FEDERAL ELECTION COMMISSION

OFFICE OF INSPECTOR GENERAL

FINAL REPORT

INSPECTION OF THE FEDERAL ELECTION COMMISSION'S

DISASTER RECOVERY PLAN AND CONTINUITY OF OPERATIONS PLANS

January 2013

ASSIGNMENT No. OIG-12-06

BROWN & COMPANY CPAs, PLLC
CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS

MEMORANDUM

To: Lynne A. McFarland
Inspector General

From: Brown & Company CPAs, PLLC

Subject: *Inspection of the Federal Election Commission's Disaster Recovery Plan and Continuity of Operations Plans*

Date: January 30, 2013

Brown & Company CPAs, PLLC conducted the *Inspection of the Federal Election Commission's Disaster Recovery Plan (DRP) and Continuity of Operations Plans (COOP)* pursuant to the contract awarded on September 26, 2012. This letter transmits the inspection report issued by Brown & Company CPAs, PLLC. The inspection was performed under a contract with, and monitored by the Office of Inspector General (OIG).

The report contains 30 recommendations to address the 14 deficiencies (findings) identified by the auditors. FEC management was given an opportunity to review this report and provide comments. Management's comments are included in this report in response to each recommendation.

We appreciate the assistance of FEC management and staff during the inspection. Should you have any questions regarding the enclosed report, or need additional information, please feel free to contact us at our main office.

Sincerely,

Gail Jenkins

BROWN & COMPANY CPAs, PLLC

1101 Mercantile Lane
Suite 122
Largo, MD 20774
Phone: (240) 770-1400

Table of Contents

Section **Page**

1 EXECUTIVE SUMMARY

The Federal Election Commission (FEC) Office of Inspector General (OIG) contracted with Brown & Company (Brown) to perform an inspection of the FEC's Disaster Recovery Plan (DRP) and Continuity of Operations Plans (COOP). The objective of the inspection was to determine if the FEC has effectively implemented the FEC's DRP and COOPs in accordance with applicable laws and regulations, and best practices for the federal government.

The FEC Information Technology Division (ITD) hired a contractor to assist in the development of ITD's DRP and FEC's COOPs, and these plans were finalized in November 2010. The COOPs and DRP provide the operating procedures and tools required to quickly resume business operations in the event of a disaster. The FEC's COOPs and DRP include a Business Area Recovery Plan for each significant FEC business unit: The Commissioners; Office of Staff Director; Office of Inspector General; Office of General Counsel; Information Technology Division; and Office of Chief Financial Officer. The COOPs and DRP are designed to cover a disaster at the FEC office building located in Washington, DC.

Under the supervision of the OIG, Brown conducted this inspection in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) *Quality Standards for Inspections and Evaluations*, January 2011. During this inspection, Brown conducted interviews with FEC staff, conducted walkthroughs, and reviewed FEC documentation to specifically determine if FEC:

- established an adequate project plan for the completion of the FEC's DRP/COOPs;
- assigned adequate/sufficient resources in order to complete a mission critical project;
- conducted continuous monitoring procedures to ensure the plans are reflective of current business processes;
- conducted appropriate testing procedures; and
- developed, implemented and tested the FEC's DRP/COOPs in compliance with applicable guidance (best practices) related to the federal government.

Brown identified many instances where processes were not in place or inadequate; COOP emergency contact information was inconsistent or outdated; and key COOP personnel were not aware or notified of their responsibilities in the event of a disaster. The FEC does not have sufficient resources (e.g. back up media readers, data entry application for Disclosure Database) to fully operate and complete mission critical projects at the alternate disaster recovery site. For example, in the event of a disaster, without the data entry application for the Disclosure Database, FEC could not meet the two day legislative disclosure requirement, which is a mission critical task. FEC also has not conducted exercises or continuous monitoring procedures to ensure the plans are reflective of current business processes. FEC's DRP/COOPs have not been fully developed, implemented, or tested. In addition, FEC does not provide or have a plan in place for COOP and DRP training for key personnel.

From FY 2008 to FY 2010, the FEC spent $277,506 on a contract to develop the DRP and COOPs. Although FEC management stated in the OIG's FY 2012 financial statement audit report, "*OCIO believes the COOP testing is complete*," the results of this inspection concluded that the FEC is unaware if their current plans are capable of restoring mission critical functions in the event of a disaster as they have not been fully tested.

FEC management has stated in previous audit reports and meetings regarding this inspection that the FEC is a category 4[1] agency, and "*management deems that policies and testing* [for]. . . *COOP and DR plans are commensurate with the risk analysis appropriate for this agency*." However, in accordance with the *National Continuity Policy Implementation Plan* issued by President George W. Bush in 2007, the FEC is not in compliance with the COOP requirements for the federal government (category 4) since it has: incomplete DRP and COOPs, inadequate plan testing, no DRP and COOP training or testing exercises conducted with key personnel, and no continuous monitoring process in place.

We identified 14 findings and provided management with 30 recommendations for improvement. These are contained in the *Inspection Findings and Recommendations* section of this report, starting on page 7.

The deficiencies identified during this inspection are important to the FEC and the agency's ability to effectively respond, recover and continue agency business from a disaster or disruption of operations. The terrorist attacks on September 11, 2001, the August 2011 5.8 magnitude Virginia earthquake, and Hurricane Irene in August 2011, are all significant events that impacted Washington DC and other areas. The likelihood of future events such as these, although difficult to imagine, is real and possible. Currently, due to the extent of deficiencies identified during this inspection, the FEC is at risk of not being able to effectively respond and maintain critical operations in the event of a disaster or disruption to operations. It is therefore critical that the FEC promptly implement the recommendations contained in this inspection report.

[1] Homeland Security Presidential Directive 20 (HSPD 20) Appendix A assigns agencies to one of four categories commensurate with their Continuity of Operations Plan (COOP)/Continuity of Government (COG)/Enduring Constitutional Government (ECG) responsibilities during an emergency.

2 BACKGROUND

The Department of Homeland Security (DHS), Federal Continuity Directive 1 (FCD 1), *Federal Executive Branch National Continuity Program and Requirements*, dated February 2008, provides guidance to federal executive branch departments and independent establishments as defined by 5 U.S.C. § 104(1), for use in developing viable and executable contingency plans for the continuity of operations. Planning for a possible disaster or significant disruption to operations is a "good business practice," part of the fundamental mission of agencies as responsible and reliable public institutions. The changing threat environment and recent emergencies, including localized acts of nature, accidents, technological emergencies, and military or terrorist attack-related incidents, have shifted awareness to the need for COOP capabilities that enable agencies to continue their essential functions across a broad spectrum of emergencies.

In accordance with DHS FCD 1, to support the continuity program management cycle, agencies will develop a continuity multiyear strategy and program management plan that provides for the development, maintenance, and annual review of continuity capabilities, requiring an agency to:

a. Designate and review Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs), as applicable.
b. Define both short-term and long-term goals and objectives for plans and procedures.
c. Identify issues, concerns, and potential obstacles to implementing the program, as well as a strategy for addressing these, as appropriate.
d. Establish planning, training, and exercise activities, as well as milestones for accomplishing these activities.
e. Identify the people, infrastructure, communications, transportation, and other resources needed to support the program.
f. Forecast and establish budgetary requirements to support the program.
g. Apply risk management principles to ensure that appropriate operational readiness decisions are based on the probability of an attack or other incident and its consequences.
h. Incorporate geographic dispersion into the organization’s normal daily operations, as appropriate.
i. Integrate the organization’s security strategies that address personnel, physical, and information security to protect plans, personnel, facilities, and capabilities, to prevent adversaries from disrupting continuity plans and operations.
j. Develop and implement a Corrective Action Program (CAP) that draws upon evaluations, after-action reports, and lessons learned from testing, training and exercises (TT&E), and real world events.

Since the Office of Inspector General’s (OIG) *Audit of the Federal Election Commission’s Fiscal Year 2004 Financial Statements*, to the most recent annual financial statement audit report for fiscal year (FY) 2012, the OIG has reported the need for the FEC to implement effective continuity of operations plans.

In FY 2008, the FEC procured a contractor for $277,506 to assist in developing an Information Technology Division disaster recovery plan and COOPs for the FEC business areas. The development of the DRP and COOPs was divided into three phases:

- Phase 1: Identify critical essential systems and develop a base IT DRP;
- Phase 2: Develop an IT DRP/COOP for the four identified critical systems to include user needs and requirements; and
- Phase 3: Create a COOP for all business areas and implement (test) the plans.

The development of the DRP and COOPs for all business areas was completed in November 2010; however, the FEC has failed to test all areas of the COOPs to verify the adequacy of the developed plans. In accordance with the *Homeland Security Presidential Directive (HSPD-20)*, section 19 (d):

> Heads of executive departments and agencies shall execute their respective department or agency COOP plans in response to a localized emergency and shall: (d) "*Plan, conduct, and support* ***annual tests and training****…*" (Emphasis added)

The COOPs must be tested and monitored to verify that the plan is efficient, effective, and properly updated. In addition, FEC has not made preparations to ensure that training for all key COOP personnel is completed on an ongoing basis. Best practice guidance and/or FEC policies used by Brown that provided guidance on issues discussed in this report include:

- National Continuity Policy Implementation Plan, Appendix A: National Security Presidential Directive (NSPD-51)/Homeland Security Presidential Directive (HSPD-20);
- FDC 1, *Federal Executive Branch National Continuity Program and Requirements*;
- National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-34, *Contingency Planning Guide for Federal Information Systems*;
- *FEC Information System (IS) Security Program Policy, Policy 58A; and*
- *FEC Continuity of Operation/Disaster Recovery Policy, Policy 58-2.9.*

The above federal requirements, best practice guidance, and FEC IT policies are intended to establish controls over the process of managing emergencies and crises that degrade or interrupt FEC information systems or network services and/or compromise FEC electronic information.

3 OBJECTIVES, SCOPE AND METHODOLOGY

3.1 Objectives

The Office of Inspector General's overall objective for conducting an inspection of the Federal Election Commission's (FEC) Continuity of Operations Plans (COOPs) and Disaster Recovery Plan (DRP) is to determine if FEC is adequately prepared to perform essential functions during a disaster recovery event resulting from human/natural disasters, national emergency or technological events which could impact the FEC's ability to continue mission-critical and essential functions. The objective also is to determine if FEC COOPs and DRP are adequately monitored, and consistent with current processes and industry best practices.

3.2 Scope

The scope of the inspection includes the IT DRP and FEC program area COOPs: The Commissioners; Office of Staff Director; Office of Inspector General; Office of General Counsel; Information Technology Division; and Office of Chief Financial Officer.

3.3 Methodology

The auditors conducted the following inspection steps:

- Reviewed the *Federal Election Commission (FEC) Information System Security Program Policy* and *Federal Election Commission Continuity of Operations and Disaster Recovery Policy* and related procedures for compliance with best practice for the federal government.
- Reviewed the FEC Continuity of Operations Plans (COOPs) for compliance with best practice for the federal government, and reviewed plan documents:
    - FEC Site Emergency Response Plan (ERP),
    - FEC Site Crisis Management Plan (SCMP),
    - Business Area Recovery Plan(s).
- Determined if the FEC COOPs and DRP were developed, implemented and maintained in accordance with federal guidelines.
- Verified if FEC alternate disaster recovery site meets industry standards.
- Inspected FEC COOPs and DRP related documents to determine if the FEC provides COOP and DRP testing, training, and exercises in accordance with federal requirements and industry best practices.
- Interviewed FEC personnel to determine if they are aware of the agency's COOP policies and procedures, and assess their ability to perform significant business functions during a disaster.
- Conducted a walkthrough of the FEC's primary data site that houses the main servers, computer equipment and all systems residing on the FEC LAN.

- Conducted a walkthrough of the FEC's alternate disaster recovery site that houses the backup servers and related IT infrastructure.
- Conducted a walkthrough of the off-site electronic media facility.

4 INSPECTION FINDINGS AND RECOMMENDATIONS

4.1 All active users are not validated on a periodic basis to ensure security policies are effective during a disaster.

As required by the *Telework Enhancement Act of 2010,* FEC has incorporated telework into their Continuity of Operations Plans (COOP). The *Telework Enhancement Act of 2010*, Security Guidelines, include controlling access to agency information and information systems. As noted in the FEC's FY 2011 & 2012 financial statement audit, FEC did not validate all active users on a timely basis which violates the agency's access control policy. When FEC fails to validate users, FEC officials have limited assurance that users have access only to information and information systems that are necessary to accomplish the users' job responsibilities. The finding has not been fully remediated and therefore, increases the risk of improper access to information systems during a disaster. In accordance with NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems,* maintaining the integrity and security of system data and software is a key component in contingency planning. If authorized users' access information is not updated, sensitive data/information can be shared with non-authorized persons, which is an information security and privacy issue.

Recommendation # 1

Until FEC has effectively implemented controls to ensure network access is timely terminated for separated employees and contractors, the FEC should validate on a quarterly review basis all active users to assure that only individuals who are currently and properly authorized have access to FEC's information and information systems during a disaster.

Management Response:

Disagrees with recommendation. The FEC does have an effective process in place to remove access for people leaving the agency. The process is the FEC Systems Access System (FSA). This system was tested and verified during other IG audits. No further action required.

Auditor Comments:

The Office of Inspector General has not tested and verified the FSA. Based on the scope of the inspection, Brown will rely on the OIG's recently released FY 2012 Financial Statement Audit report which states, "… there can never be full assurance that the FSA system will actually reflect the status of network users in active directory." In addition, since FEC has not fully resolved access control weaknesses identified in this recent audit report, we continue to believe that the recommendation should be implemented by FEC.

4.2 FEC's disaster recovery site and primary data site are in the same geographic area.

The FEC's primary data site (also known as the production site), which houses the main servers and equipment, and alternate disaster recovery site, which houses the backup servers, are located within 10 miles of one another. Therefore, the primary data site and the disaster recovery site for the agency have a high risk of experiencing the same disaster due to their locations being in close proximity. According to *Department of Homeland Security (DHS), Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements,* "Alternate operating facilities must be located in an area where disruption to the agency's ability to initiate, maintain, and terminate operations is minimized." Therefore, the FEC's current location of their primary data site and disaster recovery site are not in compliance with federal regulations. In the event of a disaster to this geographical area, the FEC will not have the capability to ensure the continuity of operations for the agency. For example, if the sites share the same power grid, and there is an electricity outage due to a disaster, both sites will be affected.

Recommendation # 2

Review and obtain another alternative for the disaster recovery site or primary data site to ensure that the new facility is located in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure).

Management Response:

Disagrees with this recommendation. The FEC accepts the risk that is associated with having the production and disaster recovery site in the same geographical location, but in separate facilities. Additionally there is a geographically separated mission essential production site to further protect productions data. FEC management deems this acceptable for the mission, disaster category, and resources of the agency. No further action required.

Auditor Comments:

If FEC fails to implement this recommendation, the agency will not be in compliance with federal government guidance. Management notes in their response that "*there is a geographically separated mission essential production site to further protect productions data,*" and this site is located in Massachusetts. However, this data site only houses the FEC's data related to Disclosure. The data that is necessary for FEC personnel to continue business as normal in the event of a disaster is located at the two facilities in Sterling, VA. Therefore, the agency's willingness to accept the risk associated with having their disaster recovery site and primary data site in the same geographical location should be reconsidered. We continue to believe that the recommendation should be implemented by FEC, since the risk can be reduced by selecting an alternate location for their disaster recovery site or primary data site that will comply with the required federal guidance.

4.3 FEC's COOP and DRP contact lists are outdated and do not contain adequate contact information.

Important components of a COOP are the Call Trees, contact information, and the roles and responsibilities for all the recovery teams. This information helps the agency to quickly respond to any disaster or disruptive event. The FEC's COOP and DRP Call Trees and contact lists are in the process of being updated for the first time in two years. According to the *Contingency Planning Guide for Federal Information Systems,* as a general rule, the plan should be reviewed for accuracy and completeness at an organization-defined frequency or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews.

The FEC's current COOP and DRP contact lists contain individuals who no longer work at the agency. In the event of a disaster, effective communication cannot be achieved to properly execute the COOP/DRP because contact information has not been updated. In addition, the information regarding individuals on the contact list is outdated and insufficient. The FEC's COOPs and DRP contain inadequate contact information, to include:

- Incorrect role/position of the listed employees (i.e. Chair and Vice Chair of the Commissioners).
- Acting positions that have been filled with permanent employees.
- Names of separated key personnel that have been replaced with new personnel (i.e. Procurement Officer, Deputy General Counsel).
- Office phone numbers with no alternative phone number that can be used in case of an emergency.

When updates are not made in a timely manner regarding changes to agency personnel, FEC runs the risk of having the COOP key personnel unaware of their responsibilities and duties in the event of a disaster or disruption to the agency.

Recommendation # 3

Update all COOP and DRP personnel contact information to reflect the most current information and distribute the updated plans to the appropriate officials by February 2013.

Management Response:
Agrees with recommendation. The FEC will update contact lists and COOP/DR policy to incorporate the recommendation.

Auditor Comments:
The FEC has agreed to this recommendation, we have no additional comments.

Recommendation # 4

Implement and document a policy that includes:

- Who is responsible for updating and monitoring the contact information in the FEC's COOPs and DRP to reflect current information;
- An organization-defined frequency for updating the FEC's COOPs/DRP contact information; and
- "Required" information that must be provided for those personnel with COOP responsibilities (i.e. FEC office and Blackberry telephone number, personal cellular telephone number and/or home number).

Management Response:
Agrees with recommendation. The FEC will update contact lists and COOP/DR policy to incorporate the recommendation.

Auditor Comments:
The FEC has agreed to this recommendation, we have no additional comments.

Recommendation # 5

For those FEC personnel who are unaware of their COOP responsibilities due to the FEC's failure to update their COOP/DRP contact information (i.e. Procurement Director), provide a copy of the plan with their associated responsibilities by February 2013.

Management Response:
Agrees with recommendation. The FEC will update contact lists and COOP/DR policy to incorporate the recommendation.

Auditor Comments:
The FEC has agreed to this recommendation, we have no additional comments.

4.4 COOP and DRP training is not provided to key COOP personnel.

FEC Continuity of Operations Plans (COOP) pre-disaster responsibilities include ensuring Disaster Recovery Teams are properly trained. Personnel responsible for mission critical systems must be trained to execute contingency procedures. In accordance with the FEC *Continuity of Operations Plan for the Federal Election Commission (FEC) for the Information Technology Division (ITD),* the "training person" is responsible for the development of the Training Plan and the subsequent ongoing timely training for ITD and user staff needed to execute the Disaster Recovery Plan. However, FEC has not developed training for the COOP and Disaster Recovery Plan (DRP), even though the COOPs and DRP were finalized in November 2010.

The Disaster Recovery Team must be properly trained according to the Guidelines of the Contingency Planning Guide for federal information systems. If teams are not properly trained, the FEC risks the chance of the COOP not being properly implemented and can affect the overall strategy of the plan.

Recommendation # 6

Develop and implement a Training Program. Training for key personnel with contingency plan responsibilities should focus on familiarizing them with COOP roles and teaching skills necessary to accomplish those roles. Key personnel should be trained on the following plan elements:

- Cross-team coordination and communication;
- Reporting procedures;
- Security requirements;
- Team-specific processes (Activation and Notification, Recovery, and Reconstitution Phases); and
- Individual responsibilities (Activation and Notification, Recovery, and Reconstitution Phases).

Management Response:
Agrees in part with recommendation. The FEC should and will develop a COOP/DR training plan that is commensurate with the level of COOP/DR as necessary for the DR category and resources available to this agency.

Auditor Comments:
While agency officials agreed with the recommendation, in part, we continue to believe that the recommendation should be fully implemented by FEC, since the COOP/DRP training is required to ensure the plans are properly executed. Management should refer to the Federal Continuity Directive 1, Annex K for the **required** 10 components of a COOP training program for executive branch agencies. If FEC fails to fully implement this recommendation, the agency will not be in compliance with federal government guidance.

Recommendation # 7

Provide COOP/DRP training at least annually. Personnel newly appointed to COOP roles should receive training shortly thereafter joining the FEC if training has already been conducted for the year.

Management Response:
Disagrees with recommendation. Training should not be conducted annually. FEC COOP training plan will provide training as personnel change.

Auditor Comments:
In accordance with HSPD-20, Appendix A: section 19, and FDC 1, which are both requirements for the FEC, COOP training is to be conducted by executive branch agencies on an annual basis. If FEC fails to implement this recommendation, the agency will not be in compliance with federal government guidance.

4.5 Significant deficiencies have not been resolved in the Alert section of the COOP.

After the development of the COOPs, the agency documented any significant deficiencies under the "Alerts" section of the COOPs. The FEC Continuity of Operations Plans (COOP) "Alerts" include the following:

1. The COOP has not been tested.
2. The Information Technology Division (ITD) Disaster Recovery Plan (DRP) has not been fully tested.
3. The data entry application needed for Disclosure has not been tested as the ITD has not procured the right hardware/software for the data entry application needed for Disclosure.
4. Kofax production server was updated without updating the Disaster Recovery (DR) version.

The COOP Alerts should be reviewed and resolved in a timely manner. FEC ITD has not reviewed the COOP Alerts to resolve the above deficiencies which have the following affects: FEC cannot validate that their COOPs are sufficient and can be executed in the event of a disaster; the two days legislative mandate for Disclosure cannot be met; and FEC does not have a complete and finalized COOP.

Recommendation # 8

Within the fiscal year 2013, ending September 30, 2013, develop and implement test plans to fully test each program offices' COOP, with a target of completing all offices' testing by December 2013.

Management Response:
Agrees with recommendation. The FEC will develop a test plan to fully test the COOP/DR - March 2013. The FEC will test the COOP by the end of 2013. The FEC will develop a COOP training plan.

Auditor Comments:
The FEC has agreed to this recommendation, we have no additional comments.

Recommendation # 9

Within the fiscal year 2013, develop and implement a test plan to fully test the ITD DRP, with a target date to begin testing on or before June 2013.

Management Response:
Agrees with recommendation. The FEC will develop a test plan to fully test the COOP/DR - March 2013. The FEC will test the COOP by the end of 2013. The FEC will develop a COOP training plan.

Auditor Comments:
The FEC has agreed to this recommendation, we have no additional comments.

Recommendation # 10

Ensure that the COOPs are tested on an annual basis.

Management Response:
Agrees with recommendation. The FEC will develop a test plan to fully test the COOP/DR during March 2013. The FEC will test the COOP by the end of 2013. The FEC will develop a COOP training plan.

Auditor Comments:
Although FEC has concurred with the recommendation, management's response does not address FEC implementing an annual test plan. We encourage management to clearly identify and document their plan for implementing annual COOP testing in a corrective action plan for this inspection.

Recommendation # 11

Procure the necessary hardware/software to fully test the data entry application needed for Disclosure by December 2013.

Management Response:
Agrees with recommendation. The FEC will develop a test plan to fully test the COOP/DR during March 2013. The FEC will test the COOP by the end of 2013. The FEC will develop a COOP training plan.

Auditor Comments:
Although FEC has concurred with the recommendation, management's response does not address FEC's plan to procure the necessary hardware/software needed for the Disclosure application. We encourage management to clearly identify and document their plan for complying with this recommendation in a corrective action plan for this inspection.

Recommendation # 12

Ensure the disaster recovery Kofax server is updated to mirror the Kofax production server by June 2013.

Management Response:
Agrees with recommendation. The FEC will develop a test plan to fully test the COOP/DR during March 2013. The FEC will test the COOP by the end of 2013. The FEC will develop a COOP training plan.

Auditor Comments:
Although FEC has concurred with the recommendation, management's response does not address FEC's plan to ensure the disaster recovery Kofax server is updated to mirror the Kofax production server. We encourage management to clearly identify and document their plan for implementing this recommendation in a corrective action plan for this inspection.

4.6 Security Control Assessment including the Security Test and Evaluation, and Plans of Action and Milestones has not been documented.

The FEC is not in compliance with their Local Area Network (LAN) System Security Plan (SSP), as the plan states:
"*All referenced General Support System (GSS) with security categorization of moderate or high have undergone independent Security Controls Assessment (SCA)/Security Test and Evaluation (ST&E). The weakness will be documented in the FEC LAN Plan of Action and Milestones (POA&M).*"

During our inspection, FEC did not provide the ST&E and POA&M; therefore, Brown & Company was not able to review the necessary documentation to identify any weakness that may have been identified during the testing.

Since the ST&E has not been conducted and documented, the FEC cannot determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
The POA&M must be updated to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Recommendation # 13

Conduct and document FEC's Security Controls Assessment (SCA)/Security Test and Evaluation (ST&E) in accordance with federal guidelines for information systems.

Management Response:
Agrees with recommendation. The FEC will solicit public bids for the accrediting and certifying the FEC LAN, which will include the ST&E and SCA recommendations. Certification and accreditation for FEC major systems will be conducted during calendar year 2013 as funding becomes available.

Auditor Comments:
The FEC has agreed to this recommendation, we have no additional comments.

Recommendation # 14:

Once the ST&E is complete, develop a POA&M to document the corrective action plan for remediating any findings.

Management Response:
Agrees with recommendation. The FEC will solicit public bids for the accrediting and certifying the FEC LAN, which will include the ST&E and SCA recommendations. Certification and accreditation for FEC major systems will be conducted during calendar year 2013 as funding becomes available.

Auditor Comments:
Although the FEC agrees with this recommendation, management's response does not address the development of a POA&M. We encourage management to clearly identify and document their plan for complying with this recommendation in a corrective action plan for this inspection.

4.7 The alternate disaster recovery site does not have backup media readers to restore backup tapes.

FEC's Information Technology Division (ITD) alternate disaster recovery site is classified as a "warm site," which requires the site to contain system hardware, software, telecommunications, and power sources that are needed to perform mission critical functions during a disaster.

The FEC system hardware at the alternate disaster recovery site does not include a backup media reader to restore backup data in case of a disaster. Therefore, the alternate disaster recovery site will not have the capability to fully retrieve backed up data if the server is down and back-up tapes are needed. If essential FEC personnel are not able to retrieve their data, they will be unable to execute the tasks necessary to fulfill the mission of the agency in the event of a disaster.

Recommendation # 15

Install and test a backup media reader in the alternate disaster recovery site.

Management Response:
Agrees with recommendation. The FEC will install and test a backup media reader at the DR site, as resources become available.

Auditor Comments:
The FEC has agreed to this recommendation, we have no additional comments.

4.8 Key personnel have not received a hard copy of the COOP and/or the file on a USB storage device to use during a disaster.

Currently, copies of the Continuity of Operations Plans (COOP) and Disaster Recovery Plan (DRP) are saved on the FEC server (ntsrv1) and at the alternate disaster recovery site. FEC IT policy requires FEC ITD to provide hardcopies, along with USB storage devices, of the COOPs to key personnel for use when they cannot access the servers during a disaster. During our interviews with key personnel, it was noted that some key personnel have not received a hard copy of the COOP and/or the file on a USB storage device.

If network access is unavailable, designated personnel will not have a guide to assist them during a disaster recovery. Without access to the COOP document, FEC is at risk of not being able to properly implement the plan, which negatively affects the overall recovery efforts.

Recommendation # 16

Comply with FEC IT policy and provide hardcopies, along with USBs, of the COOPs to recovery personnel for use when they cannot access the servers where the COOP files are stored.

Management Response:
Disagree with recommendation. The OCIO's position is that the COOP/DR plans are available to all personnel on a shared drive. It is the individual responsibility of each COOP/DR team member to obtain a copy of the plans as they see fit to fulfill their duties as team members. The FEC will, however emphasize this individual responsibility and incorporate in the training program agreed to in NFR 4 above.

Auditor Comments:
We continue to believe that the recommendation should be implemented by FEC to ensure key personnel have the information needed to fulfill their roles and responsibilities during a disaster. The agency should provide a hard copy of the COOP/DRP as part of the training program to be implemented.

Recommendation # 17

Maintain a record of the individuals who received hard copies of the COOP and/or copies of the COOP files on USB devices.

Management Response:
Disagree with recommendation. The OCIO's position is that the COOP/DR plans are available to all personnel on a shared drive. It is the individual responsibility of each COOP/DR team member to obtain a copy of the plans as they see fit to fulfill their duties as team members. The FEC will, however emphasize this individual responsibility and incorporate in the training program agreed to in NFR 4 above.

Auditor Comments:
We continue to believe that the recommendation should be implemented by FEC to ensure key personnel have the information needed to fulfill their roles and responsibilities during a disaster. The agency should maintain a record of the individuals who received a hard copy of the COOP/DRP as part of continuous monitoring procedures for the agencies overall continuity of operations program.

Recommendation # 18

Contracts with vendors (Service Level Agreements and other contracts), software licenses, system user manuals, security manuals, and operating procedures should be provided with the hard copy of the COOP/DRP.

Management Response:
Disagree with recommendation. The OCIO's position is that the COOP/DR plans are available to all personnel on a shared drive. It is the individual responsibility of each COOP/DR team member to obtain a copy of the plans as they see fit to fulfill their duties as team members. The FEC will, however emphasize this individual responsibility and incorporate in the training program agreed to in NFR 4 above.

Auditor Comments:
We continue to believe that the recommendation should be implemented by FEC to ensure key personnel have the information needed to fulfill their roles and responsibilities during a disaster. The agency should maintain contracts and service level agreements with vendors long with the hard copies of the COOP/DRP as part of continuous monitoring procedures for the agency's overall continuity of operations program.

4.9 An alternate workspace has not been secured in the event of a disaster.

The FEC data center and alternate disaster recovery site are located in Sterling, VA and do not provide alternate workspace for FEC employees. In case of a disaster that disrupts FEC services for a short period, the FEC personnel are instructed to work from home in accordance with the agency's Telework policy and procedures.

In accordance with the FEC's Continuity of Operations Plans (COOP), Plan Implementation Logistics, the FEC Procurement Office should request from the General Services Administration (GSA) an alternate location for 51 FEC employees in case of a long term disaster. This space is to include office equipment, internet connectivity and telephone connectivity. In addition, the FEC Inspector General (IG) is to be provided separate and securable space. However, the agency does not have a written agreement with GSA to provide office space in case of a long term disaster.

In the event agency work requires a group effort, the FEC does not have a physical location readily available to conduct business.

Recommendation # 19

Develop and implement a Memorandum of Understanding (MOU) with GSA to secure an alternate workspace in accordance with the COOP in case of a disaster at the FEC building by February 2013.

Management Response:

The Deputy CIO for Operations advised that the FEC has attempted to establish this MOU with GSA in FY 2009. The CFO contacted GSA to establish this arrangement but was rebuffed by GSA. GSA stated that in the event of a national emergency, alternative office space availability is determined by national disaster recovery prioritization. GSA further stated that in the event of a FEC specific and unique disaster, office space will be provided at the time, this is part of GSA's mission and will be conducted at the time of disaster rather than in advance. No further action required.

Auditor Comments:

If GSA will not agree to a MOU with the FEC based on their mission, we encourage management to develop and document an internal plan that details and prioritizes the FEC personnel (by position) who will occupy the GSA provided space in the event of a disaster, to include their most essential needs (i.e. equipment, communication, etc).

4.10 Certification &Accreditation documents or the LAN Risk Assessment to support the System Security Plan (SSP) were not provided to the auditors for review.

FEC's Certification & Accreditation (C&A) documents completed May 2009, and the LAN Risk Assessment completed December 2008 to support the System Security Plan (SSP) were not provided to the auditors for review during this inspection. The C&A documents include the official management decision to authorize operation of an information system, and to explicitly accept the risk to organizational operations and assets. Per the Information Technology Division (ITD), the FEC's major applications and general support system have not been certified since 2009.

FEC has not complied with the agency's Certification and Accreditation Policy that states "prior to operating, FEC major applications and general support systems should undergo certification."

The auditor could not complete certain Disaster Recovery Plan (DRP) and Continuity of Operations Plans (COOP) inspection steps because the FEC did not provide the documentation prior to the end of the inspection fieldwork. Therefore, the auditor could not determine whether the FEC develops, disseminates, and periodically reviews/updates:

- formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, and compliance; and
- formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

The auditor also could not complete the DRP and COOP inspection steps to determine if the FEC information system developer created a security test and evaluation plan, implemented the plan, conducted annual testing, documented the results, and tested the recovery phase and reconstitution phase. The inspection steps could not be completed because the documentation requested by the auditor was not provided prior to the end of the inspection fieldwork.

Recommendation # 20

Conduct and document FEC's Certification and Accreditation package to include Security Controls Assessment (SCA)/Security Test and Evaluation (ST&E) in accordance with federal guidelines for information systems.

Management Response:

Agrees with recommendation. The FEC will solicit public bids for the accrediting and Certifying the FEC LAN, which will include the ST&E and SCA recommendations. Certification and accreditation for FEC major systems will be conducted during calendar year 2013 as funding becomes available.

Auditor Comments:
The FEC has agreed to this recommendation, we have no additional comments.

Recommendation # 21

Complete the development of the FEC Certification and Accreditation Program by March 2013, with certification of the FEC's major applications and general support systems being completed by April 2013. The C&A should be completed before placing systems into operation.

Management Response:
Agrees with recommendation. The FEC will solicit public bids for the accrediting and certifying the FEC LAN, which will include the ST&E and SCA recommendations. Certification and accreditation for FEC major systems will be conducted during calendar year 2013 as funding becomes available.

Auditor Comments:
The FEC has agreed to this recommendation, we have no additional comments.

Recommendation # 22

Authorize (i.e., accredit) the information system for operations every two years (i.e. April 2013, April 2015, etc.).

Management Response:
Disagrees with recommendation. FEC will conduct C&A in accordance with the current policy.

Auditor Comments:
We continue to believe that the recommendation should be implemented by FEC, since FEC Certification and Accreditation Policy; Number 58-2.4, is not compliant with best practices for the federal government and does not specify a timeframe for conducting the C&A.

Recommendation # 23

Develop a security test and evaluation plan, implement the plan, and document the results as part of the C&A package.

Management Response:
Disagrees with recommendation. Testing and C&A are separate entities and the documentation will remain separate.

Auditor Comments:

Although management disagrees with this recommendation, review of management's alternate process of maintaining separate documentation will need to be reviewed in the near future to assess if separate documentation is an efficient process for maintaining and resolving test results.

4.11 COOP exercise plans have not been developed or implemented.

Management has stated in a recent OIG audit report that, "*The FEC has met all TT&E (Test, Training, and Exercise) requirements for a category 4 agency in accordance with internal IT policies and directives.*" However, the FEC Continuity of Operations Plans (COOP) for Information Technology Division (ITD) does not include a COOP exercise schedule or plan. In addition, FEC's exercise plan should be in compliance with federal government requirements such as FDC 1, rather than FEC's internal policies that are not fully aligned with federal government standards.

FEC has not developed an exercise plan that is a simulation of an emergency designed to validate the viability of one or more aspects of the COOPs. In an exercise, key personnel with roles and responsibilities in a particular COOP meet to validate the content of a plan through discussion of their roles and their responses to emergency situations, execution of responses in a simulated operational environment, or other means of validating responses that do not involve using the actual operational environment. Exercises are scenario-driven, such as a power failure in one of the organization's data centers or a fire causing certain systems to be damaged, with additional situations often being presented during the course of an exercise.

In addition, FEC has not developed and maintained a viable contingency planning program for their information systems to include exercising the plan. FEC will not be able to identify planning gaps that may only be discovered during an exercise. Key personnel have not validated their operational readiness for emergencies by performing their duties in a simulated operational environment.

Recommendation # 24

Develop and implement a COOP exercise plan. The functional exercise should include all COOPs 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 backup media.

Management Response:

Disagrees with recommendation. The FEC has exercised the COOP/DR program, through "real exercise." The FEC has experienced server outages, power interruptions, and natural disasters that interrupt services from time to time. During these outages, we have switched from the production environment to the DR environment and proved that service will continue in the DR environment during the outages. The benefit of a scheduled test in addition to the aforementioned outages does not outweigh the cost of

conducting an exercise, i.e.: downtime, overtime, lack of staff availability, and increase contract support costs.

Auditor Comments:
As "live" events that cause the FEC to execute aspects of the disaster recovery environment are great ways to ensure that components of the FEC's disaster recovery plan is efficient, it is inadequate to depend solely on "live" events to take place as FEC will not be aware of any deficiencies prior to encountering a real disaster. FEC's suggested plan is also not sufficient in conducting regular exercises, which is required by federal guidance and should be implemented by the FEC. We continue to believe that the recommendation should be implemented by FEC. The FEC's continuity exercise program should focus primarily on evaluating capabilities or an element of a capability, such as; a plan or policy, in a simulated situation.

4.12 The COOP pre-positioned equipment inventory is stored at the FEC building.

The pre-positioned equipment inventory (backup inventory of software, hardware, and equipment) for the COOP is stored at FEC headquarters, instead of a warehousing facility located a distance from the FEC building.

If there is not adequate distance between the disaster sites and pre-position equipment storage facility, the agency risks the chance of not being able to utilize the equipment in a disaster.

Recommendation # 25

Store the pre-positioned equipment inventory in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the FEC office.

Management Response:
Agrees with the recommendation. Implementing this recommendation is predicated on the availability of funds.

Auditor Comments:
The FEC has agreed to this recommendation, we have no additional comments.

4.13 FEC does not have Interconnection Security Agreements (ISA) for external systems.

The Interconnection Security Agreements (ISA) are used to document the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within the FEC and external to the organization.
The FEC LAN interconnects with Savvis Data Center in Waltham, MA which provides hosting for the FEC web site and Oracle databases. The National Finance Center (NFC) connects to the

FEC LAN for exchanging the agency payroll information. FEC does not have an ISA with Savvis. FEC did not provide the auditors with the ISA with National Finance Center (NFC).

Recommendation # 26

Authorize connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements with Savvis.

Management Response:
The FEC has a service level agreement in place. This document was placed in PBC [Prepared By Client] folder #15 on 1/11/13 for the audit review. The agreement with NFC is held on file with the CFO office [and]… will provide the agreement by 1/30/2013.

Auditor Comments:
Unfortunately the documentation mentioned in management's response was not provided for review prior to the completion of the testing phase (the week of Dec. 17, 2012). In addition, the auditors are unable to review the stated forthcoming documentation on January 30, 2013 as we have completed the inspection testing phase. Therefore, the auditor was not able to determine if the documentation resolved the finding.

Since the FEC agreed to this recommendation, we have no additional comments.

Recommendation # 27

Document each connection, the interface characteristics, security requirements, and the nature of the information communicated in an Interconnection Agreement.

Management Response:
The FEC has a service level agreement in place. This document was placed in PBC [Prepared By Client] folder #15 on 1/11/13 for the audit review. The agreement with NFC is held on file with the CFO office [and]… will provide the agreement by 1/30/2013.

Auditor Comments:
Unfortunately the documentation mentioned in management's response was not provided for review prior to the completion of the testing phase (the week of Dec. 17, 2012). In addition, the auditors are unable to review the stated forthcoming documentation on January 30, 2013 as we have completed the inspection testing phase. Therefore, the auditor was not able to determine if the documentation resolved the finding.

Since the FEC agreed to this recommendation, we have no additional comments.

Recommendation # 28

Monitor the information system connections on an ongoing basis verifying enforcement of security requirements.

Management Response:
The FEC has a service level agreement in place. This document was placed in PBC [Prepared By Client] folder #15 on 1/11/13 for the audit review. The agreement with NFC is held on file with the CFO office [and]… will provide the agreement by 1/30/2013.

Auditor Comments:
Management's response does not address this recommendation. We would encourage management to apply this recommendation to the service level agreements the agency has with SAVVIS and NFC.

4.14 System Security Plan, COOPs, and DRP are not reviewed and updated on an annual basis.

The System Security Plan (SSP) has not been reviewed or updated annually, as required by FEC policy. The System Security Plan was last updated on 12/03/09. The FEC Continuity of Operations Plans (COOP) has not been reviewed and updated to include status of "Alerts." The FEC COOPs and DRP were last updated on 11/8/2010.

If plans are not updated and tested, at least annually, they will become non-effective and inaccurate. Subsequently, the SSP, COOPs and DRP will not include recent changes in the information system environment and security controls.

Recommendation # 29

Review and update the FEC System Security Plan at least annually.

Management Response:
Agrees in principle with recommendation. The FEC will review and update the SSP, COOP and DRP annually, and document that such a review was held.

Auditor Comments:
The FEC has agreed to this recommendation, we have no additional comments.

Recommendation # 30

Establish a process to certify that the COOPs for the FEC program offices and ITD's Disaster Recovery Plan (DRP) are updated on an annual basis to reflect changes in the

information system environment and security controls in conjunction with the required annual training.

Management Response:

Disagrees with recommendation. Do not concur with recommendation since we do not concur with annual training.

Auditor Comments:

We continue to believe that the recommendation should be implemented by FEC, since the FEC program offices' information system environment and threats may change during the year. Updating the COOPs and DRP on an annual basis can be done outside of the training environment, if necessary.

Federal Election Commission
Office of Inspector General

Fraud Hotline
202-694-1015

or toll free at 1-800-424-9530 (press 0; then dial 1015)
Fax us at 202-501-8134 or e-mail us at oig@fec.gov
Visit or write to us at 999 E Street, N.W., Suite 940, Washington DC 20463

Individuals including FEC and FEC contractor employees are encouraged to alert the OIG to fraud, waste, abuse, and mismanagement of agency programs and operations. Individuals who contact the OIG can remain anonymous. However, persons who report allegations are encouraged to provide their contact information in the event additional questions arise as the OIG evaluates the allegations. Allegations with limited details or merit may be held in abeyance until further specific details are reported or obtained. Pursuant to the Inspector General Act of 1978, as amended, the Inspector General will not disclose the identity of an individual who provides information without the consent of that individual, unless the Inspector General determines that such disclosure is unavoidable during the course of an investigation. To learn more about the OIG, visit our Website at: http://www.fec.gov/fecig/fecig.shtml

Together we can make a difference.