**Recommendation 5:**

The Office of Information Technology (OIT), in conjunction with the primary program information users, should identify [REDACTED] at the alternate locations should [REDACTED] be unavailable. Further, OIT should review the Securities and Exchange Commission's (SEC) network and topology to ensure there are [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.

**Recommendation 6:**

The Office of Information Technology should ensure proper power distribution [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 3: The COOP Systems' Availability Categorization and Utilization Should be Reviewed**

Our review found inconsistencies between the availability categorization of the systems reported to OMB under FISMA and the recovery time objectives established for SEC COOP systems.

### **SEC Recovery Time Objectives are Not Consistent With FISMA's System Categorization for Availability**

Effective contingency planning begins with the development of an organization contingency planning policy and subsection of each information system to a BIA. This facilitates the prioritization of systems and processes based on the Federal Information Processing Standard (FIPS) 199 impact level (utilized under FISMA) and develops priority recovery strategies for minimizing loss. FIPS 199 provides guidelines for determining information and information system impact to organizational operations and assets, individuals, other organizations, and the nation through a formula that examines the three security objectives of confidentiality, integrity, and availability.<sup>65</sup> The highest rated of the three security objectives determines the overall security categorization for the system of high, moderate, or low, based upon the definitions contained in FIPS 199.<sup>66</sup>

By reviewing the FISMA systems that the SEC reported to OMB for 2011, we determined that most of the SEC's FISMA-reportable systems have a system security categorization of moderate, which indicates that the goal of system availability is no more than moderate and, in some cases, may be low. Recovery time objectives are the overall length of time an information system's components can be in the recovery phase before the organization's mission or business functions are negatively impacted. Our review found that some individual system BIAs indicated a recovery time objective of [REDACTED] while those same systems have only a security categorization of moderate under FISMA. Further, we found FISMA security systems categorized as moderate that were listed with recovery time objective of [REDACTED] in the COOP BIA matrix

---

<sup>65</sup> NIST SP 800-34 Rev 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 5, section 2.1.

<sup>66</sup> NIST SP 800-34 Rev 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 6, section 2.1.



recovery time objective document, even though the BIA stated a different recovery time objective for those systems. For systems with a moderate to low availability as indicated by an overall FISMA security categorization of moderate, SEC COOP established recovery time objectives may be overly aggressive and could result in unnecessary expense in documentation, testing, and infrastructure. Finally, our examination of documents provided by SEC personnel reflecting their review of the externally hosted systems included in the SEC's FISMA-reportable systems identified some instances where the availability rating was either low or not stated, while the SEC reported these systems under FISMA as having an availability rating of moderate.

### **Recovery Time Objectives Need to Be Consistent with System**

**Functionality.** As noted above, most SEC FISMA-reportable systems have a system security categorization of moderate. Moderate availability does not typically indicate a recovery time objective of [REDACTED] such a short recovery time is usually appropriate for systems with a high availability requirement. We also found COOP documentation stating that communications and information systems would be available within [REDACTED] at the alternate location after plan activation and capable of supporting the continuation of SEC essential functions for a period of up to 30 days, or until normal operations resume. An availability period of [REDACTED] does not correspond with individual system recovery time objectives of [REDACTED]

SEC management indicated that availability goals for SEC systems are defined based on FCD 1 and the SEC's definition of essential, mission essential, and program mission essential functions. These availability goals should be consistent with the FISMA ratings and BIAs for the systems. However, we found SEC systems with a recovery time objective of [REDACTED] which was inconsistent with the COOP documentation for these systems, as well as the FISMA categorization of the systems. For example, the NotiFind emergency notification system has a MEF designation of immediate, but is being externally hosted at a location with an availability rating of moderate. Further, the SEC has no DRP for NotiFind or any records showing that testing has been conducted for the system. We also found that there some systems listed as critical in the BIA Matrix Recovery Time Objectives even though the BIAs themselves state that the systems are not critical.

**Underutilization of [REDACTED]** The SEC's Disaster Recovery Planning Policy, OIT-00003-001.0, which was issued in 2002, requires SEC personnel to maintain disaster recovery information in the [REDACTED]<sup>67</sup> However, [REDACTED] is not being fully utilized for this objective at this time. While [REDACTED] has been used for templates and some list keeping, the

---

<sup>67</sup> SEC Disaster Recovery Planning Policy, OIT-00003-001.0, August 6, 2002, page 2, section 7b.

system has not been fully utilized, raising questions as to why it should be rated critical for disaster recovery purposes or even retained.<sup>68</sup>

**Recommendation 7:**

The Office of Freedom of Information Act, Records Management, and Security, in conjunction with the Office of Information Technology and system owners, should revise the Securities and Exchange Commission (SEC) system recovery time objectives to specify more realistic timeframes, based on the ability to transition to the alternate site, and then determine acceptable recovery times. The recovery plan and priority of recovery of the systems should be based on the overall mission of the agency with a focus on real-time monitoring of the markets. Further, the identification of high priority systems should focus on the immediate mission of the agency, and systems documentation should also be reviewed to ensure proper recovery priority is reflected based on the contribution to the SEC's mission and functions.

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

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

**Recommendation 8:**

For underutilized systems such as the [REDACTED] [REDACTED] the Office of Information Technology should consider discontinuing maintenance, retiring the system, or alternatively making more robust use of the system such that additional Commission funds are not wasted on underutilized systems.

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

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

---

<sup>68</sup> OIT indicated that it was considering changing the rating of [REDACTED] to non-critical based upon its review of that system.

## Finding 4: Improvements Are Needed in Recovery from [REDACTED] and Related Testing

The regional offices' disaster recovery exercises do not include restoration from [REDACTED] which is the primary method used to restore regional office data, or from the [REDACTED] that serves as the secondary recovery method. In addition, the current [REDACTED] processes are insufficient.

### The SEC Has Not Tested Recovery from [REDACTED]

[REDACTED]

According to the *Contingency Planning Guide for Federal Information Systems*, "[s]ystem data should be backed up regularly. Policies should specify the minimum frequency and scope of [REDACTED] (e.g., daily or weekly, incremental or full) based on data criticality and the frequency that new information is introduced. Data [REDACTED] policies should designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite."<sup>71</sup> In addition, "[REDACTED] media should be stored offsite in a secure, environmentally controlled location."<sup>72</sup>

The *Contingency Planning Guide for Federal Information Systems* further provides that testing is a critical element of a viable contingency capability. "Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan."<sup>73</sup>

By reviewing the FISMA systems the SEC reported to OMB for 2011, we determined that most of the SEC's FISMA reportable systems have a system security categorization of moderate, which indicates that the availability is no more than moderate and, in some cases, may be low. For a security

<sup>69</sup> As previously mentioned, the regional offices are [REDACTED] and management expects to have this effort completed during 2012.

<sup>71</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 21, section 3.4.2.

<sup>72</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 46, section 5.1.5.

<sup>73</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 27, section 3.5.1.

categorization of moderate impact, exercise procedures should be developed to include an element of system recovery from [REDACTED] [REDACTED]<sup>74</sup>

The SEC currently utilizes automated [REDACTED] as the [REDACTED] [REDACTED] for its SEC systems, although the SEC has plans to replace the [REDACTED] [REDACTED] with a [REDACTED] in the near future. We found that SEC's regional offices have not tested system recovery from [REDACTED] and have not successfully transitioned to an alternate site. We also identified several lessons learned reports from regional offices DRP testing exercises and open plans of action and milestones indicating issues and concerns with the [REDACTED]

### **Difficulties with Data Restoration at the [REDACTED]**

[REDACTED] As part of our review, we visited both the [REDACTED] [REDACTED] to observe the restoration or regularly-scheduled [REDACTED] of [REDACTED] randomly selected systems. [REDACTED] of these systems were part of the database storage area network. OIT staff indicated that in order to restore these individual systems, the entire server hosting the multiple applications and systems would have to be restored, which would have taken well over [REDACTED] hours to restore. For another group of systems we selected, OIT staff stated that the [REDACTED] of the application folder takes over [REDACTED] hours and it would take at least that long to restore the systems. As a consequence, it was questionable whether the indicated recovery time objectives for these systems of [REDACTED] could be met. Further, for the last of the [REDACTED] systems selected for testing, the [REDACTED] [REDACTED] OIT staff could not locate the [REDACTED] [REDACTED] and indicated that the [REDACTED] application was not being [REDACTED]. Finally, we found that OIT's June 2011 Headquarters disaster recovery exercise did not include restoring or testing [REDACTED] although testing of the [REDACTED]

### **Review of Individual System and Regional Office [REDACTED] Procedures.** In order to assess individual system [REDACTED] we reviewed BIAs for a random sample of [REDACTED] critical systems:

[REDACTED]  
[REDACTED]  
Our review found the [REDACTED] system (a FISMA reportable system, even though it is a test system with only 6 to 8 users) was scheduled to be backed up biweekly, instead of in daily increments and weekly [REDACTED] per the DRP requirements. We also found that the COOP, DRP and BIA documents for [REDACTED] [REDACTED] did not include language regarding [REDACTED], there was no DRP for the [REDACTED] system, and the [REDACTED] BIA

<sup>74</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 30.



**Regional Office [REDACTED] May Not Be Readily Available.** While the regional office transition sites (e.g., the [REDACTED] [REDACTED] are capable of hosting systems for the SEC's regional offices in the event of a disaster recovery, we determined that the regional office transition sites may not have ready access to [REDACTED] [REDACTED] because they are kept at [REDACTED], per the disaster recovery plans. Additionally, we found that eight regional offices [REDACTED] [REDACTED] have not identified alternate locations (or emergency operation centers) for SEC staff to work from during disaster recovery and have not addressed in DRPs or disaster recovery testing the procedures for remotely accessing information from the designated transition site. Further, the regional office DRPs do not include the number of software licenses for each product used for systems or a licensing strategy.

**Survey Questions Concerning [REDACTED] Access and Validation.** We conducted an agency-wide survey to gather information on the staff's perspectives on the SEC's COOP, including the DRP, BCP, essential personnel, and OIT continuity-related activities, as well as the SEC's pandemic plan. The survey's overall response rate was over 70 percent. The survey results indicated that there was insufficient understanding of the requirements for maintaining adequate [REDACTED] on the part of those responding to questions about [REDACTED]. Seventy-six percent of the 132 persons who responded to the pertinent survey question indicated that they knew where their division/office's [REDACTED] was located, but only 30 percent of 130 respondents indicated that they could access the [REDACTED]. Further, 43 percent of 115 respondents indicated they had not verified that their critical data was being [REDACTED] within the last year or a longer time period.

#### **Recommendation 9:**

The Office of Information Technology (OIT), in conjunction with system owners, should identify the [REDACTED] requirements (e.g., files, data, and system software) for all systems (at minimum, Federal Information Security Management Act reportable systems). OIT should ensure that [REDACTED] requirements are documented, understood by the owner, and published for future reference. Further, OIT should ensure system software licenses and key requirements are included in [REDACTED] documentation, and the location of this information is known to ensure restoration capability at the alternate location site.

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

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

**Recommendation 10:**

The Office of Information Technology, in conjunction with the regional offices, should document the processes and procedures to be used in the event that a regional office needs to restore its systems at a regional office transition site, and the corresponding effect on the [REDACTED] procedures for other regional offices that may need to use a regional office transition site or alternate method to ensure recoverability.

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

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

**Recommendation 11:**

The Office of Information Technology (OIT) should continue its efforts to replace the regional office's tape [REDACTED] systems. Additionally, OIT should define a [REDACTED] and recovery strategy for multi-hosted application restoration for the regional offices. OIT should also document the system specific files and database items, in order to facilitate the ability to restore only necessary items, rather than the entire database, which could take many hours to accomplish and is not in line with the recovery time objectives for individual systems.

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

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

**Recommendation 12:**

The Office of Information Technology should implement consistent and appropriate [REDACTED] schedules for mission essential and Federal Information System Management Act reportable systems, including daily, weekly, and monthly [REDACTED] processes and procedures, to ensure these systems are recoverable.

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

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

**Recommendation 13:**

The Office of Information Technology should include in the Disaster Recovery Plan and Business Continuity Plan, testing steps that are designed to ensure the restoration from [REDACTED] media that is consistent with the requirements for systems that are rated as moderate, in accordance with the National Institute of Standards and Technology guidance under the Federal Information Systems Management Act.

**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: Remote Access/Telework Testing Was Not Included in the SEC's DRP and Pandemic Plan Testing**

There is no evidence that remote access (user access from non-office locations) was tested during the DRP and pandemic plan testing that was conducted from 2007 to 2011.

### **The SEC is Not Fully Testing Remote Access/Telework for All Essential Personnel on a Regular Basis**

Federal legislation has placed a priority on telework. For example, on December 8, 2004, Congress enacted Public Law 108-447, which required the SEC to certify within two months that telecommuting opportunities were made available to 100 percent of the eligible workforce. On December 9, 2010, the Telework Enhancement Act of 2010, Public Law 111-292, was enacted, which required that, within 180 days, executive agencies establish a telework policy authorizing telework for all eligible employees, determine the eligibility of all employees to participate in telework programs, and notify all employees of their eligibility to telework. The Telework Enhancement Act of 2010 also required agencies to incorporate telework into their COOP plans.



An effective telework program requires that employees be able to access the SEC network remotely. The SEC has established two primary methods for remote access: (1) the use of a token to acquire virtual private network (VPN) access; (2) the use of a [REDACTED]<sup>75</sup> Through VPN and/or [REDACTED] SEC personnel and contractors can gain access to their e-mail, network applications, [REDACTED] sites, network data files, and their desktops. The SEC has issued [REDACTED] tokens for access through VPN and [REDACTED] [REDACTED] SEC staff who have been identified as essential personnel under the SEC's COOP are required to have remote network access capability through both of these two primary methods.

Based upon a review of COOP documents including those found on the [REDACTED] [REDACTED] we identified personnel: (a) listed as essential who no longer work at the SEC, (b) listed as essential who have not been issued remote access devices, and (c) who were issued devices and have not tested them. Documentation related to COOP 2009 testing indicated that remote access testing was included as part of that exercise.<sup>76</sup> Further, our review of COOP and disaster recovery test plans and reports reflected that while there was some end-user testing conducted during disaster recovery, there was no indication that users were logging into the [REDACTED] from a telework or other alternate work site.

**Essential Personnel [REDACTED] Access.** Our review found that some essential personnel who had been issued [REDACTED] devices have never logged in or have not logged in remotely within the past year and, therefore, have not effectively tested their ability to log in during an unscheduled event. Of [REDACTED] identified essential personnel, [REDACTED] have been issued [REDACTED]. We reviewed system log extracts to determine whether those essential personnel had utilized their remote [REDACTED] access and found [REDACTED] had not logged onto the SEC's network remotely since March 2010. Further, we found that [REDACTED] of the [REDACTED] had never logged onto the SEC's network remotely.<sup>77</sup>

Remote access to the SEC's network serves as an important contingency capability in the event of an emergency or serious system disruption by providing access to SEC data for recovery teams or users from another location. If remote connectivity is not tested regularly, connectivity may be difficult during an event.

---

<sup>75</sup> While the SEC has other methods of remote access, such as [REDACTED] [REDACTED] we focused our review on [REDACTED] because these methods are more appropriate for conducting business activities lasting up to 30 days.

<sup>76</sup> We received this documentation after our fieldwork was completed.

<sup>77</sup> Of the [REDACTED] that OIT has issued to SEC contractors and employees as of December 2011, we found that 167 (11.2 percent) of the recipients had not logged onto SEC's network since March 2010.

**Essential Personnel VPN Access.** To review VPN access, we randomly selected [REDACTED] of the [REDACTED] essential personnel<sup>78</sup> and found that [REDACTED] (70 percent) had not logged onto the SEC's network through VPN since May 2010.

In addition, TWM encountered difficulties for establishing remote access to the SEC network. In fact, it took TWM over two months to fully establish VPN access and connectivity on laptops running three different operating systems. We found that while the remote access environment is equipped to support the majority of the SEC users, there are issues that need to be resolved with direction and support of configurations for the end user. Therefore, end users must review, configure, and test their remote access capabilities on a scheduled basis to ensure that their systems are operational if activation is required during an event.

**Identification of Remote Access for Five Systems Revealed Problems.** We randomly selected five of the COOP identified critical systems [REDACTED]

[REDACTED]

For the systems selected, we compared the identified number of system users contained in the DRP or BIA documents with the number of users who have been issued remote access devices according to the applicable group or function. We found that 60 percent of the user base was not immediately identifiable as having remote access. For one system, no information was available concerning the number of system users. We found that two systems had adequate remote access based on the user base.

**Remote Access to Desktops Could Be Improved.** We found that SEC contractors and employees who use SEC workstation-specific applications remotely must ensure that their office desktop computers (or laptops if left at the office) are turned on. Further, our survey of SEC personnel and contractors determined that 570 of 1,871 respondents (30.5 percent) indicated that their remote access of SEC computer systems required the normal worksite desktop or laptop to be left on, while 276 of 1,871 respondents (14.8 percent) were unsure as to whether the desktop or laptop had to be left on. Additionally, if the power is out at the SEC's office locations, contractors and employees who have workstation-specific software cannot access their desktops remotely. We found that remote access capabilities would be enhanced if remote access to desktop applications could function even if the user's desktop computer was turned off or did not have power.

---

<sup>78</sup> OIT could not readily determine how many of the [REDACTED] identified essential personnel had been issued tokens for remote VPN access.

**Teleworking and Remote Access Not Defined in COOP Documents.** We observed that the SEC's COOP documents do not clearly define when teleworking may be used for COOP activities or which staff members who have not been identified as essential personnel are allowed to telework. Our survey revealed that 934 of 2,334 of respondents (40 percent) did not know if they were required to work from an alternate worksite during an unscheduled event. Further, 417 respondents indicated that they were required to go to an alternate worksite during an unscheduled event, and 215 respondents indicated that they knew the location of their alternate worksite. Of these 215 respondents, 75 (34.9 percent) identified their "home or residence," as the alternate worksite. These responses imply that these individuals are scheduled to telework during an event even though this option is not specified in the COOP documents.

**Pandemic Specific Remote Access Requires Testing.** The SEC has a pandemic plan and its remote access capabilities appear to be adequate for this purpose. Specifically, we found that the remote access architecture of the SEC could handle the estimated 40 percent absenteeism rate during a pandemic (approximately ██████ personnel)<sup>79</sup> as ██████ remote access tokens have been issued to provide access to the servers at the Operations Center and the Alternate Data Center, and the remote access servers are designed to handle more than 5,000 users at each location. However, we found that the annual remote access testing specified in the pandemic plan has not occurred.

#### **Recommendation 14:**

The Office of Information Technology should ensure that remote access testing is included as part of all Continuity of Operations Program, disaster recovery and pandemic testing activities, including those performed in the regional offices, to ensure that essential personnel and a sample of the representative users of the system are able to function remotely during an unscheduled event.

**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.

---

<sup>79</sup> According to the Interagency Statement on Pandemic Planning, page 6, absenteeism may reach 40 percent during the peak weeks of a community outbreak during a severe pandemic. The estimate of ██████ listed as required to take the annual online COOP training for 2011.

**Recommendation 15:**

The Office of Information Technology (OIT), in consultation with the Office of Freedom of Information Act, Records Management and Security (OFRMS), should require semiannual testing of remote access devices to ensure up-to-date connectivity and ability for both essential personnel and non-essential personnel to access the Commission's network. In addition, OIT and OFRMS should implement a system notification warning prior to the connectivity testing date and then disable those devices that are not updated.

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

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

**Recommendation 16:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should consider implementation of alternate remote access solutions and/or internal directory structure that [REDACTED] and Federal Information Security Management Act reportable systems.

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

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

**Recommendation 17:**

The Office of Freedom of Information Act, Records Management and Security and the Office of Information Technology should update the Continuity of Operations Program (COOP) documents and necessary agreements to appropriately reflect authorized telework activities by Commission personnel during unscheduled events under the COOP, disaster recovery and pandemic plans, including equipment that will be used for teleworking in such circumstances.

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

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

## **Finding 6: COOP and Disaster Recovery Testing Activities Can Be Improved**

The SEC is not testing all of its DRPs annually. Past DRP testing did not include the “recovery phase” and “reconstitution phase.” Further, not all test, training, and exercise activities identified in NIST SP 800-53 guidance for a FISMA security categorization rating of moderate is being conducted. Further, the regional offices have not tested restoration to an alternate site, and the pandemic plan has not been tested since 2007.

### **The SEC’s COOP and DRP Testing Activities Need Improvement**

Annex K to FCD 1 provides as follows regarding the testing, training and exercise of an agency’s COOP:

The testing, training, and exercising of continuity capabilities is essential to demonstrating, assessing, and improving an agency’s ability to execute its continuity program, plans, and procedures. Training familiarizes continuity personnel with their roles and responsibilities in support of the performance of an agency’s essential functions during a continuity event. Tests and exercises serve to assess, validate, or identify for subsequent correction, all components of continuity plans, policies, procedures, systems, and facilities used in response to a continuity event. Periodic testing also ensures that equipment and procedures are kept in a constant state of readiness.<sup>80</sup>

Two elements of disaster recovery, the recovery phase and the reconstitution phase, are often overlooked in disaster recovery testing activities. The recovery phase is the “implementation of prioritized actions required to return an organization’s processes and support functions to operational stability following an interruption or disaster.”<sup>81</sup> Second, the reconstitution phase is the “process by which surviving and/or replacement organization personnel resume normal agency operations from the original or replacement primary operating facility.”<sup>82</sup> Further, OMB’s guidance to agencies on FISMA reporting for Fiscal year 2011

---

<sup>80</sup> *Federal Continuity Directive 1 (FCD1)*, February 2008, Annex K, page K-1.

<sup>81</sup> *Federal Continuity Directive 1 (FCD1)*, February 2008, Annex, page P-8.

<sup>82</sup> *Federal Continuity Directive 1 (FCD1)*, February 2008, Appendix P, page P-8.

provides that all agency information systems, including those operated by a contractor or other organization on the agency's behalf, must be tested at least annually.<sup>83</sup> As noted above, agencies are required to categorize systems subject to FISMA based upon the three security objectives of confidentiality, integrity, and availability, and the highest rating of the three objectives determines the overall system security impact rating of high, moderate or low. The Contingency Planning Guide for Federal Information Systems specifies that a functional exercise at an organization-defined frequency should be conducted for moderate-impact systems.<sup>84</sup> "The functional exercise should include all ISCP points of contact and be facilitated by the system owner or responsible authority. Exercise procedures should be developed to include an element of system recovery from [REDACTED]."<sup>85</sup>

**DRP Testing Does Not Currently Include All Systems.** In the course of our review, we learned that during the SEC's June 2011, disaster recovery testing exercise, [REDACTED] SEC systems were identified for testing.<sup>86</sup> Of these [REDACTED] systems, [REDACTED] were shown as passing from the end user testing, [REDACTED] of which were external systems [REDACTED] system failed; and [REDACTED] were not actually tested. There were no results listed for the remaining [REDACTED] systems, which were not scheduled to be included in the testing.

We further found that [REDACTED] (39.5 percent) internal systems were not included in the [REDACTED] failover testing that took place in June 2011 and November 2011. These systems included:

[REDACTED]

<sup>83</sup> OMB Memorandum for Heads of Executive Departments and Agencies on *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, M-11-33, September 14, 2011, FY 2011 Frequently Asked questions on Reporting for the Federal Information Security Management Act and Agency Privacy management, page 11, Answer to Question 8. See also 44 U.S.C. § 344(b)(5)(requiring agencies to perform "periodic testing and evaluation of the effectiveness of information

<sup>84</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 30.

<sup>85</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 30.

<sup>86</sup> While some additional systems were tested in the November 2011 disaster recovery exercise, the results of this testing were not available at the time TWM performed its fieldwork.

<sup>87</sup> The SEC is transitioning from the [REDACTED] to a shared service provider.

[REDACTED]

We also found [REDACTED] (40.8 percent) active systems did not have a DRP testing date scheduled at the time TWM completed its fieldwork for this review. These systems included:

[REDACTED]

**Insufficient DRP Testing for Regional Offices and Externally Hosted Systems.** We found that DRPs for seven regional offices [REDACTED] have not been tested annually, and two regional offices [REDACTED] did not include recovery phase testing in their most recent disaster recovery test plans. Also seven regional offices [REDACTED] did not include reconstitution phase testing in their latest disaster recovery test plans. Further, we found that the regional offices are not testing any element (e.g., a file or data record) from the system's [REDACTED] for systems with a moderate security rating.

Moreover, the regional offices disaster recovery plan exercises that took place from 2008 to 2011 were simulated, paper exercises and did not perform full functional testing of the equipment, such as transition to an alternate data center or restoration from [REDACTED]. Comprehensive testing, which confirms that information technology operations can be restored at a [REDACTED] in the event of an extended power failure at the primary site, should be conducted periodically to ensure that the plans are reasonable, effective, and complete, and that personnel know what their roles and responsibilities are in the enactment of the plans.<sup>89</sup>

---

<sup>88</sup> OIT informed us that the [REDACTED] is not in production however, this system was reported to OMB under FISMA.

<sup>89</sup> NIST 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006, page 6-2.

An externally hosted system is a system or application that is operated outside the SEC network and is not managed by SEC. OIT reviewed the externally hosted system documentation provided by external entities (both federal and private) for disaster recovery and contingency planning activities through the certification and accreditation process. Our review of this information revealed that the [REDACTED] for [REDACTED] externally hosted system, [REDACTED] was not stored in a secure, offsite, environmentally-controlled location. We further found that another externally hosted system, [REDACTED], [REDACTED], could be unavailable for up to two weeks and that this information was taken into account in determining the recovery time objectives for dependent systems. Based upon the documentation provided, we found that the externally hosted systems did not have regular disaster recovery exercises.

**Essential Personnel Have Not Sufficiently Participated in Testing.** The SEC has indicated in its OIT contingency plan that the COOP and disaster recovery testing exercise participation satisfies the requirement to ensure a trained workforce is available to support the SEC's mission critical functions during and following a disaster. However, our review of the 2011 annual COOP testing and exercise documentation, including attendee sign-in sheets, revealed that only [REDACTED] (3.1 percent) persons identified as essential personnel under the COOP attended that exercise. We found that this did not constitute an adequate participation level to ensure that essential personnel receive proper training.

Our review also did not find a sufficient level of participation by regional office essential personnel in disaster recovery testing to ensure that they are adequately trained. We found that seven regional offices [REDACTED] identified essential personnel in their COOP supplement. By comparing this information to disaster recovery testing reports, sign-in sheets, and other related data, we determined that approximately 88 percent of personnel identified as essential, did not participate in DRP testing. The remaining four regional offices [REDACTED] did not identify their essential personnel in their COOP supplement, so we were unable to determine whether their essential personnel participated in DRP testing. We concluded that regional office essential personnel have not been trained sufficiently in their roles and responsibilities under the COOP, disaster recovery, business continuity and pandemic plans.

**System Functionality Has Not Been Fully Tested in Connection with Disaster Recovery Plans.** DRPs for many of the SEC's systems included specific scripts to be used to verify system operation and functionality when the system is being established at an alternate site. We reviewed the annual disaster recovery testing documentation for 2007 to 2011, for [REDACTED] randomly selected systems, which included the disaster recovery test results, lessons learned, and script results. We found that disaster recovery plan scripts for [REDACTED]



[REDACTED] were included in the documentation for the annual disaster recovery exercise, although from the available documentation we could not determine if the scripts were used during the exercises or if the results were reviewed. We found that the other [REDACTED] systems were not included in the annual disaster recovery testing.

**Problems Identified with Communication Channels for Essential Personnel.**

SEC COOP Program documents indicated to ensure communication channels are clear and available during an event, essential personnel are to be issued [REDACTED] elevated communication cards: [REDACTED]

We found that [REDACTED] essential personnel do not have [REDACTED] cards, and that [REDACTED] essential personnel do not have [REDACTED] cards. We also found that [REDACTED] Commission [REDACTED] users were not identified as essential personnel, and [REDACTED] users were not in the SEC Directory indicating that they may no longer be with the SEC.

**Pandemic Plan Testing Is Not Conducted Regularly.** We also found that the last SEC Pandemic Flu Exercise was conducted in September, October, and November of 2007. Further, the Pandemic Flu exercises did not include remote access testing and was only a paper questionnaire analysis. Pandemic plans should be tested regularly and remain relevant to the scope and complexity of the organization's operations.

**Recommendation 18:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should ensure that the agency's disaster recovery testing includes the Commission's mission essential and Federal Information Security Management Act reportable systems and pandemic plan testing is conducted on a regular basis.

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

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

**Recommendation 19:**

The Office of Information Technology (OIT) should determine aspects of continuity of operations disaster recovery and business continuity plan testing that should be conducted annually for regional offices and for Federal Information Security Management Act reportable systems based upon their security categorization. OIT should ensure that this testing includes the recovery phase and the reconstitution phase, as well as a restoration from [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.

**Recommendation 20:**

The Office of Information Technology should add elements to contracts and service level agreements for externally hosted systems to provide appropriate methods by which the Securities and Exchange Commission (SEC) can obtain assurance that appropriate disaster recovery plan testing is performed on mission essential and Federal Information Security Management Act reportable systems and to ensure the systems are able to function during unscheduled events. Such measures may include SEC participation in the disaster recovery plan testing for the externally hosted systems and/or a review of the results of such testing.

**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 21:**

The Office of Information Technology should include elements of testing from an alternate site in the regional office continuity of operations program, disaster recovery, and business continuity plan testing on a periodic basis to ensure the necessary capability and functionality for regional office activities are in place.

**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 22:**

The Office of Freedom of Information Act, Records Management and Security and the Office of Information Technology should include designated essential personnel for systems, divisions/offices, and regional offices in COOP and disaster recovery testing to ensure that a trained workforce is available to support the SEC's mission critical functions following a disaster.

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

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

**Recommendation 23:**

The Office of Information Technology should ensure that system specific scripts and test scenarios are included in the disaster recovery and business continuity plan testing activities to provide assurance of system functionality at alternate locations.

**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 24:**

The Office of Freedom of Information Act, Records Management, and Security (OFRMS) and the Office of Information Technology (OIT) should reassess the definition of essential personnel to ensure that this designation includes only personnel whose services are needed during an event to establish mission essential system connectivity and conduct essential activities until normal operations are resumed. OFRMS and OIT should also develop policies and procedures to ensure that elevated communication cards are distributed only to necessary personnel, cards are disabled upon an employee's departure from the agency, and all essential personnel have appropriate elevated communication cards.

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

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

## **Finding 7: Alternate Work Locations Need to Be Realistic, Maintained in a Ready State, and Communicated to Staff**

It may be difficult for [REDACTED] [REDACTED] In addition, eight regional offices have not specified alternate locations in their COOP supplements. Further, alternate work locations must be ready for access and use as required and staff need to be provided with more information about their alternative work site.

### **Realistic Alternate Work Locations Need to Be Selected, Kept Ready in the Event They Are Needed, and Better Communicated to Staff**

As part of continuity planning, all agencies must identify alternate facilities; alternate uses for existing facilities; and, as appropriate, virtual office options including telework. Risk assessments should be conducted on these facilities to provide reliable and comprehensive data to inform risk mitigation decisions that will allow agencies to protect assets, systems, networks, and functions while determining the likely causes and impacts of any disruption. All agency personnel shall be briefed on agency continuity plans that involve using, or relocating personnel to, alternate facilities, existing facilities, or virtual offices. Continuity personnel must be provided with supplemental training and guidance on relocation procedures.<sup>90</sup>

We found that eight regional offices [REDACTED] [REDACTED] have not identified alternate facilities (whether physical or telecommuting) in their COOP supplements or DRPs. Additionally, while the SEC's draft overall COOP plan identifies alternate worksites for essential personnel, there are no designated alternate worksite locations (whether physical or telecommuting) for [REDACTED] [REDACTED] personnel and non-essential [REDACTED] personnel. Further, the

---

<sup>90</sup> *Federal Continuity Directive 1 (FCD 1)*, February 2008, page 8.

COOP supplements and DRPs do not include all alternate site and travel logistics for the regional offices, [REDACTED] personnel, and non-essential [REDACTED] personnel.<sup>91</sup>

FCD 1 further provides, at Annex K, that an agency's test program must include, among other things, "[t]esting and validating equipment to ensure the internal and external interoperability and viability of communications systems, through monthly testing of the continuity communications capabilities outlined in Annex H (e.g., secure and nonsecure voice and data communications)."<sup>92</sup> We found that the immediate alternate site for the [REDACTED] [REDACTED] has outdated equipment that is locked [REDACTED] [REDACTED] has not been connected to SEC's network for quite some time.

Depending on the circumstances of an emergency event, SEC essential functions will be relocated to the one of three alternate work locations: [REDACTED]

[REDACTED] Traffic to the [REDACTED] from the Headquarters location in Washington, D.C., during an unscheduled event could become extremely difficult, making it unlikely that these destinations could be reached within [REDACTED] (which the BIAs for many systems indicates the desirable time frame after an event for systems to become operational).<sup>93</sup>

**Alternate Work Sites Are Not Sufficiently Ready.** The SEC must be prepared to address events that could disrupt Headquarters operations with a flexible and scalable response. Although it is not possible to anticipate all scenarios that would put the SEC Headquarters at risk; the SEC [REDACTED] [REDACTED]—which supports overall SEC COOP planning—should ensure a coordinated response to most scenarios. While the SEC COOP Plan addresses a wide variety of potentially disruptive scenarios, the [REDACTED] [REDACTED] focuses on catastrophic and/or widespread incidents and events that may occur—with or without warning—and render Headquarters personnel incapable of or unavailable to perform essential functions. The [REDACTED] [REDACTED] notes that the Headquarters division/office points of contacts shall, at a minimum, annually review personnel and resources at the devolution sites to ensure their ability to assume devolution responsibilities.

<sup>91</sup> As noted above, we found that the draft overall COOP plan, has limited discussion on teleworking and does not adequately address telework options (in lieu of alternate worksites) as part of the COOP process.

<sup>92</sup> *Federal Continuity Directive 1 (FCD 1)*, February 2008, Appendix K, page K-1.

During our review, we were informed that the SEC's devolution sites, [REDACTED] were not up-to-date. In particular, we learned that the equipment available at these sites was out-of-date and could not be used with the SEC network due to [REDACTED]. Further, the SEC's COOP plan indicates that there are [REDACTED] workstations/work areas available at the [REDACTED] where emergency response personnel are to relocate in the event of an emergency. However, we were provided with updated space availability information as of January 2012, which indicated there are a total of [REDACTED] in the entire building. The COOP plan documentation on space availability needs to be revised to reflect current space availability and needs, taking into account the potential for telework and remote access.

**Updated Accessibility to Alternate Work Sites.** Alternate work sites require pre-arranged activities, including lists of who can access the site, what equipment can remain at the premises, communication and connectivity information, and office furniture. Access to the [REDACTED] security system. Through discussions with SEC personnel, we learned that in order for SEC personnel to gain access to the [REDACTED] they must be cleared and on the access list maintained at the [REDACTED] site. We were further informed that the access list for SEC personnel is not current due to the transition in COOP personnel and COOP responsibilities.

**Access Problems Identified During Prearranged Visit to the [REDACTED]** In December 2011, TWM conducted a prearranged visit to [REDACTED]. During this visit, TWM found that assigned SEC personnel could not readily access the [REDACTED] because their access codes had expired. For example, we observed that the access code for one SEC staff member had expired. Further, we learned that two other staff members had to have their access codes reset because they had expired. This occurs when a person does not visit the facility on at least a quarterly basis. We also found that the process for resetting expired access codes required communication with the [REDACTED] point-of-contact and the SEC's point-of-contact, who, at that time happened to be on site. Expired codes could prove to be a problem if an actual event occurs and the necessary points of contact are not on site.

**Survey Responses Indicate Staff Need to Be Provided with More Information About Their Alternate Work Locations.** In our SEC agency-wide survey, we questioned SEC employees and contractors regarding their preparation and readiness for COOP activities, including notification of events and alternate work locations.

The survey results revealed that 174 of 2,386 (7.3 percent) respondents indicated they did not know the method by which they would be notified of an

event. Three of those 174 respondents were self-identified essential personnel. These responses raise concerns that some SEC personnel, including essential personnel, will not be notified of events because the SEC's primary method of notifying employees of an unscheduled event is the [REDACTED] which requires self-registration.

Our survey further found that 100 of 417 (24 percent) of respondents who indicated they were required to work from an alternate worksite in the event of a interruption, did not know the location of their alternate worksite. In addition, 294 of 417 (70.5 percent) respondents did not know whether their families could travel with them to the alternate work site. Further, in answering questions specifically pertaining to regional office alternate worksite locations, 57 of 210 (27.1 percent) respondents indicated that they did not know their alternate worksite locations, and two respondents, in the comment portion of the survey, identified their alternate worksite location as the public library. In addition, 2 of 32 (6.3 percent) regional office essential personnel who responded) indicated that they did not have an alternate work site location.<sup>94</sup>

**Recommendation 25:**

The Office of Freedom of Information Act, Records Management, and Security, in conjunction with the regional offices, should specify alternate work locations for which the necessary logistics, such as memoranda of agreement, service level agreements, or credit card limits for hotel conference rooms or other locations, are arranged in advance.

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

**OIG Analysis.** We are pleased that OFRMS concurred with this recommendation.

---

<sup>94</sup> Some regional office respondents indicated they would use another non-SEC federal government location, but the details were not formalized. Our review of SEC COOP plan documents revealed that there were no regional office Memoranda of Agreement, Memoranda of Understanding or Service Level Agreements to ensure that a viable location for regional office alternate worksites would be available during an unscheduled event. See Finding 10 below.

**Recommendation 26:**

The Office of Freedom of Information Act, Records Management, and Security should categorize essential personnel according to necessary functions, based on various realistic scenarios (such as Headquarters or Operations Center locations becoming inaccessible or not operational, including traffic conditions that would affect the scenario). Possible categories include personnel required for immediate activities, personnel needed to establish connections at the alternate site, and personnel needed to work remotely at designated alternate sites such as their homes, hotels, or other specified locations.

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

**OIG Analysis.** We are pleased that OFRMS concurred with this recommendation.

**Recommendation 27:**

The Office of Freedom of Information Act, Records Management, and Security, as part of its planning efforts, should specify when Commission personnel are to telework after an event and when they must go to the designated alternate locations instead of teleworking.

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

**OIG Analysis.** We are pleased that OFRMS concurred with this recommendation.

**Recommendation 28:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should define migration paths from the [REDACTED] should it become inaccessible and specify where the alternate worksite [REDACTED]  
[REDACTED]

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

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



**Recommendation 29:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology, should ensure that the designated Headquarters alternate worksites are ready for use and contain sufficient equipment and technology resources. In addition, COOP plan documentation should be revised to reflect current space availability and needs, taking into account the potential for telework and remote access.

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

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

**Recommendation 30:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should ensure that designated alternate worksite locations are visited and tested periodically to ensure ready access and use. Appropriate steps should be taken to ensure that any cards or badges required for entry to alternate worksite locations are kept up to date and have not expired.

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

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

**Recommendation 31:**

The Office of Information Technology (OIT) should reinforce the need for Securities and Exchange Commission (SEC) personnel and contractors to register in the agency's emergency notification system, which is designated as the primary method of notifying employees during a continuity of operations or pandemic event. OIT should also implement procedures to ensure the removal of personnel from the emergency notification system after they leave the SEC.

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

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

**Recommendation 32:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should clearly define in the continuity of operations, disaster recovery, and business continuity plan documentation the alternate worksite or telework locations for both essential and non-essential personnel. This documentation should also clarify whether, when relocating to an alternate site is required, family members may accompany Commission employees and contractors to the relocation site, consistent with federal regulations.

**Management Comments.** OFRMS and OIT concurred with this recommendation. See Appendix VII for management’s full comments.

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

## **Finding 8: Plans of Action and Milestones (POA&M) Need to Be Complete and Up-to-Date**

While the SEC’s COOP and disaster recovery plan test reports list identified issues, areas for improvement, and recommended corrective actions; the identified issues and recommendations were not included in POA&Ms. Also, the regional office POA&Ms have not been updated.

### **SEC POA&M Maintenance Needs to Be Improved**

As stated in the NIST Special Publication 800-53, POA&M “are developed and maintained for the program management and common controls that are deemed through assessment to be less than effective.”<sup>95</sup> The POA&M “is a key document in the security authorization package and is subject to federal reporting requirements established by OMB.”<sup>96</sup>

The SEC performs DRP testing for each regional office infrastructure and individual system applications. All the regional office’s DRPs state that POA&Ms

---

<sup>95</sup> NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, Appendix G, page G-1,

<sup>96</sup> NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, Appendix F-CA, page F-35.

will be created. Our review found 39.5 percent of the recommendations generated during the regional office DRP testing could not be tracked to POA&M and were not identified as having been resolved in the updated DRPs (dates ranging from 2010 to 2011). Further, we found that at least two items identified in the annual Headquarters COOP testing that should have been included as POA&M items (submission of filings gap during testing of [REDACTED], and order of startup for production servers on Business Objective 11 system).

**Regional Office POA&Ms Are Not Updated.** We also found that eight regional offices [REDACTED] have not updated their DRPs to include recommendations that were identified in DRP testing. Specific items of issue or concern listed in the regional office disaster recovery test plans and evaluation reports included, among other things, required server migration and the need for updated Tips, Complaints, and Referrals system DRPs. The issues that were identified in the testing have not been addressed in a post-exercise activity or included as POA&Ms. While corrective actions were noted that would require a POA&M, none was present. All recommendations generated during COOP, DRP, BCP and pandemic testing should be included in the POA&M. Otherwise, recommendations could go unresolved and encumber the recovery of a system during an event.

**Regional POA&Ms Were Not Properly Closed Out.** Further, we found that all the SEC's regional office's POA&M items that were shown to be open should reflect a status of closed, according to information provided to the TWM. An issue identified in an April 2010 exercise conducted by one regional office was the need to update the POA&M process specifically to include actions required to correct any problems or issues identified during the April 2010 exercise. There were also several open POA&M items from the December 2008 and June 2009 disaster recovery exercises that required evaluation by management to ensure final corrective actions are implemented.

**Recommendation 33:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should ensure that recommendations made as a result of the continuity of operations, disaster recovery, business continuity and pandemic testing are included in a management corrective action plan (CAP) and is maintained in the CAP until it is resolved.

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

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

**Recommendation 34:**

The Office of Information Technology (OIT) should ensure that open POA&M items from previous years are evaluated by management and final corrective actions are implemented to close the items.

**Management Comments.** OIT and OFRMS concurred with this recommendation. See Appendix VII for management’s full comments.

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

## **Finding 9: Additional Training and Cross-Training of COOP Personnel is Required**

The SEC’s COOP and disaster recovery exercises do not include the majority of the designated essential personnel. In addition the high concentration of personnel at SEC Headquarters may not provide for adequate geographic dispersion of trained personnel.

### **SEC COOP-Related Training and Cross-Training Need to Be Improved**

The Contingency Planning Guide for Federal Information Systems provides as follows: “Training for personnel with contingency plan responsibilities should focus on familiarizing them with ISCP roles and teaching skills necessary to accomplish those roles. This approach helps ensure that staff is prepared to participate in tests and exercises as well as actual outage events. Training should be provided at least annually.”<sup>97</sup>

SEC division and office heads select essential personnel based upon the following factors: (1) the predetermined essential functions that must be performed, regardless of the operational status of the SEC’s primary operating facility, (2) the staff members’ knowledge and expertise in performing these

---

<sup>97</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 28. Under NIST SP 800-53, an organization should incorporate simulated events into contingency training to facilitate effective response by personnel during crisis situations. NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, May 2010, Appendix F-CP, page F-48.

essential functions, and (3) the members' ability to rapidly deploy to the relocation site in an emergency situation. The SEC has designated [REDACTED] individuals as essential personnel.

As discussed above, the SEC has chosen to eliminate the BCP, indicating that its elements are already contained in the DRP and BIAs. As a consequence, the SEC's DRP exercises are primarily viewed as information technology exercises. As training and exercises cover the same topics, the SEC uses exercises to satisfy the training requirement in an effort to reduce the number of hours devoted to these activities.<sup>98</sup> The SEC is using the participation in regional office DRP exercises to satisfy the requirement to train essential personnel both for the COOP plan and the DRP. As noted above, we found through testing that on average, 88 percent of regional office essential personnel did not participate in DRP training or exercises between 2008 and 2011. This indicates that a large percentage of regional office essential personnel may not have been sufficiently trained in their roles and responsibilities during a disaster recovery event. As a consequence, essential personnel may not be able to perform their responsibilities during the activation of the DRP.

We also reviewed individual system disaster recovery testing by randomly selecting [REDACTED] internally hosted SEC systems. The [REDACTED] systems selected included: [REDACTED]

[REDACTED] We identified 14 Points of Contact (POC) from the DRPs for these systems, and found that 9 POCs had not participated in the DRP testing or training for their systems. Additionally, for COOP testing, we could not verify who had participated in the testing or training based on the available documentation for 2010 and 2011 (i.e., Eagle Horizon test plans, Headquarters computer based training, and related Eagle Horizon testing documents).

While OIT personnel are participating in DRP exercises, many key essential personnel are not participating in DRP exercises and, therefore, have not received the appropriate role-based training for their part in DRP and COOP activities.<sup>99</sup> Instead, they only had the annual refresher online training course. Further, we found that [REDACTED] SEC staff members deployed to the [REDACTED] and were involved in supporting the 2011 Eagle Horizon exercise. The COOP exercises that have been conducted by OFRMS primarily included OIT personnel as the participants, and the testing conducted shows the

<sup>98</sup> "Training provides the skills and familiarizes leadership and staff with the procedures and tasks they must perform in executing continuity plans," while "[t]ests and exercises serve to assess and validate all the components of continuity plans, policies, procedures, systems, and facilities used to respond to and recover from an emergency situation and identify issues for subsequent improvement." *Federal Continuity Directive 1 (FCD 1)*, February 2008, page 10.

<sup>99</sup> Training personnel before an exercise or test event is typically split between a presentation on their roles and responsibilities and activities that allow personnel to demonstrate their understanding of the subject matter. NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006, page ES-2.

ability for the [REDACTED] to exercise the basic failover of the systems. However, the same OIT personnel are being trained and there has not been sufficient testing for events that would require the participation of essential and senior personnel, in addition to system owners.

A key continuity concept identified in FCD 1 is geographic dispersion of an organization's normal daily operations, which "can significantly enhance an organization's resilience and reduce the risk of losing the capability to perform essential functions. Geographic dispersion of leadership, data storage, personnel, and other capabilities may be essential to the performance of essential functions following a catastrophic event and will enable operational continuity during an event that requires social distancing (e.g., pandemic influenza)."<sup>100</sup>

We estimated that based on the distribution of SEC personnel throughout the country (applying a 40 percent anticipated absenteeism rate<sup>101</sup> to [REDACTED] SEC personnel listed as required to take the annual online COOP training for 2011), there would be [REDACTED] potentially absent personnel. We estimated that [REDACTED] would be absent from the geographically dispersed regional offices, while the remaining [REDACTED] would be absent from the D.C. metropolitan area where the SEC's Headquarters is located. It seems likely that there is sufficient geographic dispersion of personnel and functions among the SEC regional offices, which perform similar activities. However, the high concentration of personnel at the Headquarters location may not provide for adequate geographic dispersion of trained personnel, such that additional cross-training of personnel may be warranted.

### **Recommendation 35:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should ensure that continuity of operations, disaster recovery, and business continuity plan training occur prior to annual tests exercises or events as recommended by NIST Special Publication 800-84, Guide to Test, Training, and Exercise Programs for Information Technology Plans and Capabilities, in order to ensure that individuals are prepared for their specific roles during a disaster recovery event.

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

---

<sup>100</sup> *Federal Continuity Directive 1 (FCD1)*, February 2008, page 4

<sup>101</sup> In a severe pandemic, absenteeism may reach 40 percent during the peak weeks of a community outbreak. *Interagency Statement on Pandemic Planning*, page 6.

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

**Recommendation 36:**

The Office of Freedom of Information Act, Records Management, and Security, in conjunction with the Office of Human Resources, the Office of Information Technology, and the various divisions and offices, should consider, consistent with federal personnel regulations, if there is the ability to cross-train regional office personnel in functions that are performed exclusively at the Commission Headquarters and regional offices and, if so, should define these functions and implement procedures for cross-training personnel for mission essential functions in the case of a COOP or pandemic event.

**Management Comments.** OFRMS and OIT concurred with this recommendation. See Appendix VII for management’s full comments.

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

## **Finding 10: Necessary Memoranda Of Agreement, Memoranda Of Understanding, and Service-Level Agreements Were Not Present or Are Outdated**

The SEC does not have current Memoranda of Agreement (MOA), Memoranda of Understanding (MOU), or Service-Level Agreements (SLA) that are typically included as appendices to agency COOP or DRP plans so they are easily accessible during an event.

### **Alternate Worksite MOU/MOA/SLA Were Not Present or Are Out-of-Date**

The use of formal alternate worksite locations at other federal agencies or private entities often requires the use of MOUs/MOA or SLAs. For example, “[t]wo or more organizations with similar or identical system configurations and [REDACTED] technologies may enter into a formal agreement to serve as alternate sites for each other or enter into a joint contract for an alternate site. This type of site is set up via a reciprocal agreement or [MOU].”<sup>102</sup> However, “[a] reciprocal

---

<sup>102</sup> NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, page 23.

agreement should be entered into carefully because each site must be able to support the other, in addition to its own workload, in the event of a disaster. This type of agreement requires the recovery sequence for the systems from both organizations to be prioritized from a joint perspective, favorable to both parties. Testing should be conducted at the partnering sites to evaluate the extra processing thresholds, compatible system and [REDACTED] configurations, sufficient telecommunications connections, compatible security measures, and the sensitivity of data that might be accessible by other privileged users, in addition to functionality of the recovery strategy.”<sup>103</sup>

During our review of the SEC’s COOP documents we did not identify any current (i.e., updated within the last three years) existing MOUs, MOAs or SLAs for alternate worksite locations, vendors, or services to be obtained or used during an event. We identified an outdated MOU (entered into in 2006) with the [REDACTED] [REDACTED] which the SEC no longer uses as an alternate work site. We further found that the outdated [REDACTED] MOU did not list the staff that was to be contacted in a COOP event.

Further, we found that neither the SEC’s overall COOP plan, nor the OIT contingency plan includes contract provisions for obtaining hardware, software, or services for emergencies. Further, the COOP documents we reviewed did not address the use of government purchase cards to obtain needed hardware, software, or services in the event of COOP activation, in lieu of MOUs, MOAs or SLAs. Subsequent to the issuance of the discussion draft report for this review, we obtained and reviewed two random service contracts. While we found appropriate language were in these contracts, we were not provided with enough contracts so that a sample number of the population could be properly test. Therefore, we could not firmly conclude that the required contractual language is contained in similar type contracts.

We also reviewed the regional office base DRP (which is to be augmented by the individual regional offices), as well as the regional offices DRP supplements. We found that none of these plans included any MOUs, MOAs or SLAs. Our review of the regional office base DRP disclosed that the regional offices are to use available equipment from OIT or other regional offices during COOP activation. While this may be a cost effective solution, it can also be inefficient and ineffective because the unutilized equipment contained in the disaster recovery plan hardware inventory lists may not be up-to-date or available. Moreover, it is unlikely that property transfers would be completed properly given that personnel would already taxed with the implementation of a DRP. Further, regional office

[REDACTED]

[REDACTED]



personnel may be reluctant to part with equipment until they are satisfied that the DRP event will not also affect them and they have reviewed their own DRP requirements.

Finally, our review found that OIT's contingency plan did not include MOUs, MOAs or SLAs for externally hosted systems. Rather, the plan merely noted that data communication lines are used to connect to these systems and that they fall under the cognizance of the general support system. Subsequent to the exit meeting, one externally hosted system contract document was obtained and appropriate service level metrics and availability language were included.

**Recommendation 37:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology, in conjunction with the Office of Administrative Services and the Office of the General Counsel, should document that the necessary contractual agreements and/or provisions are in place to ensure the availability of hardware, software, and services that may be required during an emergency. The use of government credit cards to procure such equipment and services should also be considered and documented. If government credit cards are to be used for this purpose, the authorized limits established should be sufficient for such purchases.

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

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

**Recommendation 38:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology, in conjunction with the regional offices, the Office of Administrative Services, the Office of Financial Management, and the Office of the General Counsel, should ensure that an appropriate and updated Memoranda of Agreement, Memoranda of Understanding and Service-Level Agreements are executed to provide for alternate work site locations, capabilities, and accommodations that may be necessary to ensure continuity of operations.

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

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

## Abbreviations

---

[REDACTED]	[REDACTED]
Business Continuity Plan	BCP
Business Impact Analysis	BIA
Chief Operating Officer	COO
Continuity of Operations Program	COOP
[REDACTED]	[REDACTED]
Disaster Recovery Plan	DRP
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
eXtensible Business Reporting Language	XBRL
Federal Continuity Directive	FCD
Federal Information Processing Standard	FIPS
Federal Information Security Management Act	FISMA
[REDACTED]	[REDACTED]
Information System Contingency Plan	ISCP
Information Technology	IT
Information Technology Contingency Plan	ITCP
[REDACTED]	[REDACTED]
Memorandum of Agreement	MOA
Memorandum of Understanding	MOU
Mission Essential Functions	MEF
National Institute of Standards and Technology	NIST
Office of Freedom of Information Act, Records Management and Security	OFRMS
Office of Inspector General	OIG
Office of Security Services	OSS
Plans of Action and Milestones	POA&M
Points of Contact	POC
Primary Mission Essential Function	PMEF
Service Level Agreement	SLA
TWM Associates, Inc.	TWM
U.S. Securities and Exchange Commission	SEC or Commission
Virtual Private Network	VPN
[REDACTED]	[REDACTED]

## List of Issues Identified in Review of Disaster Recovery and Continuity of Operations Plans

---

1. All 13 DRPs (Headquarters, Operations Center, and the regional offices)<sup>105</sup> did not have a review and approval date entered.
2. Ten regional office DRPs [REDACTED] did not include risk management.
3. No regional office DRPs included information for budget and acquisition of resources.
4. Five of 13 DRPs [REDACTED] did not include an order of succession.
5. All 13 DRPs did not include concurrent processing.
6. One regional office [REDACTED] did not include recovery priority.
7. Seven of 13 DRPs [REDACTED] included BIAs that did not appear to be current.
8. Ten of 13 DRPs [REDACTED] did not include access control policies and procedures.
9. Ten of 13 DRPs [REDACTED] did not include all alternate facilities.
10. All 13 DRPs did not include all alternate site use and travel logistics.
11. The regional office's DRPs had template language that lacked complete information.
12. Six of 13 DRPs [REDACTED] contained vital records information that did not appear to be current.
13. Five of 13 DRPs [REDACTED] hard copy vital records without any alternate source.

---

<sup>105</sup> While we found that the [REDACTED] did not specifically have DRPs, for the purposes of this Appendix, the main overall SEC COOP document is considered to be the Headquarters DRP, and the OIT contingency plan (i.e., the GSS ISCP) is considered to be the Operations Center DRP. We also reviewed the regional office base plan and the regional office COOP supplements to determine if they included any of the required information.

14. Eleven of 13 DRPs [REDACTED] did not include original or new site restoration procedures.
15. Three of 13 DRPs [REDACTED] did not include personnel and vendor contact lists.
16. Two of 13 DRPs [REDACTED] had incomplete personnel and vendor contact lists.
17. The regional office's DRPs did not include information on relocation of personnel, relocation of families of personnel, alternate site operating procedures or assumptions.
18. All 13 DRPs did not include MOA, MOUs or SLAs.
19. The overall COOP document and the OIT contingency plan were under revision, as indicated by the water mark of the word documents, the list of essential personnel was under revision, and the plans did not include a list of vendor information for all divisions and offices.
20. The overall COOP document and the OIT contingency plan contained an incomplete order of succession.
21. The recovery procedures in the overall COOP document and the OIT contingency plan's did not include additional notification procedures for more recovery staff, messages and status updates to leadership.
22. The reconstitution procedures in the overall COOP document and the OIT contingency plan did not include procedures for notifications of return to normal operations or a system full [REDACTED]
23. The overall COOP plan document did not include logistics for the Alternate Data Center.
24. Twelve of 13 DRPs [REDACTED] did not include operating system version levels for software inventory, as recommended by NIST SP 800-34.
25. All 13 DRPs did not include processors, memory, storage requirements in equipment inventory, as recommended by NIST SP 800-34.
26. The regional office base DRP's reconstitution phase did not include concurrent processing or offsite data storage return.
27. For all regional office DRPs, the signature pages were not signed or dated, and the DRPs included a large amount of template wording.
28. For 10 of 13 DRPs [REDACTED]

- ██████████ the signature pages did not include the designated Crisis Management Team and/or information technology specialist.
29. All regional office DRPs had incomplete sections, such as a ██████████ that was not updated.
  30. For 8 of 13 DRPs ██████████ the shutdown/startup procedures were a template and did not include all network devices listed in the ██████████
  31. For 10 of 13 DRPs ██████████ Appendix H: Emergency Operation Center Locations had not been completed.
  32. For 8 of the 13 DRPs ██████████ Alternate Enhanced Redirect Solutions-authorized personnel were not included.
  33. For 1 of 13 DRPs ██████████ shutdown/startup procedures was a template with incomplete name and floor fields.
  34. For 8 of 13 DRPs ██████████ the emergency communication policies and procedures were sample procedures and had not been completed.
  35. One of 13 DRPs ██████████ did not reflect the changes identified in the BIA after action report.
  36. Three regional office COOP plan supplements did not provide all, if any, of the required information.
  37. Six regional office COOP spreadsheet supplements ██████████ did not appear to be current.
  38. Contracts or related documentation were not provided to support provisions in the overall COOP plan document reference emergency provisions.
  39. Systems with lower recovery priorities were listed to be recovered before systems with more critical recovery requirements.

# List of Issues Identified From Sample Testing of System Disaster Recovery Plan and Business Impact Analysis Documents

---

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## Scope and Methodology

---

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

**Scope.** The initial scope of TWM's reviewed covered calendar years 2009 through 2011. However, during our review and requests for support documentation, OIT and OSS provided TWM with some data that was dated prior to calendar year 2009. Specifically, we reviewed documentation to support the SEC's COOP that was dated from 2007 through 2011.

We conducted our fieldwork from October 2011 to January 2012.

Further, we obtained information from OIT concerning the SEC's FISMA reportable systems for the universe of the SEC's systems. For each of the identified systems and SEC facilities, we obtained supporting artifacts (i.e., COOP plans, DRPs, BIAs, essential personnel lists, list of [REDACTED] users, list of [REDACTED] users, system log access extracts, etc.) to the extent they were available. We surveyed the Commission's employees and contractors regarding their preparation and readiness for COOP, DRP, BCP, and pandemic activities. We obtained information showing the status of SEC's implementation of prior OIG audit recommendations relevant to COOP and determined there were no additional applicable risk areas or potential findings and recommendations outside of the existing audit program steps for this review. We also observed and visited the [REDACTED]

**Methodology.** To meet the overall objective to assess the adequacy of the SEC's COOP, we reviewed the SEC's policies and procedures governing COOP, DRP, BCP and pandemic activities, documentation showing implementation of those activities, and documents reflecting supporting activities for implementation of these programs. We also reviewed relevant documentation for individual systems, Headquarters divisions and offices, regional offices, as well as the Operations Center and the Alternate Data Center. In addition, we held discussions with personnel to learn about the SEC's COOP and to discuss and confirm our findings and recommendations.

We conducted detailed testing to determine the viability of the SEC's COOP, DRP, BCP, and pandemic functions and whether the Commission is complying with its policies and procedures in these areas. We also performed testing to measure the effectiveness of the implemented procedures.

**Management Controls.** We reviewed the Commission's FISMA POA&M items that document control weaknesses related to COOP, DRP, BCP and pandemic activities to determine the impact on the existing review program procedures for this review.

**Prior Audit Coverage**

- *2011 Annual FISMA Executive Summary Report*, OIG Report No. 501, February 2, 2012
- *Review of Alternative Work Arrangements, Overtime Compensation, and COOP-Related Activities at the SEC*, OIG Report No. Number 491, September 28, 2011
- *Assessment of SEC's Continuous Monitoring Program*, OIG Report No. 497, August 11, 2011
- *2010 Annual FISMA Executive Summary Report*, OIG Report No. 489, March 3, 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 provide or managed by another agency, contractor, or other source.

**OMB Memorandum 11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, September 14, 2011.** Provides instructions to agencies for meeting Fiscal Year 2011 reporting requirements under FISMA.

**NIST Special Publication 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems, May 2010.** Provides instructions, recommendations, and considerations for federal government information system contingency planning.

**NIST Special Publication 800-53, Rev. 3, Recommended Security Controls for Federal Information systems and Organizations, August 2009.** Defines security controls recommended for use by organizations in protecting their information systems that should be employed as part of a well-defined and documented information security program.

**Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements, Issued by the Department of Homeland Security, February 2008.** Provides direction to the federal executive branch for developing continuity plans and programs.

**Federal Continuity Directive 2 (FCD 2), Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process, February 2008.** Implements the requirements of FCD 1, Annex C, and provides guidance and direction to federal executive branch departments and agencies for identification of their MEFs and potential PMEFS.

**National Strategy for Pandemic Influenza Implementation Plan, Issued by the Homeland security Council, May 2006.** Provides a high-level overview of the approach that the federal government will take to prepare for and respond to a pandemic.

**Interagency statement on Pandemic Planning, Issued by the Federal Financial Institutions Examination Executive Council Agencies.** Provides guidance to remind financial institutions that BCPs should address the threat of a pandemic influenza outbreak.

**SEC OIT Operating Directive 24-04.09 (02.0), IT Security Business Continuity Management Program, August 23, 2011.** Establishes policy and responsibilities for business continuity management consistent with requirements prescribed by FISMA and the SEC's Information Technology Security Program.

**SEC OIT Implementing Instruction 24-04.09.01 (02.0), Business Impact Analysis, August 22, 2011.** Defines the SEC's process and establishes responsibilities for conducting a BIA as directed in Operation Directive 24-04.09.

**SEC OIT Disaster Recovery Planning Policy, OIT-00003-001.0, August 6, 2002.** Maintains the OIT DRP for its infrastructure at the SEC's Operations Center, Headquarters, and regional offices.

## List of Recommendations

---

### **Recommendation 1:**

The Office of the Chief Operating Officer should ensure that the Office of Freedom of Information Act, Records Management and Security completes its review of the agency-wide continuity of operations program (COOP) to ensure the Commission's COOP is comprehensive, cohesive, and in compliance with federal guidance.

### **Recommendation 2:**

The Office of Freedom of Information Act, Records Management, and Security should revise and update the Commission's continuity of operations program policies and procedures to ensure they are comprehensive, complete, and up-to-date.

### **Recommendation 3:**

The Office of Freedom of Information Act, Records Management, and Security (OFRMS) and Office of Information Technology (OIT), in conjunction with the program divisions/offices and regional offices, should update, revise and finalize all continuity of operations program (COOP) documents, including the overall Headquarters COOP plan, individual division/office COOP plans, regional office COOP supplements, disaster recovery plans, business continuity plans and business impact analyses, and pandemic plans supplements. OFRMS and OIT should ensure these documents are complete and include all the necessary elements, and that they properly define the Commission's essential functions. In addition, processes should be implemented to ensure annual review and approval of these documents.

### **Recommendation 4:**

The Office of Freedom of Information Act, Records Management, and Security, in conjunction with program and regional offices, should ensure that vital records and lines of succession are properly identified, documented and readily available during continuity events.

**Recommendation 5:**

The Office of Information Technology (OIT), in conjunction with the primary program information users, should identify [REDACTED] at the alternate locations should [REDACTED] be unavailable. Further, OIT should review the Securities and Exchange Commission's (SEC) network and topology to ensure there are [REDACTED]

**Recommendation 6:**

The Office of Information Technology should ensure proper power distribution [REDACTED]

**Recommendation 7:**

The Office of Freedom of Information Act, Records Management, and Security, in conjunction with the Office of Information Technology and system owners, should revise the Securities and Exchange Commission (SEC) system recovery time objectives to specify more realistic timeframes, based on the ability to transition to the alternate site, and then determine acceptable recovery times. The recovery plan and priority of recovery of the systems should be based on the overall mission of the agency with a focus on real-time monitoring of the markets. Further, the identification of high priority systems should focus on the immediate mission of the agency, and systems documentation should also be reviewed to ensure proper recovery priority is reflected based on the contribution to the SEC's mission and functions.

**Recommendation 8:**

For underutilized systems such as the [REDACTED] [REDACTED] the Office of Information Technology should consider discontinuing maintenance, retiring the system, or alternatively making more robust use of the system such that additional Commission funds are not wasted on underutilized systems.

**Recommendation 9:**

The Office of Information Technology (OIT), in conjunction with system owners, should identify the [REDACTED] requirements (e.g., files, data, and system software) for all systems (at minimum, Federal Information Security Management Act reportable systems). OIT should ensure that [REDACTED] requirements are documented, understood by the owner, and published for future reference. Further, OIT should ensure system software licenses and key requirements are included in [REDACTED] documentation, and the location of this information is known to ensure restoration capability at the alternate location site.

**Recommendation 10:**

The Office of Information Technology, in conjunction with the regional offices, should document the processes and procedures to be used in the event that a regional office needs to restore its systems at a regional office transition site, and the corresponding effect on the [REDACTED] procedures for other regional offices that may need to use a regional office transition site or alternate method to ensure recoverability.

**Recommendation 11:**

The Office of Information Technology (OIT) should continue its efforts to replace the regional office's tape [REDACTED] systems. Additionally, OIT should define a [REDACTED] and recovery strategy for multi-hosted application restoration for the regional offices. OIT should also document the system specific files and database items, in order to facilitate the ability to restore only necessary items, rather than the entire database, which could take many hours to accomplish and is not in line with the recovery time objectives for individual systems.

**Recommendation 12:**

The Office of Information Technology should implement consistent and appropriate [REDACTED] schedules for mission essential and Federal Information System Management Act reportable systems, including daily, weekly, and monthly [REDACTED] processes and procedures, to ensure these systems are recoverable.



**Recommendation 13:**

The Office of Information Technology should include in the Disaster Recovery Plan and Business Continuity Plan, testing steps that are designed to ensure the restoration from [REDACTED] that is consistent with the requirements for systems that are rated as moderate, in accordance with the National Institute of Standards and Technology guidance under the Federal Information Systems Management Act.

**Recommendation 14:**

The Office of Information Technology should ensure that remote access testing is included as part of all Continuity of Operations Program, disaster recovery and pandemic testing activities, including those performed in the regional offices, to ensure that essential personnel and a sample of the representative users of the system are able to function remotely during an unscheduled event.

**Recommendation 15:**

The Office of Information Technology (OIT), in consultation with the Office of Freedom of Information Act, Records Management and Security (OFRMS), should require semiannual testing of remote access devices to ensure up-to-date connectivity and ability for both essential personnel and non-essential personnel to access the Commission's network. In addition, OIT and OFRMS should implement a system notification warning prior to the connectivity testing date and then disable those devices that are not updated.

**Recommendation 16:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should consider implementation of alternate remote access solutions and/or internal directory structure [REDACTED]

[REDACTED] and Federal Information Security Management Act reportable systems.

**Recommendation 17:**

The Office of Freedom of Information Act, Records Management and Security and the Office of Information Technology should update the Continuity of Operations Program (COOP) documents and necessary agreements to appropriately reflect authorized telework activities by Commission personnel during unscheduled events under the COOP, disaster recovery and pandemic plans, including equipment that will be used for teleworking in such circumstances.

**Recommendation 18:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should ensure that the agency's disaster recovery testing includes the Commissions mission essential and Federal Information Security Management Act reportable systems and pandemic plan testing is conducted on a regular basis.

**Recommendation 19:**

The Office of Information Technology (OIT) should determine aspects of continuity of operations disaster recovery and business continuity plan testing that should be conducted annually for regional offices and for Federal Information Security Management Act reportable systems based upon their security categorization. OIT should ensure that this testing includes the recovery phase and the reconstitution phase, as well as a restoration from [REDACTED]

**Recommendation 20:**

The Office of Information Technology should add elements to contracts and service level agreements for externally hosted systems to provide appropriate methods by which the Securities and Exchange Commission (SEC) can obtain assurance that appropriate disaster recovery plan testing is performed on mission essential and Federal Information Security Management Act reportable systems and to ensure the systems are able to function during unscheduled events. Such measures may include SEC participation in the disaster recovery plan testing for the externally hosted systems and/or a review of the results of such testing.

**Recommendation 21:**

The Office of Information Technology should include elements of testing from an alternate site in the regional office continuity of operations program, disaster recovery, and business continuity plan testing on a periodic basis to ensure the necessary capability and functionality for regional office activities are in place.

**Recommendation 22:**

The Office of Freedom of Information Act, Records Management and Security and the Office of Information Technology should include designated essential personnel for systems, divisions/offices, and regional offices in COOP and disaster recovery testing to ensure that a trained workforce is available to support the SEC's mission critical functions following a disaster.

**Recommendation 23:**

The Office of Information Technology should ensure that system specific scripts and test scenarios are included in the disaster recovery and business continuity plan testing activities to provide assurance of system functionality at alternate locations.

**Recommendation 24:**

The Office of Freedom of Information Act, Records Management, and Security (OFRMS) and the Office of Information Technology (OIT) should reassess the definition of essential personnel to ensure that this designation includes only personnel whose services are needed during an event to establish mission essential system connectivity and conduct essential activities until normal operations are resumed. OFRMS and OIT should also develop policies and procedures to ensure that elevated communication cards are distributed only to necessary personnel, cards are disabled upon an employee's departure from the agency, and all essential personnel have appropriate elevated communication cards.

**Recommendation 25:**

The Office of Freedom of Information Act, Records Management, and Security, in conjunction with the regional offices, should specify alternate work locations for which the necessary logistics, such as memoranda of agreement, service level agreements, or credit card limits for hotel conference rooms or other locations, are arranged in advance.

**Recommendation 26:**

The Office of Freedom of Information Act, Records Management, and Security should categorize essential personnel according to necessary functions, based on various realistic scenarios (such as Headquarters or Operations Center locations becoming inaccessible or not operational, including traffic conditions that would affect the scenario). Possible categories include personnel required for immediate activities, personnel needed to establish connections at the alternate site, and personnel needed to work remotely at designated alternate sites such as their homes, hotels, or other specified locations.

**Recommendation 27:**

The Office of Freedom of Information Act, Records Management, and Security, as part of its planning efforts, should specify when Commission personnel are to telework after an event and when they must go to the designated alternate locations instead of teleworking.

**Recommendation 28:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should define migration paths from the [REDACTED] should it become inaccessible and specify where the alternate worksite locations for the [REDACTED] [REDACTED]

**Recommendation 29:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology, should ensure that the designated Headquarters alternate worksites are ready for use and contain sufficient equipment and technology resources. In addition, COOP plan documentation should be revised to reflect current space availability and needs, taking into account the potential for telework and remote access.

**Recommendation 30:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should ensure that designated alternate worksite locations are visited and tested periodically to ensure ready access and use. Appropriate steps should be taken to ensure that any cards or badges required for entry to alternate worksite locations are kept up to date and have not expired.

**Recommendation 31:**

The Office of Information Technology (OIT) should reinforce the need for Securities and Exchange Commission (SEC) personnel and contractors to register in the agency's emergency notification system, which is designated as the primary method of notifying employees during a continuity of operations or pandemic event. OIT should also implement procedures to ensure the removal of personnel from the emergency notification system after they leave the SEC.

**Recommendation 32:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should clearly define in the continuity of operations, disaster recovery, and business continuity plan documentation the alternate worksite or telework locations for both essential and non-essential personnel. This documentation should also clarify whether, when relocating to an alternate site is required, family members may accompany Commission employees and contractors to the relocation site, consistent with federal regulations.

**Recommendation 33:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should ensure that recommendations made as a result of the continuity of operations, disaster recovery, business continuity and pandemic testing are included in a management corrective action plan (CAP) and is maintained in the CAP until it is resolved.

**Recommendation 34:**

The Office of Information Technology (OIT) should ensure that open POA&M items from previous years are evaluated by management and final corrective actions are implemented to close the items.

**Recommendation 35:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology should ensure that continuity of operations, disaster recovery, and business continuity plan training occur prior to annual tests exercises or events as recommended by NIST Special Publication 800-84, Guide to Test, Training, and Exercise Programs for Information Technology Plans and Capabilities, in order to ensure that individuals are prepared for their specific roles during a disaster recovery event.

**Recommendation 36:**

The Office of Freedom of Information Act, Records Management, and Security, in conjunction with the Office of Human Resources, the Office of Information Technology, and the various divisions and offices, should consider, consistent with federal personnel regulations, if there is the ability to cross-train regional office personnel in functions that are performed exclusively at the Commission Headquarters and regional offices and, if so, should define these functions and implement procedures for cross-training personnel for mission essential functions in the case of a COOP or pandemic event.

**Recommendation 37:**

The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology, in conjunction with the Office of Administrative Services and the Office of the General Counsel, should document that the necessary contractual agreements and/or provisions are in place to ensure the availability of hardware, software, and services that may be required during an emergency. The use of government credit cards to procure such equipment and services should also be considered and documented. If government credit cards are to be used for this purpose, the authorized limits established should be sufficient for such purchases.

**Recommendation 38:**


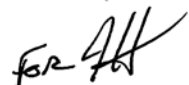
The Office of Freedom of Information Act, Records Management, and Security and the Office of Information Technology, in conjunction with the regional offices, the Office of Administrative Services, the Office of Financial Management, and the Office of the General Counsel, should ensure that an appropriate and updated Memoranda of Agreement, Memoranda of Understanding and Service-Level Agreements are executed to provide for alternate work site locations, capabilities, and accommodations that may be necessary to ensure continuity of operations.

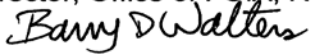
# Management Comments

---

## MEMORANDUM

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

**THRU:** Jeff Heslop, Chief Operating Officer  ↔ 

**FROM:** Thomas A. Bayer, Director, Office of Information Technology (OIT)  
Barry D. Walters, Director, Office of FOIA, Records Management, and Security (OFRMS) 

**RE:** *Review of SEC's Continuity of Operations Program*, Report No. 502 (Draft)

**DATE:** April 12, 2012

This memorandum is in response to the Office of Inspector General's (OIG) Draft Report No. 502, titled *Review of the SEC's Continuity of Operations Program*. Thank you for the opportunity to review and respond to this report. We concur with all recommendations and will implement them as resources permit.

### Recommendation 1.

The Office of the Chief Operating Officer should ensure that the OFRMS completes its review of the agency-wide COOP to ensure the Commission's COOP is comprehensive, cohesive, and in compliance with federal guidance.

*OFRMS concurs with this recommendation.*

### Recommendation 2.

OFRMS should revise and update the Commission's continuity of operations program policies and procedures to ensure they are comprehensive, complete, and up-to-date.

*OFRMS concurs with this recommendation.*

### Recommendation 3.

OFRMS and OIT, in conjunction with the program divisions/offices and regional offices, should update, revise and finalize all COOP documents, including the overall Headquarters COOP plan, individual division/office COOP plans, regional office COOP supplements, disaster recovery plans, business continuity plans and business impact analyses, and pandemic plans supplements. OFRMS and OIT should ensure these

documents are complete and include all the necessary elements, and that they properly define the Commission's essential functions. In addition, processes should be implemented to ensure annual review and approval of these documents.

*OIT and OFRMS concur with this recommendation.*

**Recommendation 4**

OFRMS, in conjunction with program and regional offices, should ensure that vital records and lines of succession are properly identified, documented and readily available during continuity events.

*OFRMS concurs with this recommendation.*

**Recommendation 5**

OIT, in conjunction with the primary program information users, should identify [REDACTED] at the alternate locations should [REDACTED] be unavailable. Further, OIT should review the SEC's network and topology to ensure there are [REDACTED]

*OIT concurs with this recommendation.*

**Recommendation 6**

OIT should ensure proper power distribution throughout the [REDACTED]

*OIT concurs with this recommendation.*

**Recommendation 7**

OFRMS, in conjunction with the working with OIT and system owners, should revise the SEC system recovery time objectives to specify more realistic timeframes, based on the ability to transition to the alternate site, and then determine acceptable recovery times. The recovery plan and priority of recovery of the systems should be based on the overall mission of the agency with a focus on real-time monitoring of the markets. Further, the identification of high priority systems should focus on the immediate mission of the agency, and systems documentation should also be reviewed to ensure proper recovery priority is reflected based on the contribution to the SEC's mission and functions.

*OIT and OFRMS concur with this recommendation.*

**Recommendation 8**

For underutilized systems such as the [REDACTED] the Office of Information Technology should consider discontinuing maintenance, retiring



the system, or alternatively making more robust use of the system such that additional Commission funds are not wasted on underutilized systems.

*OIT concurs with this recommendation.*

**Recommendation 9**

OIT, in conjunction with system owners, should identify the [REDACTED] requirements (e.g., files, data, and system software) for all systems (at minimum, Federal Information Security Management Act reportable systems). OIT should ensure that [REDACTED] requirements are documented, understood by the owner, and published for future reference. Further, OIT should ensure system software licenses and key requirements are included in [REDACTED] documentation, and the location of this information is known to ensure restoration capability at the alternate location site.

*OIT concurs with this recommendation.*

**Recommendation 10**

OIT, in conjunction with the regional offices, should document the processes and procedures to be used in the event that a regional office needs to restore its systems at a regional office transition site, and the corresponding effect on the [REDACTED] procedures for other regional offices that may need to use a regional office transition site or alternate method to ensure recoverability.

*OIT concurs with this recommendation.*

**Recommendation 11**

OIT should continue its efforts to replace the regional office's tape [REDACTED] systems. Additionally, OIT should define a [REDACTED] and recovery strategy for multi-hosted application restoration for the regional offices. OIT should also document the system specific files and database items, in order to facilitate the ability to restore only necessary items, rather than the entire database, which could take many hours to accomplish and is not in line with the recovery time objectives for individual systems.

*OIT concurs with this recommendation.*

**Recommendation 12**

OIT should implement consistent and appropriate [REDACTED] schedules for mission essential and Federal Information System Management Act reportable systems, including daily, weekly, and monthly [REDACTED] processes and procedures, to ensure these systems are recoverable.

*OIT concurs with this recommendation.*

**Recommendation 13**

OIT should include in the Disaster Recovery Plan and Business Continuity Plan, testing steps that are designed to ensure the restoration from [REDACTED] that is consistent with the requirements for systems that are rated as moderate, in accordance with the National Institute of Standards and Technology guidance under the Federal Information Systems Management Act.

*OIT concurs with this recommendation.*

**Recommendation 14**

OIT should ensure that remote access testing is included as part of all Continuity of Operations Program, disaster recovery and pandemic testing activities, including those performed in the regional offices, to ensure that essential personnel and a sample of the representative users of the system are able to function remotely during an unscheduled event.

*OIT concurs with this recommendation.*

**Recommendation 15**

OIT, in consultation with the OFRMS, should require semi-annual testing of remote access devices to ensure up-to-date connectivity and ability for both essential personnel and non-essential personnel to access the Commission's network. In addition, OIT and OFRMS should implement a system notification warning prior to the connectivity testing date and then disable those devices that are not updated.

*OIT and OFRMS concur with this recommendation.*

**Recommendation 16**

OFRMS and OIT should consider implementation of alternate remote access solutions and/or internal directory structure [REDACTED] and Federal Information Security Management Act reportable systems.

*OIT and OFRMS concur with this recommendation. As a note, Citrix and VPN, two of our remote access solutions, do not require desktops to be left on for access to specialized desktop software.*

**Recommendation 17**

OFRMS and OIT should update the COOP documents and necessary agreements to appropriately reflect authorized telework activities by Commission personnel during unscheduled events under the COOP, disaster recovery and pandemic plans, including equipment that will be used for teleworking in such circumstances.

*OIT and OFRMS concur with this recommendation.*

**Recommendation 18**

OFRMS and OIT should ensure that the agency's disaster recovery testing includes the Commissions mission essential and Federal Information Security Management Act reportable systems and pandemic plan testing is conducted on a regular basis.

*OIT and OFRMS concur with this recommendation.*

**Recommendation 19**

OIT should determine aspects of continuity of operations disaster recovery and business continuity plan testing that should be conducted annually for regional offices and for Federal Information Security Management Act reportable systems based upon their security categorization. OIT should ensure that this testing includes the recovery phase and the reconstitution phase, as well as a restoration from [REDACTED]

*OIT concurs with this recommendation.*

**Recommendation 20**

OIT should add elements to contracts and service level agreements for externally hosted systems to provide appropriate methods by which the SEC can obtain assurance that appropriate disaster recovery plan testing is performed on mission essential and Federal Information Security Management Act reportable systems and to ensure the systems are able to function during unscheduled events. Such measures may include SEC participation in the disaster recovery plan testing for the externally hosted systems and/or a review of the results of such testing.

*OIT concurs with this recommendation.*

**Recommendation 21**

OIT should include elements of testing from an alternate site in the regional office continuity of operations program, disaster recovery, and business continuity plan testing on a periodic basis to ensure the necessary capability and functionality for regional office activities are in place.

*OIT concurs with this recommendation. This is typically accomplished by allowing the designated personnel to telework.*

**Recommendation 22**

OFRMS and OIT should include designated essential personnel for systems, divisions/offices, and regional offices in COOP and disaster recovery testing to ensure that a trained workforce is available to support the SEC's mission critical functions following a disaster.

*OIT and OFRMS concur with this recommendation. Disaster recovery personnel are designated in DR documentation.*

**Recommendation 23**

OIT should ensure that system specific scripts and test scenarios are included in the disaster recovery and business continuity plan testing activities to provide assurance of system functionality at alternate locations.

*OIT concurs with this recommendation.*

**Recommendation 24**

OFRMS and OIT should reassess the definition of essential personnel to ensure that this designation includes only personnel whose services are needed during an event to establish mission essential system connectivity and conduct essential activities until normal operations are resumed. OFRMS and OIT should also develop policies and procedures to ensure that elevated communication cards are distributed only to necessary personnel, cards are disabled upon an employee's departure from the agency, and all essential personnel have appropriate elevated communication cards.

*OIT and OFRMS concur with this recommendation.*

**Recommendation 25**

OFRMS, in conjunction with the regional offices, should specify alternate work locations for which the necessary logistics, such as memoranda of agreement, service level agreements, or credit card limits for hotel conference rooms or other locations, are arranged in advance.

*OFRMS concurs with this recommendation.*

**Recommendation 26**

OFRMS should categorize essential personnel according to necessary functions, based on various realistic scenarios (such as Headquarters or Operations Center locations becoming inaccessible or not operational, including traffic conditions that would affect the scenario). Possible categories include personnel required for immediate activities, personnel needed to establish connections at the alternate site, and personnel needed to work remotely at designated alternate sites such as their homes, hotels, or other specified locations.

*OFRMS concurs with this recommendation.*

**Recommendation 27**

OFRMS, as part of its planning efforts, should specify when Commission personnel are to telework after an event and when they must go to the designated alternate locations instead of teleworking.

*OFRMS concurs with this recommendation.*

**Recommendation 28**

OFRMS and OIT should define migration paths from the [REDACTED] should it become inaccessible and specify where the alternate worksite locations for the [REDACTED]

*OIT and OFRMS concur with this recommendation.*

**Recommendation 29**

OFRMS and OIT should ensure that the designated Headquarters alternate worksites are ready for use and contain sufficient equipment and technology resources. In addition, COOP plan documentation should be revised to reflect current space availability and needs, taking into account the potential for telework and remote access.

*OIT and OFRMS concur with this recommendation.*

**Recommendation 30**

OFRMS and OIT should ensure that designated alternate worksite locations are visited and tested periodically to ensure ready access and use. Appropriate steps should be taken to ensure that any cards or badges required for entry to alternate worksite locations are kept up to date and have not expired.

*OIT and OFRMS concur with this recommendation.*

**Recommendation 31**

OIT should reinforce the need for SEC personnel and contractors to register in the agency's emergency notification system, which is designated as the primary method of notifying employees during a continuity of operations or pandemic event. OIT should also implement procedures to ensure the removal of personnel from the emergency notification system after they leave the SEC.

*OIT concurs with this recommendation.*

**Recommendation 32**

OFRMS and OIT should clearly define in the continuity of operations, disaster recovery, and business continuity plan documentation the alternate worksite or telework locations for both essential and non-essential personnel. This documentation should also clarify whether; when relocating to an alternate site is required, family members may accompany Commission employees and contractors to the relocation site, consistent with federal regulations.

*OIT and OFRMS concur with this recommendation.*

**Recommendation 33**

OFRMS and OIT should ensure that recommendations made as a result of the continuity of operations, disaster recovery, business continuity and pandemic testing are

included in a management corrective action plan (CAP) and is maintained in the CAP until it is resolved.

*OIT and OFRMS concur with this recommendation. OIT documents recommendations related to vulnerabilities discovered through COOP and DR testing through its POA&M process, per NIST 800-53. Not all recommendations or lessons learned are vulnerability related.*

**Recommendation 34**

OIT should ensure that open POA&M items from previous years are evaluated by management and final corrective actions are implemented to close the items.

*OIT and OFRMS concur with this recommendation.*

**Recommendation 35**

OFRMS and OIT should ensure that continuity or operations, disaster recovery, and business continuity plan training occur prior to annual tests exercises or events as recommended by NIST Special Publication 800-84, Guide to Test, Training, and Exercise Programs for Information Technology Plans and Capabilities, in order to ensure that individuals are prepared for their specific roles during a disaster recovery event.

*OIT and OFRMS concur with this recommendation.*

**Recommendation 36**

OFRMS, in conjunction with the OHR, OIT, and the various divisions and offices, should consider, consistent with federal personnel regulations, if there is the ability to cross-train regional office personnel in functions that are performed exclusively at the Commission Headquarters and regional offices and, if so, should define these functions and implement procedures for cross-training personnel for mission essential functions in the case of a COOP or pandemic event..

*OIT and OFRMS concur with this recommendation.*

**Recommendation 37**

OFRMS and OIT, in conjunction with the OAS and OGC, should document that the necessary contractual agreements and/or provisions are in place to ensure the availability of hardware, software, and services that may be required during an emergency. The use of government credit cards to procure such equipment and services should also be considered and documented. If government credit cards are to be used for this purpose, the authorized limits established should be sufficient for such purchases.

*OIT and OFRMS concur with this recommendation.*

**Recommendation 38**

OFRMS and OIT, in conjunction with the regional offices, OAS, OFM, and OGC, should ensure that an appropriate and updated Memoranda of Agreement, Memoranda of Understanding and Service-Level Agreements are executed to provide for alternate work site locations, capabilities, and accommodations that may be necessary to ensure continuity of operations.

*OIT and OFRMS concur with this recommendation.*

## OIG Response to Management's Comments

---

We are pleased that SEC management has concurred with the 38 recommendations contained in this report. We believe that full implementation of these recommendations will act to strengthen the SEC's Continuity of Operations Program.



# Audit Requests and Ideas

---

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

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

Tel. #: 202-551-6061  
Fax #: 202-772-9265  
Email: [oig@sec.gov](mailto:oig@sec.gov)

## Hotline

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

Phone: 877.442.0854

Web-Based Hotline Complaint Form:  
[www.reportlineweb.com/sec\\_oig](http://www.reportlineweb.com/sec_oig)