LEON SNEAD
& COMPANY, P.C.

The Commission, Federal Election Commission
Inspector General, Federal Election Commission

Independent Auditor's Report

We have audited the balance sheets of the Federal Election Commission (FEC) as of September 30, 2012 and 2011, and the related statements of net cost, changes in net position, budgetary resources, and custodial activity (the financial statements) for the years then ended. The objective of our audit was to express an opinion on the fair presentation of those financial statements. In connection with our audit, we also considered the FEC's internal control over financial reporting and tested the FEC's compliance with certain provisions of applicable laws and regulations that could have a direct and material effect on its financial statements.

SUMMARY

As stated in our opinion on the financial statements, we found that the FEC's financial statements as of and for the years ended September 30, 2012 and 2011, are presented fairly, in all material respects, in conformity with accounting principles generally accepted in the United States of America.

Our consideration of internal control would not necessarily disclose all deficiencies in internal control over financial reporting that might be material weaknesses under standards issued by the American Institute of Certified Public Accountants. However, our testing of internal control identified no material weaknesses in financial reporting. We did note one significant deficiency related to internal controls for the FEC's agency-wide Information Technology (IT) security program that are discussed later in our report.

The results of our tests of compliance with certain provisions of laws and regulations disclosed no instance of noncompliance that is required to be reported herein under *Government Auditing Standards*, issued by the Comptroller General of the United States and Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements* (as amended).

The following sections discuss in more detail our opinion on the FEC's financial statements, our consideration of the FEC's internal control over financial reporting, our tests of the FEC's compliance with certain provisions of applicable laws and regulations, and management's and our responsibilities.

OPINION ON THE FINANCIAL STATEMENTS

We have audited the accompanying balance sheets of the FEC as of September 30, 2012 and 2011, and the related statements of net cost, changes in net position, budgetary resources and custodial activity for the years then ended.

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position, net cost, changes in net position, budgetary resources and custodial activity of the FEC as of and for the years ended September 30, 2012 and 2011, in conformity with accounting principles generally accepted in the United States of America.

Accounting principles generally accepted in the United States of America require that Management's Discussion and Analysis be presented to supplement the basic financial statements. Such information, although not a part of the basic financial statements, is required by the Federal Accounting Standards Advisory Board (FASAB) who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic financial statements, and other knowledge we obtained during our audit of the basic financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

RESPONSIBILITIES

Management Responsibilities

Management of the FEC is responsible for: (1) preparing the financial statements in conformity with generally accepted accounting principles; (2) establishing, maintaining, and assessing internal control to provide reasonable assurance that the broad control objectives of the Federal Managers Financial Integrity Act (FMFIA) are met; and (3) complying with applicable laws and regulations. In fulfilling this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs of internal control policies.

Auditor Responsibilities

Our responsibility is to express an opinion on the financial statements based on our audit. We conducted our audit in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and OMB Bulletin 07-04, *Audit Requirements for Federal Financial Statements* (as

amended). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement.

An audit includes (1) examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements; (2) assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audit provides a reasonable basis for our opinion.

In planning and performing our audit, we considered the FEC's internal control over financial reporting by obtaining an understanding of the agency's internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements.

We limited our internal control testing to those controls necessary to achieve the objectives described in OMB Bulletin 07-04 (as amended) and *Government Auditing Standards*. We did not test all internal controls relevant to operating objectives as broadly defined by FMFIA. Our procedures were not designed to provide an opinion on internal control over financial reporting. Consequently, we do not express an opinion thereon.

As part of obtaining reasonable assurance about whether the agency's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, and significant provisions of contracts, noncompliance with which could have a direct and material effect on the determination of financial statement amounts, and certain other laws and regulations specified in OMB Bulletin 07-04, (as amended). We limited our tests of compliance to these provisions and we did not test compliance with all laws and regulations applicable to the FEC. Providing an opinion on compliance with certain provisions of laws, regulations, and significant contract provisions was not an objective of our audit and, accordingly, we do not express such an opinion.

INTERNAL CONTROL OVER FINANCIAL REPORTING

In planning and performing our audit of the financial statements of the FEC as of and for the years ended September 30, 2012 and 2011, in accordance with auditing standards generally accepted in the Unites States of America, we considered the FEC's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the FEC's internal control. Accordingly, we do not express an opinion on the effectiveness of the FEC's internal control.

Because of inherent limitations in internal controls, including the possibility of management override of controls, misstatements, losses, or noncompliance may nevertheless occur and not be detected. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance of the FEC.

Our consideration of internal control was for the limited purpose described in the first paragraph in this section of the report and would not necessarily identify all deficiencies in internal control that might be deficiencies, significant deficiencies or material weaknesses. We did not identify any deficiencies in internal control that we consider to be material weaknesses, as defined above. However, as discussed below, we identified a deficiency in internal control that we consider to be a significant deficiency.

Findings and Recommendations

FEC's governance and management officials' decision to not fully adopt Information Technology (IT) best practices increases risk to the agency's information and information systems. Other federal agencies exempted from the Federal Information Security Management Act (FISMA)[1] have adopted these best practices to ensure information and information systems are properly secured. The absence of FEC policies requiring the Office of the Chief Information Officer (OCIO) personnel to perform and document a fact-based risk assessment when deciding not to adopt an IT security best practice requirement increases risk to the agency's information and information systems. Without adopting and implementing National Institute of Science and Technology (NIST)

[1] The National Institute of Science and Technology (NIST) noted that the E-Government Act (Public Law 107-347), passed by the 107th Congress and signed into law by President George W. Bush in December 2002, recognized the importance of information security to the economic and national security interests of the United States. "NIST employs a comprehensive public review process on every FISMA standard and guideline to ensure the security standards and guidelines are of the highest quality—that is, technically correct and implementable. NIST actively solicits and encourages individuals and organizations in the public and private sectors to provide feedback on the content of each of the FISMA publications. In most cases, the FISMA security publications go through three full public vetting cycles providing an opportunity for individuals and organizations to actively participate in the development of the standards and guidelines. NIST also works closely with owners, operators, and administrators of information systems within NIST to obtain real-time feedback on the implementability of the specific safeguards and countermeasures (i.e., security controls) being proposed for federal information systems. Finally, NIST has an extensive outreach program that maintains close contact with security professionals at all levels to ensure important feedback can be incorporated into future updates of the security standards and guidelines. The combination of an extensive public review process for standards and guideline development, the experience in prototyping and implementing the safeguards and countermeasures in the information systems owned and operated by NIST, and the aggressive outreach program that keeps NIST in close contact with its constituents, produces high-quality, widely accepted security standards and guidelines that are not only used by the federal government, but are frequently adopted on a voluntary basis by many organizations in the private sector."

minimum security controls, the FEC's computer network, data and information is at an increased risk of loss, theft, manipulation, interruption of operations, and other adverse actions.

Best practice guidance and/or FEC policies that provide guidance on issues discussed in this finding include: OMB Circular A-130, *Management of Federal Information Resources* (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems;* Special Publication (SP) 800-53, *Recommended Security Controls for Federal Systems and Organizations*; SP 800-118, *Guide to Enterprise Password;* SP 800-34, *Contingency Planning Guide for Federal Information Systems;* OMB Bulletins; Department of Homeland Security directives; and FEC IT Security Policies 58.2.2, 58.2.4, and 58-4.3. In addition, Office of Management and Budget Circular A-50, *Audit Follow-up,* as revised, and FEC Directive 50, *Audit Follow-up,* provide guidance on the requirements for audit follow-up.

The issues we identified with FEC IT security controls are detailed below.

A. Full Adoption of NIST Best Practices Would Strengthen FEC's Information and Information Systems

As we have reported since 2009, FEC, unlike other Federal agencies exempted from FISMA compliance, has not fully adopted the minimum government-wide IT security controls and techniques released by the NIST. FEC officials advised that they follow NIST "best practices" where applicable to their operations. However, there are no FEC policies that guide when an analysis should be performed in making a decision whether or not to implement required government-wide security practices. In addition, we were advised that there is no documentation retained to support such critical decisions that impact the security of FEC's information and information systems. Tests of selected IT security controls found numerous instances where applicable best practice controls were not implemented by FEC, and we were unable to locate substantive analysis of the risk to the agency of not adopting these minimum best practices. Controls tested included: vulnerability scanning of the FEC's entire network; implementation of minimum established password controls; configuration management; user access controls; certification and accreditation controls; and implementation of one of the President's national security initiatives, TIC (Trusted Internet Connections).

In prior audit reports, we recommended that FEC adopt the NIST IT security controls established in FIPS 200 and SP 800-53, and other related FISMA security documents. We also reported that the Government Accountability Office (GAO), another Federal agency exempt from FISMA, had adopted the NIST security requirements. GAO stated[2] that it "adheres to federal information security governance, such as OMB and National Institute of Standards and Technology guidance."

[2] See GAO Performance and Accountability Report – 2011, page 58.

The Inspector General's "Statement on the Federal Election Commission's Management and Performance Challenges," dated October 14, 2011, stated:

> "…Since 2004, the OIG (Office of Inspector General) has reported, and continues to believe that it is in the best interest of the agency to formally adopt government-wide IT security standards to ensure the FEC has an effective information security program. For several years, the OIG's auditors have identified IT practices that are not aligned with the minimal best practice standards that are followed by federal agencies government-wide. Lastly, the agency has failed to adequately define the set of best practices used to secure the FEC's information technology."

FEC officials have indicated that the agency makes informed decisions when deciding whether to adopt government-wide IT security requirements. As part of our audit testing, we requested that OCIO officials provide us with FEC policy guidance that requires a risk-based analysis of IT security requirements, and/or documentation that would provide support for a decision to not adopt a government-wide IT security requirement for the period 2010 to present. We also requested that FEC provide us with any documentation that would support the decision to not adopt two key government-wide IT security requirements, the Trusted Internet Connections (TIC)[3] which has been a requirement since 2007, and Federal Acquisition Regulations[4](FAR) that mandate that FISMA security requirements be included in IT service and related contracts. OCIO officials advised us that FEC does not have a procedure that requires such an analysis, and there was no documentation of any analysis identifying the risks of not adopting these two key security requirements.

An illustration of the importance of FEC implementing a policy requirement to perform a risk-based analysis when deciding not to adopt a government-wide security requirement, and to document this decision with the approval of the CIO, at a minimum, is the decision of FEC officials to not implement the TIC.

TIC was introduced in OMB Memorandum M-08-05, dated November 20, 2007. The initiative was described in the memorandum as an effort to develop "a common [network] solution for the federal government" that would reduce the

[3] TIC was introduced in OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections (TIC)*, dated November 20, 2007, and required that agencies develop "a common solution for the federal government" that would reduce the number of external Internet connections for the entire government to 50. National Security Presidential Directive 54/Homeland Security Presidential Directive 23, *Cyber Security and Monitoring*, (NSPD-54 and HSPD-23) issued in January 2008 included TIC as Initiative #1, Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections. The Trusted Internet Connections (TIC) initiative, headed by the Office of Management and Budget and the Department of Homeland Security, covers the consolidation of the Federal government's external access points (including those to the Internet). This consolidation will result in a common security solution which includes: facilitating the reduction of external access points; establishing baseline security capabilities; and, validating agency adherence to those security capabilities.

[4] Page 7.1-2, FAR Section 7.103 states: "Agency-head responsibilities--- The agency head or a designee shall prescribe procedures for ensuring that agency planners on information technology acquisitions comply with the information technology security requirements in the Federal Information Security Management Act (44 U.S.C. 3544)..."

number of external Internet connections for the entire government to 50. The memorandum stated that "each agency will be required to develop a comprehensive POA&M (Plan of Action and Milestones)" to implement TIC, but it neither defined "agency" nor referred to any legal authority supporting the initiative. FEC's Office of General Counsel (OGC) analyzed this document and determined that since POA&Ms were required by FISMA or its predecessor statute, and because this POA&M requirement appeared to be an expansion of an existing requirement from which the Commission was exempt, the FEC was exempt from TIC.

In a June 2009 memorandum to the Staff Director, OGC noted that on January 8, 2008, former President Bush signed Homeland Security Presidential Directive (HSPD) Number 23 which authorizes the Department of Homeland Security (DHS) to deploy Einstein 2, an automated intrusion detection system, across Federal networks. Einstein 2 would allow the DHS, National Cyber Security Division, and U.S. Computer Emergency Readiness Team (US-CERT) to consolidate Federal system intrusion detection, incident analysis and cyber response capabilities. HSPD-23 is classified; therefore, the specific authorizing statute for the directive and the extent of its application to the Federal Election Commission is unknown. The OGC stated that "We confirmed with DHS on November 12, 2008 that in DHS's view the Commission is within the scope of the presidential directive. However, unclassified legal briefing materials provided by the Department of Justice indicate that at least part of the directive may be authorized by FISMA, from which the FEC is exempt. Thus, there is a possibility that HSPD-23 is only partially applicable to the FEC, or is not applicable at all to the FEC. Since the directive itself is classified, and limited unclassified information has been released, we do not have sufficient information at this time to confirm HSPD-23's applicability to the FEC."

While it was DHS's position, as confirmed by the FEC GC in a memorandum issued in August 2012 to the Staff Director, that the TIC was a critically important IT security measure that was applicable to FEC; the FEC did not implement this Presidential security initiative. Instead, FEC officials took no action to assess the importance of this government-wide initiative or evaluate whether risks would be reduced if FEC implemented this security requirement. As a result of this audit, the FEC now agrees that the TIC initiative must be implemented. A failure by the FEC to perform due diligence on this control as required in 2007, increased the risk that the agency's network could have been exposed to a network intrusion or other computer network attack.

Recommendations

1. Formally adopt as a model for FEC, the NIST IT security controls established in FIPS 200 and SP 800-53, as the Government Accountability Office has done.

Agency Response

The Deputy CIO for Operations advised that the OCIO disagrees with this recommendation. The FEC has adopted, and has put in place the necessary security requirements and controls to ensure that the FEC IT systems are secure. As an agency exempt from FISMA, the controls in place reflect the appropriate level of security and acceptable risk to support the mission and safeguard the data of the agency. The agency's security program is governed by Directive 58 which consists of 34 policies, 8 distinct procedures, adoption of 18 standards, all documented and signed and endorsed by the CIO.

Auditor's Comments

We continue to believe that the FEC's information and information systems are at high risk because of the decision made by FEC officials not to adopt all minimum security requirements that the Federal government has adopted, including the GAO which is also exempt from FISMA requirements. We do not dispute that the FEC has issued policies and procedures. Our position is that these policies and procedures are not currently adequate to secure FEC's information and information systems. As discussed above, had FEC not declined to adopt mandatory security procedures included in the "trusted internet connection," even after the DHS advised the requirement was applicable to FEC, risk to the agency computer network could have been minimized.

2. Revise FEC policies to require that FEC contractors adhere to the FAR FISMA related requirements, and mandate that FEC contractors follow FISMA IT controls when providing services to the federal government. Use NIST SP 800-53 as guidance for establishing IT controls that contractors must follow.

Agency Response

The Deputy CIO for Operations advised that the OCIO disagrees with this recommendation. As a FISMA exempt agency, the FEC incorporates language and is supported by FAR clauses that address the level of security necessary to safeguard agency security in all of its contracts. This language was agreed to by the agency contracting officer and ISSO, contractors are required to adhere to the same level of security that FEC employees are.

Auditor's Comments

FEC should not use the agency's FISMA exemption to also exempt its contractors from meeting minimum federal government IT security requirements. The federal government has established a comprehensive IT services contracting process that assures that minimum security requirements are met, including the requirement of a continuous monitoring process over these IT services. If FEC continues to refuse to adopt these federal requirements, the agency will be required to stand alone in its development of

IT security controls, and complete a duplicate and ineffective continuous monitoring process.

3. Develop a time-phased corrective action plan to address the prompt implementation of the TIC by FEC. Ensure that TIC is implemented as soon as possible, but no later than June 2013.

Agency Response

The Deputy CIO for Operations advised that the OCIO agrees with this recommendation that the FEC must now comply with TIC. In light of new information provided to the FEC in August 2012, that requires the FEC to implement TIC, the FEC will develop a plan to address TIC implementation. This plan will be developed dependent upon the availability of resources required, and we cannot commit to a specific timeframe until a detailed analysis of what is required is performed. The FEC is scheduled to meet with Commerce Department to discuss lessons learned.

Auditor's Comments

The OCIO agreed to implement this recommendation; however, the agency would not commit to a specific timeframe for completion. It has been almost four years since the DHS advised the agency that the implementation of TIC was a requirement for FEC. We believe that this Presidential initiative should be implemented immediately, and until the agency fully implements this project, the agency's information and information systems remain at high risk.

4. Revise FEC policies and procedures to require a documented, fact-based risk assessment prior to deciding not to adopt a government-wide IT security best practice, or IT security requirement contained in the Federal Acquisition Regulations. Require the CIO to approve and accept the risk of any deviation from government-wide IT security best practices (i.e. NIST, FAR IT controls) that are applicable to the FEC business operations. Retain documentation of these decisions.

Agency Response

The Deputy CIO for Operations advised that the OCIO disagrees with this recommendation. The Office of General Counsel provides opinion on which government-wide security requirements are applicable to this agency, based upon specific exemptions granted by Congress. If the agency is indeed exempted from a requirement, the OCIO will determine whether or not the agency will establish and maintain "best practice" of that exemption within the resources available. Documentation of the opinion of the agency's General Counsel on each exemption of applicable law or regulation is maintained on file.

Auditor's Comments

The FEC's information and information systems will continue to remain at risk until the agency begins to make documented, risk-based IT security decisions. Currently, FEC's IT security decisions appear to be based primarily upon whether the agency is legally exempt from the government-wide requirement, instead of a determination that implementation of the security requirement would make the agency's information and information systems more secure. As noted above, the agency failed to implement one of the President's top IT security priorities because the agency erroneously believed it may have been indirectly linked to the legislation that implemented FISMA.

B. Access Controls

FEC's access controls do not meet best practice controls, and in some instances FEC policies. Our tests of this key IT security control identified the following problems:

User Accounts: Passwords are the keys to accessing FEC's general support system (GSS) and related information and information systems, and provide front-end access to FEC's accounting, financial management and payroll systems. Therefore, the strength of FEC's access controls and passwords is critically important. We have reported since 2009 that the password requirements established by FEC are weak, and do not meet OMB mandated government-wide requirements for password strength (see issues below for further details). Because FEC is exempt from the legislation underlining OMB requirements relating to this area, FEC officials have elected not to implement several of the minimum government-wide requirements for strengthening passwords. The agency did not have any documentation to support this decision.

Accounts with Passwords that Never Expire: During our review of access controls, we obtained a listing of user accounts with passwords set never to expire (therefore, the same password would be used for this account until either this setting is changed, or the account's password is changed manually). From a total listing of about 570 accounts, approximately 140 accounts had passwords without expiration dates. We identified that approximately 100 of the 140 accounts had passwords that had not been changed since 2010. According to the records provided, approximately 80 of the 140 accounts had not had a password change since 2007, and a large number of these dated to 1998. In addition, our analysis of the records provided, found approximately 40 of the 140 accounts listed as active users were shown as having never logged into the accounts. Further, we noted that many of these accounts contained some form of administrator[5] authority for selected areas or network operations.

[5] The term used for an account that has access privileges that a normal account would not be allowed to obtain. In most cases, for the system or network on which it is located, the administrator account could have almost unlimited authority.

Disabled Accounts Remain on Active Directory: As part of our analysis of user accounts, we noted that approximately 400 apparently disabled user accounts remained on the active directory. The records provided by OCIO showed that the accounts had never logged into the network. OCIO officials advised that a review will be conducted of these accounts this year.

Processes for Assigning Replacement and Initial Passwords[6]: We requested all FEC policies and operating procedures relating to this area for testing. However, we were advised by OCIO officials that the FEC does not have written policies or operating procedures for establishing initial account passwords or replacement passwords. OCIO officials stated that "When systems administrators (SAs) are notified, through the FEC System Access (FSA) system, that there is a need to establish an account, the SA then establishes an account with a generic password of his or her choosing; this is not recorded for security reasons. Then either through the new hire orientation program, or through the help desk, the person is instructed to change this password and it must be changed before access to the system is granted."

The absence of specific FEC policies and operating procedures prevents FEC from setting requirements for this important area. For example, as discussed below, we identified that a FEC issued default password had not been changed in six months. Because of the absence of appropriate controls in this area, we were able to obtain access to other contractor personnel email accounts using this default password.

Login Passphrase for Contractors: An audit report released by OIG, *2010 Follow-Up Audit of Privacy and Data Protection, Federal Election Commission, Audit Report Number OIG-10-03,* contained a finding related to access controls, the Inspector General stated, "We were informed by the Information Systems Security Officer that encrypted laptops assigned to contractors use an encryption passphrase assigned by the FEC. This is done to allow access to the information on the laptop if the contractor suddenly or unexpectedly departed the FEC. This process differs from that of FEC employees, who choose their own unique passphrase. Based on mobile devices assigned to contract auditors as part of another follow-up audit, it appears the same passphrase is used for all contractors. The passphrase assigned to contractors is not suitably complex, is relatively intuitive, and could be easily guessed or "hacked" by using basic password detection or "cracking" software. The lack of a unique secret passphrase for each

[6] These terms are used to describe that part of password administration (authentication controls) when a predetermined password is provided to a new user during initial login process and when replacement passwords are provided to existing users who are unable to login with an existing password (e.g. password is forgotten). We experienced difficulty in finalizing our audit testing of the policies, procedures and processes FEC follows when assigning replacement and initial passwords for users' network accounts. Because of the departure of a key OCIO official and other reasons, delays occurred in obtaining necessary documentation to enable us to complete testing for this area. However, based upon the information provided, we have identified areas where policies, procedures and processes are absent, or need improvement.

individual increases the risk that the data on that laptop could be accessed by an unauthorized individual."

We followed up on this issue and confirmed that the problem reported by the auditors in 2010 continued in 2012. For example, the same passphrase for contractor laptops has been used since 2009, and cannot be changed by the contractor. We agree with the prior auditors' conclusion that this weakness substantially negates the effectiveness of this control.

Remote Access: During our audit, we identified that FEC had recently purchased approximately 150 laptop computers for use by FEC employees. These laptops can be used to access the FEC system remotely when the employees are working offsite. We identified that these laptops currently are not configured to use two-factor authentication, as required by best practices and FEC policies.

Recommendations

5. Immediately implement government-wide requirements relating to strengthened password controls. Revise FEC policies and operating procedures to require the minimum best practices controls contained in FDCC and USGCB[7].

Agency Response

The Deputy CIO for Operations advised that the OCIO does not agree with this recommendation. The agency's password standard contains sufficiently strong password controls for the classification of this agency.

Auditor's Comments

FEC advised that the password controls for the agency are sufficient for the classification of this agency. However, government-wide best practices as established by OMB and endorsed by the council of CIOs require that passwords contain twelve characters. These controls are applicable to the risk rating of the FEC general support system.

6. Undertake a comprehensive review of user accounts that have been granted non-expiring passwords. Require certification from account owners detailing the need for non-expiring accounts, including the development of other alternatives, before reauthorizing the accounts' access. Develop FEC policies and operating procedures to implement this recommendation.

[7] Federal Desktop Core Configuration (FDCC) and United States Government Configuration Baseline (USGCB) are requirements that OMB have set for government-wide security settings directing agencies with Windows deployed operating system to adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS).

7. Whenever possible, require accounts with non-expiring passwords to be changed at least annually. Establish substantially more robust password requirements for accounts granted non-expiring passwords. Develop FEC policies and operating procedures to implement this recommendation.

8. Immediately terminate those accounts with non-expiring passwords that have not accessed their accounts within the last 12 months. Develop FEC policies and operating procedures to implement this recommendation.

Agency Response (Recommendations 6 through 8)

The Deputy CIO for Operations advised that the OCIO agrees in part with these recommendations. There are no user accounts that have been granted non-expiring passwords. The only accounts that have non-expiring passwords are accounts that have been established as administrative accounts or application accounts that need to be set up to run applications. These accounts are only accessible by systems administrators in the performance of "sys admin" duties. There are such accounts that have been established in the past that are no longer required, and we are reviewing these accounts for applicability. The operating procedures that are followed in this process are standard system administration functions performed by qualified system administrators. The account review will be completed by July 2013.

Auditor's Comments (Recommendations 6 through 8)

We continue to believe that the recommendations should be implemented by FEC, in total, based upon the problems noted with these accounts.

9. Remove the 400 disabled accounts noted during this audit by the end of the calendar year, and on a semi-annual basis conduct a review of the active directory to remove disabled accounts. Revise FEC policies and operating procedures to implement this recommendation.

Agency Response

The Deputy CIO for Operations advised that the disabled accounts remain in the list of accounts for historical purposes, and will be reviewed as part of the actions taken for recommendations 2-4.

Auditor's Comments

We continue to believe that the recommendation should be implemented by FEC based upon the problems noted with these accounts.

10. Strengthen controls over the establishment of initial and replacement (default) passwords, to include requiring that random passwords be used, and the default passwords used be changed monthly. Develop FEC policies and operating procedures to implement this recommendation.

Agency Response
The Deputy CIO for Operations advised that the OCIO disagrees with this recommendation. The FEC password standard is documented and followed by the FEC. The password standard is adequate for the security level of this agency.

Auditor's Comments
We continue to believe that the recommendation should be implemented by FEC based upon the problems noted with these accounts.

11. Research and fix the problem that enables use of a default password to access other contractor email accounts.

Agency Response
The Deputy CIO for Operations advised that the OCIO agrees with this recommendation. FEC will research this issue, but policy dictates that each contractor that requires an email account has a unique password.

Auditor's Comments
Since the FEC agreed to this recommendation, we have no additional comments.

12. Establish procedures that require contractors to create their own unique login passphrase.

Agency Response
The Deputy CIO for Operations advised that the OCIO agrees with this recommendation. The FEC will research this recommendation to ensure that all FEC policies are applied equally, unless a unique exemption is documented.

Auditor's Comments
Since the FEC agreed to this recommendation, we have no additional comments.

13. Require all employees and contractors with remote access to FEC's networks to comply with the dual-factor authentication requirement for their FEC laptop, as federal and FEC policies mandate.

Agency Response
The Deputy CIO for Operations advised that the OCIO agrees with this recommendation. The FEC does require all employees and contractors to comply with dual factor authentication. The agency requires a password and a secure key or HSPD-12 ID to affect dual authentication. The agency is currently in transition from secure key to HSPD-12 ID's and expects to complete the transition by March 2013.

Auditor's Comments

While FEC officials agreed with this recommendation, and stated that the agency requires dual factor authentication, FEC currently has up to 150 laptops in service that currently do not have dual factor authentication and can remotely access the FEC network.

C. A System to Recertify Users Access Authorities is Needed

FEC has not developed an effective process to periodically review user access authorities by the users' supervisors, even though agency officials agreed to implement this recommendation in response to our 2009 financial statement audit. Auditing standards required our follow up on the actions taken by FEC to address this problem. FEC officials indicated that a new approach to implementing this control process would be associated with the FEC's "Livelink" project. However there was no documentation provided to support that this process was being implemented into "Livelink," and we were advised that "Livelink" was never meant to provide a means for users' supervisors to review their employees' access authorities.

In meetings with the CIO and Deputy CIO for Operations we were advised that the FEC still had not developed a method for performing periodic reviews of user access authorities. The CIO indicated that this project was one that the FEC wanted to implement, and when the new CISO was on board the OCIO would again address this project. FEC is at unnecessary risk, and is not in compliance with best practice control processes and its own policies. Without periodically performing a review of user access authorities, FEC officials do not have assurance that users only have access to information and information systems that are necessary to accomplish job responsibilities, resulting in a recent incident of an FEC employee having unauthorized access to information on network files.

Recommendations

14. Establish an FEC policy that requires annual recertification of users' access authorities.

15. Review FEC current system capabilities in implementing recertification of user access authorities. Develop and document a detailed project plan based on management's review, and assign sufficient resources to this project so that it can be completed on or prior to June 2013.

Agency Response (Recommendations 14 and 15)

The Deputy CIO for Operations advised that the OCIO disagrees with these recommendations. Annual recertification is not necessary and would be redundant with the procedures of the agency's FEC System Access system. All access requests and removals are recorded in the agency's FSA. Access remains in effect until the request for removal is submitted.

Auditor's Comments (Recommendations 14 and 15)

Since we first reported that FEC needed to perform a recertification of user access authorities, and made recommendations in our 2009 financial statement audit report, FEC officials have agreed to implement this recommendation. In a recent meeting in September 2012, senior agency officials confirmed that the agency intended to implement a recertification process. OCIO officials have now changed the agency's position and disagree with our recommendation. OCIO officials advised that the FSA system provides this recertification control, and a separate independent recertification of user access authorities would be redundant. However, there can never be full assurance that the FSA system will actually reflect the status of network users in active directory. The recertification of active users must come from the original controlling files – active directory. FSA does not provide an accurate snapshot of users' access authorities. For example, we identified five separated contractors listed as active users in the FSA system, and having access to FEC's network although they no longer worked for the FEC. We have noted similar problems with the system in prior audits. In addition, FSA allows FEC personnel who are not managers or supervisors to grant network access to other FEC staff. These requests are not required to be approved or reviewed by a supervisor and/or manager prior to granting access. Further, all managers and supervisors do not have access to FSA, and have not been trained on FSA in order to periodically review FEC personnel access authorities. Therefore, in its current state, FSA cannot be used as an accurate source for recertification of user's access authorities. Without such a control, FEC will continue to experience problems with separated personnel retaining network access as we have reported since our 2009 audit.

D. Certification and Accreditation Controls

FEC's Certification and Accreditation Controls need to be strengthened to ensure that appropriate IT security controls are in place and operating as designed. FEC has not performed a certification review of its key medium risk GSS since December 2008. In addition, our review of FEC IT policies identified that FEC needs to strengthen FEC policy 58.2.4, *Certification and Accreditation (C&A) Policy*, issued September 2004, to provide additional guidance on what decision points drive when a new C&A is required, and to provide specific documentation requirements to be maintained in order for the agency to track changes made to systems, and to make informed decisions on when major changes drive the need for a re-certification. OMB best practices require that a re-certification review be performed at least every three years.

FEC performed a certification of its general support system, using NIST SP 800-53 as guidance, and issued a security controls assessment report (SCAR) in December 2008. The CIO accredited the system in January 2009 with authority to operate until January 15, 2010. The SCAR identified a significant number of high and medium risks, and FEC developed a corrective action plan to address

most weaknesses. Some of the weaknesses FEC decided not to implement because the agency is "exempt from FISMA."

We discussed the importance of C&A controls, the status of a new C&A on the GSS, whether the certification would follow NIST guidelines, and the date the certification would take place with the prior CISO and the Deputy CIO for Operations. We also requested information on how the agency determined when changes made to the GSS, individually or in aggregate, modified or upgraded the system in a way that impacted information security and assurance, and therefore warranted a new C&A. We were advised that the agency is planning to perform another C&A, but a date has not been set, and a decision has not made on whether the agency would use NIST SP 800-53 as the guidance document. In addition, OCIO officials were unable to provide information as to how the agency made determinations that changes to the GSS met the FEC standard that would require another C&A.

Recommendations

16. Revise FEC policies to: require a certification of its systems at least once every three years.

Agency Response

The Deputy CIO for Operations advised that the OCIO does not agree with this recommendation. Recertification is addressed in policy 58-2.4. FEC performed the Certification and Accreditation of systems pursuant to the first iteration of NIST SP 800-37 which recommended continuous monitoring of selected security controls, plus comprehensive testing of all security controls and reauthorization every three years. However, the new framework (NIST SP 800-37 rev1, Risk Management Framework) provides a more dynamic approach which leverages robust continuous monitoring to support on-going authorization and risk management as part of a more steady state, less cyclical process. The FEC is investigating this as an option.

Auditor's Comments

The OCIO is correct that the risk management framework discusses a robust continuous monitoring framework, similar to the recommendations that we have been making since our 2009 audit report. FEC has not performed a complete assessment of the GSS, either through continuous monitoring or as a periodic assessment since the first assessment was completed in December 2008, almost four years ago. OMB Circular A-130, Appendix III, provides that agencies should "review the security controls in each system when significant modifications are made to the system, but at least every three years."

17. Perform a re-certification of the GSS using NIST SP 800-53 as review criteria within this calendar year.

Agency Response

The Deputy CIO for Operations advised that the OCIO disagrees with this recommendation. Recertification of any FEC system will be performed in accordance with policy 58-2.4

Auditor's Comments

FEC policy 58-2.4 is in need of substantial revision. The FEC policy discusses that all FEC major applications and general support systems shall be re-certified/re-accredited when modified or upgraded in a way that impacts information security and assurance, or in response to changes in the risk environment. However, when we inquired as to how the agency determines, individually and in aggregate, when system modifications or upgrades impacted the system's security, OCIO officials were unable to provide a meaningful response. In addition, when we requested documentation of such reviews and decisions on system changes, such as the changes made for the FEC System Access module, or the changes made for the Enterprise Content Management, OCIO officials were unable to provide any documentation of such analyses.

We continue to believe that a new security assessment, completed in accordance with the NIST SP 800-37, Risk Management Framework, needs to be completed as soon as possible.

18. Strengthen FEC Policy 58.2.8 so that it provides additional guidance on what decision points drive when a new C&A is required; and specific documentation requirements that need to be maintained in order for the agency to track changes so it can make informed decisions on when major changes drive the need for a re-certification.

Agency Response

The Deputy CIO for Operations advised that the OCIO agrees in part. The FEC is in consultation with the Department of Commerce will obtain lessons learned and perform a cost-benefit analysis on potentially implementing the new recommendation by NIST in lieu of prior Certification and Accreditation recommendation. FEC does not have a startup, or finish date to implement the new Risk Management Framework due to unknown cost at this time. However, FEC hopes to implement in fiscal year 2014, if funding is available.

Auditor's Comments

While agency officials agreed with the recommendation, in part, we believe that the problems discussed in this report support the recommendation. Without full adoption of the recommendation, FEC information and information systems will remain at high risk.

E. Vulnerability Scanning

Problems related to FEC's vulnerability scanning[8] program reported in our 2011 and prior audit reports have not been addressed by FEC. While the FEC had established a vulnerability scanning program; the program did not meet best practices in several key areas. For example, individual workstations were excluded from the scanning process – a significant omission, and vulnerabilities identified in the components of the general support system that were scanned, were not mitigated timely.

We identified that about 60 percent of the 250 vulnerabilities identified in the agency's 2012 scanning report had also been identified in scans performed by the agency in 2011. In addition, we continued to find that improvements are needed in the agency's patching system[9]. For example, about 65 percent of the vulnerabilities identified in the agency's 2012 scan results related to outdated versions of software or inadequate patching of systems. These vulnerabilities would have been mitigated had FEC implemented an effective patch management program.

Recommendations

19. Include all components of the general support system, including workstations, into the organization's vulnerability/security scanning process and ensure that the general support system in its entirety is assessed at least annually.

Agency Response

The Deputy CIO for Operations advised that the OCIO agrees in part with this recommendation. All components of the general support system, including workstations have been recently scanned for vulnerability and security. The report of this scanning will be available in November and the confidential results will determine the frequency of future scans. The OCIO disagrees on the need for a semi-annual assessment. Frequency of vulnerability scanning will be determined based upon results of scan and available resources and funding.

[8] NIST controls for a vulnerability scanning program include: performing scans for vulnerabilities in the information system and hosted applications on a periodic basis; checklists and procedures for the scanning program; processes for analyzing vulnerability scan reports; and processes for remediating legitimate vulnerabilities.

[9] NIST defines patch management as the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they are mitigating software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation. Also, patches are usually the most effective way to mitigate software flaw vulnerabilities, and are often the only fully effective solution.

Auditor's Comments

Because of the number and age of the vulnerabilities identified in agency scans, and the exclusion of workstations from periodic scans, we continue to believe that this recommendation should be implemented.

20. Implement procedures to ensure that scan results are subject to a "root cause" analysis to ensure that remediation actions address technical as well as organizational processes and procedures.

Agency Response

The Deputy CIO for Operations advised that the OCIO disagrees with this recommendation. The agency's current processes contained in Directive 58-2.1 addresses root cause analysis, and it's role in mitigation techniques.

Auditor's Comments

While FEC policy 58-2.1 provides "This policy takes into consideration: Threat/vulnerability identification and root cause analyses," our 2012 and prior audit tests found that these analyses were not effectively performed. For example, our 2010 and 2011 audit reports identified that a large number of vulnerabilities that were identified by the agency were related to outdated software and inadequate patching. We also noted that many of the issues had been included in more than one scanning report. A "root cause" analysis of the scanning results would have identified that the FEC's patch management system was not working properly, and that additional corrective actions were necessary.

21. Strengthen controls to ensure that vulnerabilities identified through the vulnerability scanning tests are remediated within 30 days, or document acceptance of these risks.

Agency Response

The Deputy CIO for Operations advised that the OCIO agrees in part with this recommendation. The FEC will address level 1 threats, within the 30 day requirement. Threats of a lesser nature will be dealt with as soon as possible depending on staff and budget restrictions. The policies and procedures established in Directive 58, address all this recommendation, and are deemed to meet the requirements of the FEC.

Auditor's Comments

FEC officials agreed in part with this recommendation. While FEC officials plan to address more significant threats within 30 days, the officials did not provide a timeframe for completing other risks identified in the agency scans. We believe that the agency directives are in need of revision, and should address the problems noted in this report.

F. Configuration Security Controls and FDCC/USGCB Requirements

While FEC has incorporated workstations into the change management[10] framework which addressed a problem we identified in our prior audits, the agency's change management process relies on the manual recording of all system changes in an outside application. As reported in our 2011 audit, there was no effective process in place to identify all changes to the configuration of FEC's system, and no logs identifying changes to the system are collected. Therefore, there is reduced assurance that all changes are processed under the agency's change management framework, or that changes made outside the framework will be identified.

In addition, while FEC has issued configuration baseline standards for a number of its systems, these standards have not been fully implemented for the computers we tested. We compared the FEC provided configuration settings to several laptop computers, and identified that the baseline configuration standards were not fully implemented for any of the computers we tested. For workstations and configuration standards tested, we identified that 5 of the 15 baseline configuration standards settings had not been implemented. We also noted that two of the configuration settings could be changed by the user, as users were provided administrative rights to the local machine. The current FEC baseline configuration standards require that on Windows XP machines the "administrator account" be renamed and that access to administrator authorities is limited to only those users requiring such access. However, based on the computer settings we reviewed, users had been given administrator rights allowing them to change local settings.

As we have reported since our 2009 audit, FEC has not fully implemented security control requirements that OMB mandated in 1997 for Windows computers. FEC has established a project to adopt "selected" control requirements, and estimates that full implementation of "selected" controls will not be implemented until the end of 2012. Our tests found the following non-compliant requirements that can be easily implemented and strengthen FEC's network:

[10] The objective of change management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service. Changes in the IT infrastructure may arise reactively in response to problems or externally imposed requirements, e.g. legislative changes, or proactively from seeking improved efficiency and effectiveness or to enable or reflect business initiatives, or from programs, projects or service improvement initiatives. Change Management can ensure standardized methods, processes and procedures which are used for all changes, facilitate efficient and prompt handling of all changes, and maintain the proper balance between the need for change and the potential detrimental impact of changes.

Access Control Objective	FEC Settings	FDCC Requirements	Meets or exceed OMB Requirements
Enforce password history	5 passwords	24	No
Maximum password age	180 days	60	No
Minimum password age	0 days	1	No
Minimum password length	8 characters	12 characters	No

Recommendations

22. Implement baseline configuration standards for all workstations.

23. Fully implement USGCB/FDCC standards and perform scanning of Internet Explorer configuration settings.

Agency Response (Recommendations 22 and 23)
The Deputy CIO for Operations advised that the OCIO agrees with these recommendations. The FEC is in the process of implementing baseline configuration. The CIO estimated the completion date as the summer 2013.

Auditor's Comments (Recommendations 22 and 23)
Since the agency agreed to implement these recommendations, we have no additional comments.

24. Implement logging of all configuration changes and review logs regularly to ensure that all system changes, including changes to workstations, are processed through the change management framework.

Agency Response
The Deputy CIO for Operations advised that the OCIO believes that the current processes are in compliance with the recommendation. All change management processes are logged and maintained by the Change Advisory Board.

Auditor's Comments
While the current GSS security plan states that an automated system logging of configuration changes is in place for network components, our audit tests determined that FEC personnel had not been consistently reviewing the system logs. Instead, we found that FEC's current change management process relies on a manual process in which personnel are to record configuration changes into a tracking system. However, there is no process in place to compare the system logs being generated on these network components to those configuration changes recorded in the manual tracking system. A comparison would identify configuration changes that were made outside the current change management process, and also reveal policy

deviations. Further, based on the FDCC/USGCB evaluation performed by the agency, the system logging capabilities available on the workstations have not been implemented. Therefore, there is no assurance that all changes are identified and managed through the Change Advisory Board, and the current change management framework.

G. Personnel Security Controls

Follow up on the actions taken by FEC to address recommendations in our 2011 report identified the following unresolved personnel security control issues:

- While improvements were noted in controls related to separated FEC employees, we did note that for five FEC employees tested, one was not removed within the one day requirement established in FEC procedures. The employee's network access was terminated seven days after separation.

- Our tests of FEC contractors who had access to FEC's network showed five separated contractor employees were listed in the FEC System Access (FSA) system as active users indicating weaknesses in the agency's main application for tracking employees/contractors network access.

Recommendations

25. Review the conditions that caused the employee to retain network access beyond the FEC's standard, and strengthen controls as appropriate.

Agency Response

The Deputy CIO for Operations advised that the OCIO has reviewed the condition and it was due to the nature of the person's position. The employee was allowed to retain access beyond the FEC's standard due to a human bypass of FSA policy. The employee was allowed to exit the agency without completing the FSA process. The FSA process and policy was put in place to preclude any human intervention.

Auditor's Comments

We are uncertain of the agency's response to this recommendation. However, we continue to believe an analysis of the problems that continue to impact the prompt removal of network access for separated personnel needs to be performed. We have reported problems related to continued network access for separated personnel since our 2009 audit report, and the prior financial statement auditors reported similar problems in their 2008 audit report.

26. Review the FSA database and remove those personnel shown as current employees or contractors who have departed the agency.

Agency Response

The Deputy CIO for Operations advised that the OCIO disagrees with this recommendation. To maintain historical records, employees that have departed will be kept in the system even though their access rights are disabled.

Auditor's Comments

The agency's response does not address our recommendation. Contractors listed in FSA as currently on-board had, in fact, separated, in some cases years ago. We continue to believe that the FEC should implement this recommendation to reduce the risk of unauthorized access.

H. Oversight and Monitoring of IT Corrective Actions

FEC has not timely implemented actions necessary to remediate identified weaknesses in IT controls, some of which were first reported in 2008. We reviewed financial statement audit reports along with other reports issued since 2008 to determine whether the FEC has timely and effectively implemented controls on weaknesses that FEC officials agreed to correct.

The results of our review of open financial statement audit recommendations are discussed in detail in Attachment 1.

Recommendations

27. Review all outstanding audit recommendations contained in the agency's financial statement audit reports, and develop a current, detailed, time-phased corrective action plan (CAP) for each audit finding and recommendation.

Agency Response

The Deputy CIO for Operations advised that the OCIO disagrees with this recommendation since there is already an agreement in place with OIG that CAP's are updated twice per year in May and November.

Auditor's Comments

Management's May and November CAP updates have been required by Commission Directive 50: Audit Follow-up since 2006, and are not the result of "an agreement in place with the OIG…." In addition, the CAP updates have not resulted in resolution of outstanding financial statement audit recommendations that have been reported since 2009. The FEC continuously fails to meet implementation due dates, and to adequately monitor and resolve outstanding audit recommendations. Failure to adequately plan and develop useful and achievable corrective actions, results in repeat audit findings being reported for several years. For example, concerning the periodic recertification of users' access authorities, FEC has not yet implemented this recommendation even though the agency agreed with the recommendation in

their response to the 2009 financial statement audit. We continue to believe that this recommendation should be implemented.

28. Modify key officials' position descriptions and rating elements to include, as a critical element, the timely completion of corrective action plans.

Agency Response

The Deputy CIO for Operations advised that the OCIO disagrees with this recommendation. Completion of CAP's is not appropriate for inclusion into a key official's position description and is not a critical element.

Auditor's Comments

We have identified a significant number of problems that remained uncorrected, in many cases since 2009. In addition, the OIG's report, *Review of Outstanding Audit Recommendations*, dated June 2012, reported issues with timely completion of corrective actions.

We disagree that it is not appropriate for timely completion of agreed upon corrective actions to be included as a rating element for applicable FEC officials. As OMB Circular A-50, *Audit Followup,* provides, "Audit followup is an integral part of good management, and is a shared responsibility of agency management, officials, and auditors. Corrective action taken by management on resolved findings and recommendations is essential to improving the effectiveness and efficiency of Government operations." Because of the problems noted, we continue to believe that this recommendation should be implemented.

29. Develop a tracking process that would include monthly reports to the CIO, highlight key tasks that may or have miss(ed) target dates, and assign one key OCIO official as responsible for monitoring OCIO corrective action plans.

Agency Response

The Deputy CIO for Operations advised that the OCIO agrees in part with this recommendation. OCIO will review CAP's on a monthly basis at the weekly OCIO management meetings.

Auditor's Comments

The issues included in this report support that this recommendation should be fully implemented by FEC.

I. Testing and Exercise FEC's COOP

During fiscal year 2011, FEC completed most of the last phase of its multi-year plan to implement a Continuity of Operations Plan (COOP) document. However, FEC has not yet fully tested and exercised the COOP – a critical element in development of a comprehensive and effective plan. FEC's planning documents

showed the agency was to have completed necessary testing and exercise by July 2011. FEC officials advised that the delay was due to the illness of a key project team member, and that completion of testing was deferred until approximately the beginning of calendar year 2012. As of September 2012, testing has not been completed.

At the beginning of our 2012 audit, we requested documentation from FEC officials to enable us to determine whether the FEC COOP had been appropriately tested, and whether the tests and related documentation met FEC's policies and Federal Continuity Directive No. 1 requirements for testing. We were initially advised by OCIO personnel that no documentation was available related to COOP testing. Subsequently, some FEC COOP test planning and related documents were located and provided. We were unable to determine from these documents whether FEC met either its own testing requirements, or the federal requirements that are applicable to the agency.

The table below lists key federal requirements, and whether documentation provided enabled us to conclude whether FEC was in substantial compliance with these requirements.

FCD[11] No. 1, Appendix K	Auditor's Comments
Annual testing of alert, notification, and activation procedures for continuity personnel and quarterly testing of such procedures for continuity personnel at agency headquarters.	No documentation provided to show that this requirement was met.
Annual testing of plans for recovering vital records (both sensitive and non-sensitive), critical information systems, services, and data.	Some documentation was provided to show that critical information systems were tested.
Annual testing of primary and backup infrastructure systems and services (e.g., power, water, fuel) at alternate facilities.	No documentation provided to show that this requirement was met.
Annual testing and exercising of required physical security capabilities at alternate facilities.	No documentation provided to show that this requirement was met.
Testing and validating equipment to ensure the internal and external interoperability and viability of communications systems, through monthly testing of the continuity communications capabilities.	No documentation provided to show that this requirement was met.
An annual opportunity for continuity personnel to demonstrate their familiarity with continuity plans and procedures and to demonstrate the agency's capability to continue its essential functions.	No documentation provided to show that this requirement was met.

[11] Federal Continuity Directive (FCD) No.1, Federal Executive Branch National Continuity Program, Appendix K, Test, Training and Exercise, was issued by the Department of Homeland Security to guide federal agencies in the development of COOP documents.

FCD[11] No. 1, Appendix K	Auditor's Comments
An annual exercise that incorporates the deliberate and preplanned movement of continuity personnel to an alternate facility or location.	No documentation provided to show that this requirement was met.
An opportunity to demonstrate that backup data and records required supporting essential functions at alternate facilities or locations are sufficient, complete, and current.	Some records were available to show some aspects of this requirement were tested.

Because the documentation provided was insufficient to support that FEC met these federal requirements or addressed the issues reported in our 2011 audit report, this problem remains open and requires further review and corrective action by FEC personnel.

Recommendations

30. Ensure that sufficient resources are assigned to timely complete the testing of FEC's COOP in order to reduce risk to the FEC.

Agency Response

The Deputy CIO for Operations advised that the OCIO agrees with this recommendation. In accordance with Annex A of HSPD 20, the FEC is a category 4 agency. The agency COOP is sufficiently tailored to appropriate level of preparedness for a Cat 4 agency. The COOP is more aptly aimed at providing guidance for continuity after an incident at a local agency level, affecting only this agency. The testing completed and documented and results provided as a PBC item.

31. Ensure that appropriate documentation is retained as required by FCD No. 1 to support that FEC has met all applicable federal testing requirements.

Agency Response

The Deputy CIO for Operations advised that the OCIO agrees with this recommendation. The FEC has met all TT&E requirements for a category 4 agency in accordance with internal IT policies and directives. Management deems that policies and testing of those policies, directives, COOP and DR plans are commensurate with the risk analysis appropriate for this agency.

32. Develop a detailed POA&M to ensure that required COOP testing and exercises are completed as soon as possible.

Agency Response

The Deputy CIO for Operations advised that the OCIO disagrees with this recommendation and the OCIO believes the COOP testing is complete and CAP submitted as a PBC.

Auditor's Comments (Recommendations 30 through 32)

Documentation provided by FEC was analyzed and did not meet federal requirements. Therefore, we continue to believe that the recommendations should be implemented by FEC.

COMPLIANCE WITH LAWS AND REGULATIONS

The results of our tests of compliance with certain provisions of laws and regulations, as described in the Responsibilities section of this report, disclosed no instance of noncompliance with laws and regulations that is required to be reported under *Government Auditing Standards* and OMB Bulletin 07-04, (as amended).

AGENCY RESPONSE AND AUDITOR COMMENTS

FEC management responded to the draft report in a memorandum dated November 9, 2012, which indicated that the agency responses to each recommendation are included in the body of this report. We have included their comments and our response after each recommendation. FEC also noted in their response that they believe "that such an extensive IT concentrated audit is perhaps not appropriate" as part of the financial statement audit.

As we have previously discussed with FEC officials, *Government Auditing Standards* require us to perform testing of agency IT systems that could have a direct and material effect on the audited agency's financial controls and/or financial statement presentation, or disclosures. Therefore, we continue to believe our audit testing of IT controls was appropriate.

The FEC's written response to the significant deficiency identified in our audit was not subjected to the auditing procedures applied in the audit of the financial statements and accordingly, we express no opinion on it.

DISTRIBUTION

This report is intended solely for the information and use of the management, the FEC Board, the Office of Inspector General, and others within the FEC, OMB, and Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Leon Snead & Company, P.C.
November 14, 2012

Audit Reports	Finding	Recommendation	FEC Responses[12]	Background Information/Current Status
2008-2012 FEC Financial Statement Audit Reports	Configuration Management FDCC/USGCB	Ensure that FEC baseline configuration standards are implemented in accordance with FDCC requirements for all workstations.	FEC generally agreed to implement recommendations in its response to our 2009 audit.	**Remains open.** First reported in our 2009 audit report. We found in our 2012 audit that according to FEC scans, the agency has implemented a large percentage of FDCC requirements. However, several key controls that would be easily implemented have not been implemented by FEC relating to password strength and related areas. Also, the FDCC and USGCB contain control settings for Internet Explorer. We were advised that FEC does not scan for these settings.
		Perform periodic assessments of baseline configuration settings as part of FEC's continuous monitoring program.	FEC generally agreed to implement recommendations in its response to our 2010 audit.	**Remains open.** First reported in our 2010 audit report. We found in our 2012 audit that the problems remain essentially the same as we reported in 2010.
	Vulnerability Scanning	Include all components of the general support system, including workstations, into the organization's vulnerability scanning process to ensure that the general support system, in its entirety, is periodically assessed.	FEC generally agreed to implement recommendations in its response to our 2009 audit. However, FEC added that the agency needed to implement portions of FDCC it agreed to adopt prior to implementing this recommendation.	**Remains open.** First reported in our 2009 audit report. We found in our 2012 audit that the problems remain essentially the same as we reported in 2009. FEC officials advised us that they have recently completed scanning of the FEC's network. However, we have not reviewed the scanning process or the scanning reports.

[12] FEC responses are briefly summarized for presentation. Where FEC disagreed with a recommendation, or significant portions of a recommendation, we show that information. However, when in our opinion, the FEC response is in general agreement with the recommendations we did not include minor points.

Audit Reports	Finding	Recommendation	FEC Responses[13]	Background Information/Current Status
	Personnel Security and Access Controls	Implement additional controls to ensure that former employees' access to the network is terminated in accordance with FEC policies.	FEC generally agreed to implement recommendations in its response to our 2009 audit.	**Remains open.** Issue first reported in 2008 audit report. While we found improvements in this control from the significant problems noted in our 2011 audit, we noted that one sampled individual was removed untimely, and five separated contractor employees were listed in the FEC System Access (FSA) system as active users indicating weaknesses in the agency's main application for tracking employees/contractors network access.
		Assure sufficient resources are provided to complete the project dealing with the establishment of processes to enable periodic review of users' access authorities.	FEC in its response generally agreed to implement the recommendations in this area in our 2009 audit report.	**Remains open.** First reported in our 2009 audit report. We found in our 2012 audit that the problems remain essentially the same as we reported in 2009.
	Security Awareness Training	Revise FEC procedures to require that all new personnel and contractors take the security awareness training, and acknowledge rules of behavior prior to being granted access to FEC systems.	First reported in our 2010 audit report. Management partially agreed with recommendations, and provided alternative process. We agreed to this alternative process as a way of remediating the issue.	**Remains open.** Completion of the security awareness training was delayed until after our scheduled field work completion date, and was not tested during this year's audit. Security awareness training was included as a problem area in our 2011 audit report.
	COOP Development and Testing	Multiple recommendations were made on this area since our 2009 audit report, and it was reported in the predecessor auditor's 2008 audit report.	FEC management concurred with our recommendation that the COOP be completed and fully tested by the end of 2010 calendar year.	**Remains open.** Over the five years, FEC has developed the COOP and implemented portions of a testing, training, and exercise (TTE) program required by FCD No. 1, Appendix K. However, documentation of test plans, test results, and analysis of test results was not sufficient to enable us to conclude that FEC met the federal requirements for TTE of its COOP.

[13] FEC responses are briefly summarized for presentation. Where FEC disagreed with a recommendation, or significant portions of a recommendation, we show that information. However, when in our opinion, the FEC response is in general agreement with the recommendations we did not include minor points.

Attachment 2

Status of Prior Year Recommendations

Rec. No.	Recommendation	Status As of September 30, 2012
1.	Continue to work with NFC and GSA so that the two service provider's systems can be interfaced according to the current timeline.	Recommendation closed.
2.	Develop a time-phased corrective action plan to convert the manual accounts receivable process to an automated and integrated system.	Recommendation closed.
3.	Implement baseline configuration standards for all workstations and require documentation and approval of any deviations from this standard.	Recommendation open.
4.	Fully implement USGCB/FDCC standards.	Recommendation open.
5.	Implement logging of configuration changes to ensure that all system changes are processed through the change management framework.	Recommendation open.
6.	Include all components of the general support system, including workstations, into the organization's vulnerability scanning process.	Recommendation open.
7.	Implement procedures to ensure that scan results are subject to a "root cause" analysis to ensure that problems are fully resolved.	Recommendation open.
8.	Develop a process to ensure that vulnerabilities identified through scanning are documented in a corrective action plan, and monitored to ensure timely remediation.	Recommendation open.
9.	Establish and publish a policy that requires annual recertification of users' access authorities.	Recommendation open.
10.	Assure sufficient resources are provided to the document and records management system (Livelink) so that it can be completed no later than June 2012.	Recommendation closed. This recommendation was rolled into Recommendation 9 since LiveLink is no longer being used for this purpose.
11.	Validate all active users to assure that only individuals who are currently and properly authorized have access to FEC's information and information systems.	Recommendation open.
12.	Analyze the reasons separated personnel retained access to FEC systems, and develop additional controls to ensure that FEC timely removes access for individuals who leave the agency.	Recommendation open.
13.	Establish controls that would automatically suspend an individual's network access if security awareness training is not completed within required timeframes.	Recommendation open.
14.	Ensure all personnel and contractors that have not yet taken the security awareness training complete it within the next 30 days.	Recommendation open.
15.	Ensure that sufficient resources are assigned to the task of testing the COOP in order to reduce the risks to FEC operations.	Recommendation open.

Rec. No.	Recommendation	Status As of September 30, 2012
16.	Develop specific control processes and issue operational policies that establish automated control procedures to ensure that FEC uses software and associated documentation in accordance with contract agreements and copyright laws.	Recommendation closed.
17.	Restrict network folders & subfolders containing copyright applications and software to only authorized users based on the operational policies developed and implemented.	Recommendation closed.
18.	Review all folders and files on the "userinstall" network folder, and remove all applications and data that are not current, or do not meet the specific operational purposes of this folder.	Recommendation closed.
19.	Formally adopt the NIST IT security controls established in FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, and SP 800-53, Recommended Security Controls for Federal Systems and Organizations.	Recommendation open.
20.	Require FEC contractors to adhere to the FAR related IT controls when providing services to the FEC to ensure sufficient controls are in place to meet best practices.	Recommendation open.

THE FEDERAL ELECTION COMMISSION
Washington, DC 20463

November 9, 2012

MEMORANDUM

TO: Leon Snead and Company

FROM: Judy Berning
Acting Chief Financial Officer

Judy Berning
Digitally signed by Judy Berning
DN: cn=Judy Berning, o=OCFO, ou=OCFO, email=jberning@fec.gov, c=US
Date: 2012.11.09 13:31:11 -05'00'

SUBJECT: Management Responses to Audit Findings

Please find attached the management responses to the audit findings as provided in the draft document sent by the Office of the Inspector General on November 6, 2012.

Please contact me at X1230 should there be additional questions.

cc: Lynne McFarland, Inspector General
Alec Palmer, Staff Director
Tony Herman, General Counsel

Federal Election Commission

Fiscal Year 2012 Financial Statement Audit

Management Responses to Audit Findings

The Federal Election Commission has made significant strides in addressing findings and recommendations that arise through the annual financial statement audit. In FY 2012, the FEC fully resolved the significant deficiency related to internal controls over financial reporting and continues to address Information Technology (IT) security control needs identified that relate to Information Technology policies, practices and procedures. The Federal Election Commission's responses to the FY 2012 audit findings were provided in the draft document sent by the Office of the Inspector General on November 6, 2012.

The agency maintains the highest level of commitment to its information technology security and systems. Although the FEC is exempt from most of the requirements of the Federal Information Security Management Act (FISMA), the agency still incorporates many of FISMA's best practices. The FEC has in place directives and a corrective action plan that is reviewed twice a year to mitigate potential risk factors. The agency's financial management systems are provided by NFC and GSA under shared service agreements. The FEC receives and relies upon SSAE 16 audit reports to obtain assurance over financial applications provided by GSA and NFC.

The FEC has established 34 policies, 18 standards and 8 procedures to govern and define the agency's IT security program, following the guidance published by the National Institute of Standards and Technology (NIST), although the agency is exempt from many of those requirements. The FEC has concurred with a number of the recommendations provided by the audit, and will continue to implement those recommendations where economically and technically feasible and where such actions fit within the management framework of the agency. While the FEC requests budget funds to comply with applicable IT control standards, the FEC does not find it feasible to request additional funding to adopt FISMA requirements that Congress has exempted this agency from adhering to. The Office of the Chief Information Officer has incorporated many industry "best practices" in establishing the FEC's IT security and monitoring program.

A large portion of the findings and recommendations stemming from the Financial Statements Audit are concerned with the agency's Continuity of Operations Plan (COOP). The audit does not identify the FEC's category rating in the continuity of government plans. The FEC is a category 4 agency in the continuity of government plans which translates to the lowest priority for continuing agency operations in the event of a government-wide disruption of government services. Therefore, the FEC's approach to the COOP centers on an event that would affect FEC agency operations only, and does not address events affecting the government as a whole. An

example of this would be if the FEC's building alone became unavailable for use due to a building malfunction. This approach greatly reduces the scope of the COOP to FEC-specific mission functions. To further reduce the risk of FEC systems loss due to a building malfunction, the agency has recently completed the data center consolidation project to close down its internally operated data center and move it off-site to a certified contractor data center. Therefore, the FEC's COOP has been tailored to suffice in support of the agency's mission and responsibility to the government as a whole, as well as within the availability of resources (budget and personnel) as approved through the budget process.

Management's responses to each individual IT finding are contained within this report, with an explanation as to why the FEC may not agree with the finding. It is also noted that such an extensive IT concentrated audit is perhaps not appropriate under the guise of a Financial Statement Audit, and may dilute the objective of the audit.