FEDERAL ELECTION COMMISSION

OFFICE OF INSPECTOR GENERAL

FINAL REPORT

Audit of the Federal Election Commission's Fiscal Year 2011 Financial Statements

November 2011

ASSIGNMENT No. OIG-11-01

FEDERAL ELECTION COMMISSION
WASHINGTON, D.C. 20463
Office of Inspector General

MEMORANDUM

TO: The Commission

FROM: Inspector General

SUBJECT: Audit of the Federal Election Commission's Fiscal Year 2011 Financial Statements

DATE: November 14, 2011

Pursuant to the Chief Financial Officers Act of 1990, commonly referred to as the "CFO Act," as amended, this letter transmits the Independent Auditor's Report issued by Leon Snead & Company (LSC), P.C. for the fiscal year ending September 30, 2011. The audit was performed under a contract with, and monitored by, the Office of Inspector General (OIG), 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 applicable provisions of Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*, as amended.

Opinion on the Financial Statements

LSC audited the balance sheet of the Federal Election Commission (FEC) as of September 30, 2011, and the related statements of net cost, changes in net position, budgetary resources, and custodial activity (the financial statements) for the year then ended. The objective of the audit was to express an opinion on the fair presentation of those financial statements. In connection with the audit, LSC 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. The financial statements of the FEC as of September 30, 2010, were also audited by LSC whose report dated November 12, 2010, expressed an unqualified opinion on those statements.

In LSC's opinion, the financial statements 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 year ending September 30, 2011, in conformity with accounting principles generally accepted in the United States of America.

Report on Internal Control

In planning and performing the audit of the financial statements of the FEC, LSC considered the FEC's internal control over financial reporting (internal control) as a basis for designing auditing procedures for the purpose of expressing their opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the FEC's internal control. Accordingly, LSC did 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. According to the American Institute of Certified Public Accountants:

- 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 significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is a more than remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control.
- A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

LSC's consideration of internal control was for the limited purpose described in the first paragraph in this section and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. LSC did not identify any deficiencies in internal control that LSC would consider to be material weaknesses, as defined above. However, LSC identified, as listed below, two deficiencies in internal controls that LSC considers to be significant deficiencies.

- Internal Controls over Financial Reporting
- Information Technology (IT) Security Control Weaknesses

Report on Compliance with Laws and Regulations

FEC management is responsible for complying with laws and regulations applicable to the agency. To obtain reasonable assurance about whether FEC's financial statements are free of material misstatements, LSC performed tests of compliance with certain provisions of laws and regulations, noncompliance 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 No. 07-04, as amended. LSC did not test compliance with all laws and regulations applicable to FEC.

The results of LSC's tests of compliance with laws and regulations described in the audit report disclosed no instance of noncompliance with laws and regulations that are required to be reported under U.S. generally accepted government auditing standards or OMB guidance.

<u>Audit Follow-up</u>

The independent auditor's report contains recommendations to address deficiencies found by the auditors. Management was provided a draft copy of the audit report for comment and generally concurred with the findings and recommendations. In accordance with OMB Circular No. A-50, *Audit Follow-up*, revised, the FEC's corrective action plan is to set forth the specific action planned to implement the recommendations and the schedule for implementation. The Commission has designated the Chief Financial Officer to be the audit follow-up official for the financial statement audit.

<u>OIG Evaluation of Leon Snead & Company's Audit Performance</u>

We reviewed LSC's report and related documentation and made necessary inquiries of its representatives. Our review was not intended to enable the OIG to express, and we do not express an opinion on the FEC's financial statements; nor do we provide conclusions about the effectiveness of internal control or conclusions on FEC's compliance with laws and regulations. However, the OIG review disclosed no instances where LSC did not comply, in all material respects, with *Government Auditing Standards.*

We appreciate the courtesies and cooperation extended to LSC and the OIG staff during the audit. If you should have any questions concerning this report, please contact my office on (202) 694-1015.

Lynne A. McFarland

Lynne A. McFarland
Inspector General

Attachment

Cc: Alec Palmer, Staff Director/Chief Information Officer
Mary G. Sprague, Chief Financial Officer
Anthony Herman, General Counsel

FEDERAL ELECTION COMMISSION

Audit of Financial Statements

As of and for the Years Ended
September 30, 2011 and 2010

Submitted By

Leon Snead & Company, P.C.
Certified Public Accountants & Management Consultants

TABLE OF CONTENTS

<u>Page</u>

LEON SNEAD
& COMPANY, P.C.

Certified Public Accountants
& Management Consultants

416 Hungerford Drive, Suite 400
Rockville, Maryland 20850
301-738-8190
fax: 301-738-8210
leonsnead.companypc@erols.com

Inspector General
The Federal Election Commission

Independent Auditor's Report

We have audited the balance sheets of the Federal Election Commission (FEC) as of September 30, 2011 and 2010, 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, 2011 and 2010, 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 in internal controls over financial reporting, and 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, 2011 and 2010, 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, 2011 and 2010, in conformity with accounting principles generally accepted in the United States of America.

The information in the Management's Discussion and Analysis section is not a required part of the basic financial statements but is supplementary information required by accounting principles generally accepted in the United States of America or OMB Circular A-136, *Financial Reporting Requirements, revised*. We have applied certain limited procedures, which consisted principally of inquiries of FEC management regarding the methods of measurement and presentation of the supplementary information and analysis of the information for consistency with the financial statements. However, we did not audit the information and express no opinion on it. The Performance and Accountability Report, except for Management's Discussion and Analysis, is presented for the purposes of additional analysis and is not a required part of the basic financial statements. Such information has not been subjected to the auditing procedures applied in the audit of the basic financial statements and, accordingly, we express no opinion on it.

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, 2011 and 2010, in accordance with auditing standards generally accepted in the United 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 significant 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 control deficiency, or combination of control deficiencies, 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 certain deficiencies in internal control that we consider to be significant deficiencies.

Findings and Recommendations

1. Internal Controls over Financial Reporting

a. Controls over Disbursements Needed Strengthening

Office of the Chief Financial Officer (OCFO) personnel incorrectly paid current year expenses with prior year funds. We attributed this problem to OCFO personnel who bypassed established internal controls. As a result, FEC was not in compliance with federal regulations.

Title 31 U.S.C. §1502 (a) provides that, "The balance of an appropriation or fund limited for obligation to a definite period is available only for payment of expenses properly incurred during the period of availability or to complete contracts properly made within that period of availability and obligated consistent with section 1501 of this title. However, the appropriation or fund is not available for expenditure for a period beyond the period otherwise authorized by law." OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*, revised, also provides guidance in this area.

During our audit, we selected a statistical sample of 45 expense transactions and performed audit tests to ensure the propriety of the transactions. Our tests found that three of the transactions were not processed in compliance with budgetary requirements and agency policies. The three payments, all relating to the same vendor, totaling approximately $11,500, were incorrectly processed to 2010 and 2009 fiscal year obligations instead of current fiscal year obligations.

OCFO officials concurred that a misclassification had taken place, researched and corrected the budget year classifications, and analyzed other payments as recommended in our interim Notice of Finding and Recommendation (NFR). OCFO officials also advised that additional training was provided to personnel to strengthen internal controls in this area.

Because we verified that the OCFO took action to implement the recommendations contained in our NFR, we are making no recommendations in this report regarding the correction of the misclassification error.

Agency Response

Management concurs, in part, that a misclassification occurred due to an administrative error. The error was due to a training issue rather than an employee bypassing internal controls. The amount was insignificant and had no impact on the financial statements. Of the $11,500 identified by the auditors, only $6,300 applied to the current year. The OCFO corrected the error before the end of the fiscal year, as recommended by the auditors. Since the auditors found no further issues with regard to this error, no other recommendations were made. Management does not concur with the finding that the error contributed to the significant deficiency for internal controls over financial reporting. Management believes that this error was insignificant and does not reflect a significant deficiency in the agency's internal controls.

Auditor Comments

We do not believe that the errors we identified were insignificant as FEC officials stated in their response. Based upon our assessment of these errors, we concluded that the weakness identified contributed to a significant deficiency in internal controls over financial reporting. We believe that violation of 31 U.S.C. 1502 which states that appropriations may be obligated or expended only during the period of availability specified by law is a significant issue. Documents we obtained as part of our testing showed that accounting personnel had voiced concerns about processing the transactions against prior year obligations. Despite these concerns, OCFO personnel overrode controls and improperly processed the payments to prior fiscal year obligations in order to use funding available in prior years.

FEC officials in their response stress that the errors noted were insignificant and had no impact on the financial statements. However, what must be considered is that OCFO personnel bypassed their established control procedures in order to improperly process payments. While we agree that the errors do not represent a misstatement in the financial statements, it should be noted that our statistical sample found an error rate of approximately seven percent for the transactions tested. FEC processed approximately 2,100 non-payroll expense transactions with an approximate dollar value of $17.6 million during FY 2011.

b. Manual Systems Introduce Unnecessary Risk

As of the end of the 2011 fiscal year, FEC had not converted its manual systems and processes to automated systems that are integrated or interfaced with the core accounting system. We attributed this problem to delays by FEC's service providers regarding the integration of the payroll system, and to FEC's position that manual systems regarding accounts receivable should not be converted. As a result, FEC accounts receivable and payroll systems remained at unnecessary risk, and are not in compliance with best practice control processes.

OMB Circular No. A-127, *Financial Management Systems*, revised, defines a core financial system as the system of record that maintains all transactions resulting from financial events. It may be integrated through a common database or interfaced electronically to meet defined data and processing requirements.

FEC uses a service provider (General Services Administration (GSA) - Pegasys) for its general ledger and core financial management system operations, and the National Finance Center (NFC) for payroll. The FEC also uses Excel spreadsheets and a PeopleSoft application to perform selected accounting operations. The financial management processes that still use significant manual operations include:

- Payroll Accounting. The NFC based payroll system does not interface with the Pegasys accounting system. FEC used a PeopleSoft application throughout FY 2011 that was no longer supported to perform limited accounting operations in order to process payroll transactions into the agency's accounting system. This process also required FEC to perform manual operations to reconcile the payroll data, and prepare standard vouchers to input the payroll data into its accounting system. As of October 2011, the agency has eliminated use of the PeopleSoft application.

  OCFO officials advised us that the FEC is working closely with NFC and GSA to integrate the NFC subsidiary system with Pegasys. The current timeline provides for these systems to be completely interfaced by March 2012.

- Accounting for Collections of Fines and Penalties. The accounting for accounts receivables within FEC consists of several manual operations. The OCFO receives accounts receivable information from three divisions within the agency in several formats including Excel, Law Manager (a legal case tracking application), and Word. After the data is received, the information is input into a spreadsheet for further manual processing. OCFO personnel use the information from the spreadsheet to prepare a standard voucher that is submitted monthly to the agency's service provider for posting to the general ledger. Collections received by FEC, however, are processed to the general ledger throughout the month when the payments are received. Therefore, only at the end of each month, after the standard voucher is posted to the general ledger, does the accounts receivable in the general ledger reflect an accurate balance.

Recommendations:

1. Continue to work with NFC and GSA so that the two service provider's systems can be interfaced according to the current timeline.

2. Develop a time-phased corrective action plan to convert the manual accounts receivable process to an automated and integrated system.

Agency Response

Management concurs that it is important for agencies to consider automating manual processes whenever it is appropriate and cost effective to do so. However, management does not agree with the auditor's interpretation of a financial management system. OMB Circular A-127, as revised in 2009, defines a financial management system as a system that "includes the core financial systems and the financial portions of mixed systems necessary to support financial management, including automated and manual processes, procedures, and controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions."

While the OCFO does have some manual steps in its financial process, the office has implemented compensating controls consistent with industry best practices to eliminate unnecessary risks.

The OCFO evaluated the GSA Accounts Receivable and Collection System (ARCS) and determined that the system could not be utilized for FECA receivables because it does not allow the customization needed to meet the individual needs of the offices that enforce FECA debts.

The Accounts Receivable balance is immaterial to the FEC's financial statements and the volume of transactions is minimal. The expense of migration to an automated process is currently not in the best interest of the FEC or the Federal Government because it is not cost effective. The cost-effectiveness criterion is consistent with the GAO's Report on Financial Management Systems (GAO-09-328), the testimony of OMB Controller before Congress on April 14, 2010, the draft of A-127 circulated October 15, 2010, and the OMB Memorandum M-11-29 Chief Information Officer Authorities, issued August 8, 2011.

As it relates to the payroll accounting, the OCFO verifies NFC data, independent of the PeopleSoft application, before submitting to GSA. The FEC is working closely with NFC and GSA on the integration of the payroll system with the GSA Pegasys accounting system. Additionally, the FEC is working on an Oracle upgrade project to replace the PeopleSoft application. These projects are expected to be completed during FY 2012.

Auditor Comments

We continue to believe that it is important for FEC to convert its manual processes to automated systems that are integrated or interfaced with the core accounting system. It should be noted that this problem was reported by our predecessor auditors as part of a material weakness in their 2008 audit report. While the agency has made progress in correcting this past material weakness, the importance of eliminating manual systems or systems that do interface with the general ledger can be seen by the recent failure of its PeopleSoft application. A problem we and the prior auditors had identified for a number of years.

FEC officials cite a GAO report to support their position that systems do not need to be standardized and integrated. In fact, the report cited addresses problems with the lack of standardization and integration of financial systems. For example, the report cites, "Over a number of years, we have reported that modernizing federal financial management systems has been a challenge at many federal agencies due, in part, to the past practices of each federal agency attempting to implement its own systems which have all too often resulted in failure, have been delayed, and cost too much. Recognizing the seriousness of this problem, in March 2004, the Office of Management and Budget (OMB) launched the financial management line of business (FMLOB) initiative, in part, to improve the outcome of government wide financial management system modernization efforts and provide timely and accurate data for decision making through the use of more cost-effective shared service solutions. Under this approach, agencies are to consider the use of certain shared service providers for meeting common support services, such as information technology (IT) hosting and application management, rather than investing in costly and redundant agency-specific solutions."

We continue to disagree with management's conclusions as to the significance of the agency's accounts receivable and collections system. FEC's total custodial revenue for FY 2011 was over $1.1 million, and the volume of transactions is not minimal. The accounting for revenue consists of cumbersome manual and /or non-integrated operations involving several departments. Collections are posted to the general ledger when the payments are received, while accounts receivable is adjusted only at the end of each month, after the standard voucher is posted to the general ledger. We believe the agency should explore a more streamlined and timely approach which would be achieved through an integrated system.

2. IT Security Control Weaknesses

While we reported in our 2010 financial statement audit report that FEC had implemented corrective actions or had plans developed to address most of the IT control weaknesses, progress has slowed during the 2011 fiscal year and most problem areas continued to impact FEC's agency-wide IT security program. This was primarily due to the need for additional oversight by agency governance, and the absence of IT security procedures that meet best practices. As a result, FEC's information and information systems are at additional risk until actions are taken to fully remediate the weaknesses discussed below.

a. **Configuration Management and USGCB/FDCC Security Controls Needs to be Fully Implemented**

Configuration management issues continue to impact FEC. FEC has issued procedures to address some of the problem areas identified in prior reports. However, our tests found that the configuration management process does not identify and log all changes to the configuration of FEC's systems. Additionally, we again identified that the organization had not fully implemented the United States Government Configuration Baseline (USGCB)[1] requirements or ensured that its systems are in compliance with its own baseline configuration standards.

Best practices addressing configuration management provide that the organization should develop, document, and maintain under configuration control a current baseline configuration of the information system. Best practices further note that the baseline configuration should provide information about the standard software loaded for a workstation, server, or network component including operating system, installed applications with current version numbers and patch information, network topology, etc.

We compared the FEC provided configuration settings to a sample of laptop computers, and identified that the baseline configuration standards were not fully implemented. For example, one baseline configuration standard required that Simple File Sharing be disabled on workstations. However, our audit tests showed that this function had not been disabled. In addition, we identified specific services, such as; Universal Plug and Play, Netmeeting Remote Desktop Sharing, Remote Desktop Help Session Manager, and Remote Registry accesses that should have been disabled based on FEC's baseline configuration standards, but remained active on workstations tested.

The current FEC baseline configuration standards require that the "administrator account" be renamed and that access to administrator authorities is limited to users requiring such access. However, based on the computer settings we reviewed, users had been given local administrator rights that allowed them to change local settings such as screen saver usage, as well as the ability to start "services." We were able to perform selected administrator authorities on laptops we tested. In addition, our review of available reports identified servers that did not have necessary patches, fixes, or service packs installed. For example, for

[1] The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration (FDCC) mandate.

two devices we tested, the service packs installed were outdated, and had not been supported for approximately a year.

As we reported in our prior audit reports, FEC has not yet fully implemented security control requirements that OMB had established in 1997 as "best practices" security requirements for Windows computers (USGCB/FDCC). While FEC has established a project to adopt "selected" control requirements, the agency estimates that full implementation of "selected" controls will not be implemented until later in 2012. To illustrate, we have listed several requirements that could be easily changed, but have not, since we first reported this problem in our 2009 audit report. Details follow:

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

Chief Information Officer (CIO) officials opined that FEC is 75 percent USGCB/FDCC compliant, and is working to implement selected additional components of the standard. These officials also opined that implementing many of the best practice security controls are too severe for FEC's computing environment.

We believe FEC's position that "…implementing many of mentioned security controls are not best practice and too severe for its computing environment…" conflicts with guidance issued by all authoritative sources for IT security in the federal government. This includes the OMB, the National Institute for Standards and Technology (NIST), the Government Accountability Office (GAO), and the Chief Information Officers Council (CIOC). In addition, NIST IT security standards which incorporate the FDCC standards are established through a work group that consists of representatives of Civil, Defense, and Intelligence communities, as well other organizations in the public and private sectors, in an effort to produce a unified information security framework for the federal government.

The CIOC (the principal interagency forum on federal IT management practices), of which the FEC CIO is a member, has endorsed the implementation of the FDCC and the USGCB. According to the CIOC, the USGCB creates a security configuration that provides baseline settings that federal agencies are required to implement for security reasons. The CIOC goes on to state in a September 15, 2010 memorandum, issued to all Council members, that the USGCB (and the FDCC) settings are "...the minimum requirements…intended to be the core set of security configuration settings by which all agencies should comply…." FEC's

information and information systems are at increased risk by not adopting the minimum security requirements established for the federal government through the USGCB/FDCC standards.
Recommendations:

3. Implement baseline configuration standards for all workstations and require documentation and approval of any deviations from this standard.

4. Fully implement USGCB/FDCC standards.

5. Implement logging of configuration changes to ensure that all system changes are processed through the change management framework.

<u>Agency Response</u>

Management concurs, in part, with recommendation 3. The agency plans to establish baseline configuration standards for all workstations. However, these baseline configuration standards cannot be implemented until the completion of the FEC USGCB/FDCC Project. Management concurs, in part, with recommendation 4. The FEC is already 75 percent USGCB/FDCC compliant and is working to implement additional components of the standard. However, management disagrees with the auditors that every agency must fully implement the USGCB/FDCC standard. It is the intent of the standard that only those controls within USGCB/FDCC conducive to each agency's unique environment be implemented, and the decision to implement a particular control is left to the agency.

Management concurs, in part, with recommendation 5. Management recognizes the need to review and approve all configuration changes (including workstation configuration changes); however, management is currently evaluating whether the best course of action is to integrate this into the current change management framework.

<u>Auditor Comments</u>

FEC officials have concurred, in part to our recommendations. The primary difference between FEC's response and the audit recommendations relate to USGCB/FDCC security requirements. Federal IT security experts have determined that implementation of the USGCB/FDCC is required to meet minimal IT security levels. FEC officials, however, consider the standards advisory. As we have discussed above, we believe FEC's information and information systems are at increased risk by not adopting the minimum security requirements established for the federal government through the USGCB/FDCC standards.

b. Vulnerability Scanning Process Needs Strengthening

FEC has established a vulnerability scanning program; however, not all segments of FEC's network are currently included in the program. In addition, a comprehensive analysis of scanning results to identify root causes and track remedial actions were not always performed. We attributed this problem to FEC not adopting IT best practices. As a result, FEC has reduced assurances that the agency will detect potential vulnerabilities within its network.

OMB Circular A-130, *Management of Federal Information Resources*, Appendix III provides that agencies "should assure that each system appropriately uses effective security products and techniques, consistent with standards and guidance from NIST (best practices)." Best practices note that vulnerability scanning is a key security control that is part of an agency's risk assessment process.

Our review of the vulnerability scanning performed by FEC during fiscal year 2011 showed that many of the same problems reported in our prior audit continued to exist. For example, we found that over 200 of the 255 vulnerabilities identified in the 2011 scanning were also identified as problems in the scans performed in 2010 by FEC. We also found that individual workstations were excluded from the scanning process – a critical gap in the implementation of this control process. Therefore, the current vulnerability scanning process does not provide an accurate picture of FEC's security posture.

We discussed these problems with OCIO personnel who advised that although vulnerability scanning of workstations is prudent from a security standpoint, management has not evaluated the feasibility of integrating workstation scanning into its current vulnerability mitigation program. OCIO officials added that "scanning of workstations is not scheduled to occur until completion of the FDCC implementation project and the determination as whether workstation scanning will be a separate process or integrated into the current process cannot be made until then."

We continue to believe that vulnerability scanning is necessary for all of FEC's IT assets. Without a robust vulnerability scanning program, FEC is not aware of all vulnerabilities that may exist in its network, and; therefore, is unable to mitigate potential vulnerabilities that could risk FEC's information and information systems.

Recommendations:

6. Include all components of the general support system, including workstations, into the organization's vulnerability scanning process.

7. Implement procedures to ensure that scan results are subject to a "root cause" analysis to ensure that problems are fully resolved.

8. Develop a process to ensure that vulnerabilities identified through scanning are documented in a corrective action plan, and monitored to ensure timely remediation.

Agency Response

Management concurs, in part, with recommendation 6. Although FEC already scans workstations for viruses and spyware and has implemented an automated process for pushing security patches to all workstations to eliminate operating system vulnerabilities, additional vulnerability scanning of workstations is prudent. However, management has not evaluated the feasibility of integrating workstation scanning into its current vulnerability mitigation program. Scanning of workstations is not scheduled to occur until completion of the FDCC's project. Management cannot determine whether workstation scanning will be a separate process or integrated into the current process until then. Management concurs with recommendations seven and eight.

Auditor Comments

FEC officials agreed with our recommendations except for a decision as to how the scanning of workstations will be performed (separate process or integrated). Our concern is that workstations should be included as part of the scanning program by FEC. This scanning could be accomplished either as a standalone scanning program, or integrated with other network scanning.

c. Progress is Needed on System to Recertify Users' Access Authorities

FEC has not completed a periodic review of users' access authorities. We attributed this problem to the need for additional management oversight over this problem area. As a result, FEC officials have limited assurance that users have access only to information and information systems that are necessary to accomplish the users' job responsibilities. Best practices provides that an organization manage information system accounts, including reviewing accounts on a periodic basis.

We reviewed the progress made by FEC to implement agreed upon corrective actions concerning periodic certification of users' access authorities. We found that during fiscal year 2011 the agency had terminated the project established to develop processes to enable supervisors to recertify users' access authorities. OCIO officials advised us that the project was incorporated into another ongoing project dealing with a document and records management system. FEC officials estimated that the overall project will be completed by approximately June 2012.

Recommendations:

9. Establish and publish a policy that requires annual recertification of users' access authorities.

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.

Agency Response

Management concurs, in part, with recommendation 9. Although management agrees that recertification of user access authorities is prudent, management believes a biennial review would be a more efficient use of scarce resources. Management concurs, in part, with recommendation 10. However, management cannot guarantee that available resources will not be reallocated to accommodate the level of activity anticipated in connection with the 2012 election cycle.

Auditor Comments

FEC officials agree in part with our recommendations, and notes staffing issues as an impediment to our recommendation for annual reviews of user access authorities. Because FEC has never fully performed an agency-wide review of user access authorities, we believe that the review should be made annually until the number of issues noted is reduced to minimal levels.

d. Removal of User Access for Departed Personnel Needs Improvement

FEC continues to have problems timely removing network access for separated employee and contractor personnel. The absence of an effective process to control the removal of separated personnel from FEC's network poses a significant security risk to the agency's information and information systems.

Problems continued to exist even though FEC established a new system, FEC System Access (FSA), to control the timely addition and termination of users to FEC's network. As shown below, we identified personnel that had departed for up to three years, but were still active on FEC's network. Details follow:

Employee	Date Left Agency
Number 1	September 30, 2008
Number 2	May 26, 2010
Number 3	December 19, 2009
Number 4	March 2011
Number 5	March 2011

Recommendations:

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.

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.

Agency Response

Management concurs with recommendations 11 and 12. Management has discovered the reasons why five individuals' access was not properly removed and is evaluating various additional controls to ensure that FEC timely removes access for individuals who leave the agency.

Auditor Comments

Since FEC concurs with this finding and the associated recommendations, we have no additional comments.

e. Effective Tracking of Security Awareness Training Needed

FEC needs to strengthen its control processes dealing with providing security awareness training and obtaining acknowledgement of the rules of behavior for employees and contractors. We attributed the problems to the absence of an effective tracking system that would identify personnel who did not take required training. As a result, FEC is not in compliance with its policies and best practices.

OMB Circular A-130, Appendix III requires that agencies provide security awareness training and rules of behavior to personnel prior to granting access to an agency's systems.

Information obtained on the 2011 security awareness training provided to FEC personnel and contractors disclosed ten people who had not completed the training by the required date. OCIO personnel were unable to provide documentation to support why the training had not been completed, and the personnel continued to have access to the system. In addition, since acknowledgement of rules of behavior is a part of the security training process, current rules of behavior were also not obtained for these individuals.

Recommendations:

13. Establish controls that would automatically suspend an individual's network access if security awareness training is not completed within required timeframes.

14. Ensure all personnel and contractors that have not yet taken the security awareness training complete it within the next 30 days.

Agency Response

Management concurs, in part, with recommendation 13 and 14. Management agrees that removing network access is prudent for those individuals who fail to complete security awareness training in a timely fashion; however, Commission approval will be required prior to implementation.

Auditor Comments

FEC concurs with this finding and the associated recommendations, and notes that Commission approval will be required before any changes can be implemented. We believe that adopting the audit recommendations will further strengthen FEC's IT security program.

f. Last Phase of COOP and Contingency Planning Needs Completion

While FEC has completed most of the last phase of its multi-year plan to implement a Continuity of Operations Plan (COOP) document, we found that FEC has not yet tested and exercised the COOP – a critical element in the development of a comprehensive and effective plan. We attributed this problem to the need for more effective oversight over the COOP testing process. As a result, FEC systems are at increased risk without a properly tested COOP document.

FEC's most recent COOP planning documents showed that the agency had planned to complete necessary testing and exercise of its COOP by July 2011. We discussed this matter with FEC officials, and were advised that the COOP testing was delayed due to the illness of a key project team member. The official added that the completion of testing was deferred until approximately the beginning of calendar year 2012.

Federal Continuity Directive No.1, *Federal Executive Branch National Continuity Program*, requires that COOP documents must be validated through tests, training, and exercises (TT&E), and that all agencies must plan, conduct, and document periodic TT&E to prepare for all-hazards continuity emergencies, identify deficiencies, and demonstrate the viability of their continuity plans and programs.

Recommendation:

15. Ensure that sufficient resources are assigned to the task of testing the COOP in order to reduce the risks to FEC operations.

Agency Response

Management concurs, in part, with recommendation 15. Management cannot guarantee available resources will not be reallocated to accommodate the level of activity anticipated in connection with the 2012 election cycle.

Auditor Comments

FEC officials concurred with the recommendation, except that resources may not be available to reallocate during an important election cycle. We believe that the testing of the COOP plan is a key area, and the agency should ensure that necessary resources are available to accomplish this important task.

g. Controls over Copy Protected Software and User Installed Files Needs Improvement

FEC needs to develop, document, and implement control processes dealing with copy protected software that address best practice requirements, and to restrict access over the applications, folders and data stored in the "userinstall" network folder. As discussed below, we identified control weaknesses in both areas, resulting in increased risk to the agency's information and information systems and non-compliance with software quantity license restrictions.

Best practices control requirements provide that the organization uses software and associated documentation in accordance with contract agreements and copyright laws, and employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution.

- **User Installed Files**
  FEC personnel provided the auditors system data reports which identified that all FEC personnel and contractors with access to FEC's network have the authority to access the "userinstall" folder. We initially accessed this folder to perform control testing relating to copy protected software for one sample application. However, when we began our tests, we noted a large number of folders and files located in this network folder appeared to be executable applications, and some applications appeared to be copy protected software.

  We identified over 200 folders and files in the "userinstall" network folder. These folders and files consisted of approximately 75 applications, some of which dated to 2007, that were listed as executable. In addition, we identified approximately 80 additional sub-folders that in many cases also contained executable files. The remaining files and folders consisted of miscellaneous information and data. We tested the executable files in approximately 20 of these folders, and found that over fifty percent allowed us to install the application. We did not continue to fully install the application when it appeared the application would install an older version and/or was a network server application. For some files, we were denied access because of security controls or other errors that prevented installation of the application.

For those files where we continued to fully install the application, we installed copy protected software, and an old "trial version" of an application. For two applications in this folder relating to updates to server applications, we discussed the results of our testing with the CIO officials, and the applications were removed from this folder.

- **Copy Protected Software**
  To test the controls that FEC had established over copy protected software, we selected an application that had a quantity license limitation of 50 users. For this application, we found that the software was placed on an FEC network drive that was accessible to all FEC employees and contractors with FEC network access.

  When we requested from OCIO personnel the processes FEC followed to ensure that this application would be limited to 50 users, we were advised that the application's folder was secured, and only specific authorized users could install the application. However, our audit determined that the software could be installed by any of the approximately 400 users with access to FEC's network. As a result, FEC was at risk of being in violation of quantity licensing requirements for copy protected software.

  We requested from FEC the specific written control processes followed by the agency to ensure that it complied with purchased software quantity licensing requirements. However, we were not provided with specific written control procedures or processes that addressed best practice requirements or Commission directives. In fact, Commission Directive 58: *Electronic Records, Software and Computer Usage*, states, "Strict control over computer software is necessary to maintain the integrity and coherence of the agency's information technology architecture (ITA), (and) to comply with intellectual property copyright laws and licensing agreements.…"

Recommendations:

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.

17. Restrict network folders & subfolders containing copyright applications and software to only authorized users based on the operational policies developed and implemented.

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.

Agency Response

Management concurs, in part, with recommendation 16. However, management disagrees with many of the conclusions cited in the finding. Management believes the risk of violating any copyright laws or user authorization is minimal compared to the increase in productivity of facilitating controlled user software installation software. Many of the items cited in the finding (such as older versions of software) are based upon operational necessity. However, management believes there may be room for improvement, and will review its methods to ensure that FEC uses software and associated documentation in accordance with contract agreements and copyright laws. Upon conclusion of the review, management will adjust its procedures and policies accordingly.

Implementing an automated process to control the security of the software installation process is dependent upon funding. In addition, limiting the use of software and associated documentation protected by quantity licenses to purchased licenses is dependent upon evaluating the cost versus risk of purchasing quantity licenses or purchased licenses per software package.

Management concurs, in part, with recommendation 17. Access to network folders & subfolders containing copyright applications and software is already restricted; however, management will evaluate the impact on operational effectiveness of further restricting access to userinstall and adjust its methods accordingly. Management concurs with recommendation 18.

Auditor Comments

FEC has a legal responsibility to comply with contract requirements, including meeting the licensing requirements for the software it purchases. The Government Accountability Office (GAO), *Standards for Internal Control,* in the Federal Government, defines the minimum levels of internal control in government and provides the basis against which internal control is to be evaluated. The standards require management to establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management. OMB Circular A-123, *Management’s Responsibility for Internal Control*, provides that agencies and individual Federal managers must take systematic and proactive measures to develop and implement appropriate, cost-effective internal control for results-oriented management.

We disagree with FEC’s position that it has implemented the necessary security controls to mitigate the risk to an acceptable level. Our tests showed that there were no effective controls in place to ensure that the agency complied with the software's quantity licensing requirements.

h. FEC's IT Security Program Would be Strengthened by Adopting Federal Government Security Standards

FEC has not adopted government-wide IT security controls and techniques issued by the National Institute of Standards and Technology (NIST). We attributed this condition to FEC management's belief that the agency's IT information and information systems are adequately secured even if many of the government-wide minimum security requirements have not been adopted by FEC. As a result, FEC's information and information systems are at increased risks.

In our 2009 and 2010 audit reports, we recommended that FEC 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*, and other related NIST security documents. We also reported that the Government Accountability Office (GAO), that is also exempt from FISMA compliance, has voluntarily adopted the NIST security requirements. GAO stated that it adopted FISMA requirements to strengthen its information security program, and that FISMA and related federal guidance from the Office of Management and Budget constitute the cornerstone of its security program, establishing the procedures and practices that strengthen their protections through the implementation of security "best practices."

The Inspector General's "Statement on the Federal Election Commission's Management and Performance Challenges" dated October 14, 2010, stated:

> "… [we] first identified information technology security as a challenge in 2004, the first year the Inspector General prepared a report of this kind. While the commitment of the FEC staff to improve IT security is vital, the OIG continues to believe the adherence to government-wide IT security standards is an important part of an effective security program. GAO has cited the enactment of the Federal Information Security Management Act of 2002 (FISMA) as important legislation requiring the development, documentation, and implementation of an agency-wide information security program…the OIG feels that the FEC should formally adopt adherence in principle to FISMA and the NIST standards. We continue to believe this is a necessary and an important step for the FEC to ensure that the agency's vital operations are safe and secure according to government standards."

The FEC commented on the Inspector General's management challenges, and noted that "In sum, the level of security provided by the FEC IT Security Program is within the guidance provided by applicable federal standards, including the exemption of the agency from FISMA and National Institute of Standards and Technology standards."

Although the FEC has actions ongoing to address some of the problem areas we have reported, overall progress has been slow. In other areas, FEC has not agreed to implement strengthened controls by fully adopting best practice control requirements. For example: FEC has not fully adopted: (1) USGCB/FDCC standards; (2) certification and accreditation controls that require independent reviews at least every three years; (3) risk assessment controls and vulnerability scanning; and (4) systems and services acquisition controls, including Federal Acquisition Regulations (FAR) related IT controls for contractors. The FAR requires agencies to include in IT contracts requirements that contractors must follow NIST security requirements. However, FEC officials advised us that the agency is exempt from these FAR requirements because the agency is exempt from the Paperwork Reduction Act and it's corresponding IT security requirements.

We requested documentation to determine whether FEC had completed an analysis of the risks associated with not adopting recognized IT security controls, and that officials had accepted the increased risks to the FEC information and information systems. However, we found neither a procedure that required such an analysis, nor documentation that an analysis had been performed.

We discussed this matter with OCIO officials who advised that it would be improper for the FEC to disregard the will of Congress, which has exempted FEC from FISMA compliance. These OCIO officials added that it was not the original intent of NIST to impose a set of standards to which all federal agencies must adhere. However, these officials added that FEC does utilize NIST as one source of guidance when determining best practice.

FEC officials' statements about disregarding the will of Congress have already been addressed by FEC's own Office of General Counsel (OGC). In documents provided to us, OGC has noted that FEC could elect to adopt NIST standards. In addition, FEC's comment that "…it was not the original intent of NIST to impose a set of standards that all federal agencies must adhere to" is not correct. For example, OMB Memorandum M-10-15, dated April 21, 2010, states: "…Is use of National Institute of Standards and Technology (NIST) publications required? Yes. For non-national security programs and information systems, agencies must follow NIST standards and guidelines."

Recommendations:

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*.

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.

Agency Response

Management does not concur with recommendation 19 for several reasons. Although the FEC is exempt from the Paperwork Reduction Act (PRA), which requires federal agencies to adhere to the National Institute of Standards and Technology (NIST) standards for information technology security, it continues to use these standards as guidance. As a small agency, the FEC would be especially burdened by the additional overhead expenses associated with adhering to all NIST standards. Instead, the agency retains the flexibility to adopt NIST guidelines as appropriate, which was the original intent of these standards, and to consider best practices identified from other sources where those standards will best serve the FEC's needs. NIST standards nevertheless form the basis for the FEC's security program.

Utilizing this guidance, the FEC has identified 29 best practices and implemented policies based upon them. The FEC is currently evaluating additional best practices to determine whether incorporating them into its security program will support the agency's overall IT security needs. In addition, the agency's 2009 third party, independent Certification and Accreditation project was based upon NIST standards. These policies and the Certification and Accreditation process not only describe the FEC's minimum security controls, but also affirm its decision not to rely upon a single source of guidance for best practices. Instead, the FEC draws upon other sources and tailors those best practices to its unique computing environment.

Management does not concur with recommendation 20. The FEC already requires contractors to comply with its IT security policies and best practices.

Auditor Comments

As we discussed in this and our prior audit reports, we believe that until FEC adopts best practice requirements that establish minimum security levels, the agency's information and information systems will remain at risk.

A summary of the status of prior year findings is included as Appendix 1.

We noted another control deficiency over financial reporting and its operation that we do not consider a significant deficiency, but still needs to be addressed by management. We have reported this matter to the management of the FEC, and those charged with governance in a separate letter dated November 10, 2011

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).

We noted a matter involving compliance with certain provisions of laws and regulations and its operation that we do not consider to be significant. We have reported this matter to the management of the FEC, and those charged with governance in a separate letter dated November 10, 2011.

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 believe that our audit provides a reasonable basis for our opinion.

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 required by OMB Bulletin 07-04 (as amended), with respect to internal control related to performance measures determined to be key and reported in Management's Discussion and Analysis, we made inquiries of management concerning the methods of preparing the information, including whether it was measured and presented within prescribed guidelines; changes in the methods of measurement or presentation from those used in the prior period(s) and the reasons for any such changes; and significant assumptions or interpretations underlying the measurement or presentation. We also evaluated the consistency of Management's Discussion and Analysis with management's responses to the foregoing inquiries, audited financial statements, and other audit evidence obtained during the examination of the financial statements. Our procedures were not designed to provide assurance on internal control over reported performance measures, and, accordingly, we do not provide 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.

DISTRIBUTION

This report is intended solely for the information and use of the management, the Commission, 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, PC

Leon Snead & Company, P.C.
November 10, 2011

Status of Prior Year Reportable Conditions

Recommendation	Status As of September 30, 2011
1. Provide additional training to personnel involved in accounts payable control processes, and stress to supervisors that reviews of accounts payable accruals must be more effective. Ensure when errors are noted, the reviewer follows up to ensure corrections are made.	Recommendation closed.
2. Convert FEC manual systems and processes to automated systems that are integrated or interfaced with the core accounting system.	Recommendation open – reported as significant deficiency.
3. Ensure that FEC baseline configuration standards are implemented in accordance with FDCC requirements for all workstations.	Recommendation open – reported as significant deficiency.
4. Perform periodic assessments of baseline configuration settings as part of FEC's continuous monitoring program.	Recommendation open – reported as significant deficiency.
5. 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.	Recommendation open – reported as significant deficiency.
6. Implement additional controls to ensure that former employees' access to the network is terminated in accordance with FEC policies.	Recommendation open – reported as significant deficiency.
7. Assure sufficient resources are provided to complete the project dealing with the establishment of processes to enable periodic review of users' access authorities.	Recommendation open – reported as significant deficiency.
8. Require that dial-up access is properly secured as required by best practices, or terminate this type of access for users.	Recommendation closed.
9. 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.	Recommendation open – reported as significant deficiency.
10. Monitor the POA&M to ensure that the documents are completed and fully tested by the end of the 2010 calendar year.	Recommendation open – reported as significant deficiency.
11. Adopt as a model 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 – reported as significant deficiency.

Appendix 2

THE FEDERAL ELECTION COMMISSION
Washington, DC 20463

November 10, 2011

MEMORANDUM

TO: Leon Snead and Company

FROM: Mary Sprague
Chief Financial Officer

Mary G. Sprague, CFO
Digitally signed by Mary G. Sprague, CFO
DN: cn=Mary G. Sprague, CFO, o=Federal Election Commission, ou=OCFO, email=msprague@fec.gov, c=US
Date: 2011.11.10 09:17:29 -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 7, 2011.

Please contact me at X1217 should there be additional questions.

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

1. Internal Controls over Financial Reporting

Auditor Recommendation 1a: Controls over Disbursements Needed Strengthening

Management Response to 1a: Management concurs, in part, that a misclassification occurred due to an administrative error. The error was due to a training issue rather than an employee bypassing internal controls. The amount was insignificant and had no impact on the financial statements. Of the $11,500 identified by the auditors, only $6,300 applied to the current year. The OCFO corrected the error before the end of the fiscal year, as recommended by the auditors. Since the auditors found no further issues with regard to this error, no other recommendations were made. Management does not concur with the finding that the error contributed to the significant deficiency for internal controls over financial reporting. Management believes that this error was insignificant and does not reflect a significant deficiency in the agency's internal controls.

Auditor Recommendation 1b: Manual Systems Introduce Unnecessary Risk

Management Response to Recommendations #1 and 2: Management concurs that it is important for agencies to consider automating manual processes whenever it is appropriate and cost effective to do so. However, management does not agree with the auditor's interpretation of a financial management system. OMB Circular A-127, as revised in 2009, defines a financial management system as a system that "includes the core financial systems and the financial portions of mixed systems necessary to support financial management, including automated and manual processes, procedures, and controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions."

While the OCFO does have some manual steps in its financial process, the office has implemented compensating controls consistent with industry best practices to eliminate unnecessary risks.

The OCFO evaluated the GSA Accounts Receivable and Collection System (ARCS) and determined that the system could not be utilized for FECA receivables because it does not allow the customization needed to meet the individual needs of the offices that enforce FECA debts.

The Accounts Receivable balance is immaterial to the FEC's financial statements and the volume of transactions is minimal. The expense of migration to an automated process is currently not in the best interest of the FEC or the Federal Government because it is not cost effective. The cost-effectiveness criterion is consistent with the GAO's Report on Financial Management Systems (GAO-09-328), the testimony of OMB Controller before Congress on April 14, 2010, the draft of A-127 circulated October 15, 2010, and the OMB Memorandum M-11-29 Chief Information Officer Authorities, issued August 8, 2011.

As it relates to the payroll accounting, the OCFO verifies NFC data, independent of the PeopleSoft application, before submitting to GSA. The FEC is working closely with NFC and GSA on the integration of the payroll system with the GSA Pegasys accounting system. Additionally, the FEC is working on an Oracle upgrade project to replace the PeopleSoft application. These projects are expected to complete during FY 2012.

2. IT Security Control Weaknesses

Auditor Recommendation #3: Implement baseline configuration standards for all workstations and require documentation and approval of any deviations from this standard.

Management Response to Recommendation #3: Management concurs, in part, with recommendation #3. The agency plans to establish baseline configuration standards for all workstations. However, these baseline configuration standards cannot be implemented until the completion of the FEC USGCB/FDCC Project.

Auditor Recommendation #4: Fully implement USGCB/FDCC standards.

Management Response to Recommendation #4: Management concurs, in part, with recommendation #4. The FEC is already 75 percent USGCB/FDCC compliant and is working to implement additional components of the standard. However, management disagrees with the auditors that every agency must fully implement the USGCB/FDCC standard. It is the intent of the standard that only those controls within USGCB/FDCC conducive to each agency's unique environment be implemented, and the decision to implement a particular control is left to the agency.

Auditor Recommendation #5: Implement logging of configuration changes to ensure that all system changes are processed through the change management framework.

Management Response to Recommendation #5: Management concurs, in part, with recommendation #5. Management recognizes the need to review and approval all configuration changes (including workstation configuration changes); however, management is currently evaluating whether the best course of action is to integrate this into the current change management framework.

Auditor Recommendation #6: Include all components of the general support system, including workstations, into the organization's vulnerability scanning process.

Management Response to Recommendation #6: Management concurs, in part, with recommendation #6. Although FEC already scans workstations for viruses and spyware and has implemented an automated process for pushing security patches to all workstations to eliminate operating system vulnerabilities, additional vulnerability scanning of workstations is prudent. However, management has not evaluated the feasibility of integrating workstation scanning into its current vulnerability mitigation program. Scanning of workstations is not scheduled to occur until completion of the FDCC's project. Management cannot determine whether workstation scanning will be a separate process or integrated into the current process until then.

Auditor Recommendation #7: Implement procedures to ensure that scan results are subject to a "root cause" analysis to ensure that problems are fully resolved.

Management Response to Recommendation #7: Management concurs with recommendation #7.

Auditor Recommendation #8: Develop a process to ensure that vulnerabilities identified through scanning are documented in a corrective action plan, and monitored to ensure timely remediation.

Management Response to Recommendation #8: Management concurs with recommendation #8.

Auditor Recommendation #9: Establish and publish a policy that requires annual recertification of users' access authorities.

Management Response to Recommendation #9: Management concurs, in part, with recommendation #9. Although management agrees that recertification of user access authorities is prudent, management believes a biennial review would be a more efficient use of scarce resources.

Auditor Recommendation #10: Assure sufficient resources are provided to the document and records management system so that it can be completed no later than June 2012.

Management Response to Recommendation #10: Management concurs, in part, with recommendation #10; however, management cannot guarantee that available resources will not be reallocated to accommodate the level of activity anticipated in connection with the 2012 election cycle.

Auditor Recommendation #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.

Management Response to Recommendation #11: Management concurs with recommendation #11**.**

Auditor Recommendation #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.

Management Response to Recommendation #12: Management concurs with recommendation #12**.** Management has discovered the reasons why five individuals' access was not properly removed and is evaluating various additional controls to ensure that FEC timely removes access for individuals who leave the agency.

Auditor Recommendation #13: Establish controls that would automatically suspend an individual's network access if security awareness training is not completed within required timeframes.

Management Response to Recommendation #13: Management concurs, in part, with recommendation #13**.** Management agrees that removing network access is prudent for those individuals who fail to complete security awareness training in a timely fashion; however, Commission approval will be required prior to implementation.

Auditor Recommendation #14: Ensure all personnel and contractors that have not yet taken the security awareness training complete it within the next 30 days.

Management Response to Recommendation #14: Management concurs with recommendation #14.

Auditor Recommendation #15: Ensure that sufficient resources are assigned to the task of testing the COOP in order to reduce the risks to FEC operations.

Management Response to Recommendation #15: Management concurs, in part, with recommendation #15. Management cannot guarantee available resources will not be reallocated to accommodate the level of activity anticipated in connection with the 2012 election cycle.

Auditor Recommendation #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.

Management Response to Recommendation #16: Management concurs, in part, with recommendation #16. Management disagrees with many of the conclusions cited in the finding. Management believes the risk of violating any copyright laws or user authorization is minimal compared to the increase in productivity of facilitating controlled user software installation software. Management has implemented the necessary security controls to mitigate the risk to an acceptable level. Many of the items cited in the finding (such as older versions of software) are based upon operational necessity. However, management believes there may be room for improvement and will review its methods to ensure that FEC uses software and associated documentation in accordance with contract agreements and copyright laws. Upon conclusion of the review, management will adjust its procedures and policies accordingly.

Implementing an automated process to control the security of the software installation process is dependent upon funding. In addition, limiting the use of software and associated documentation protected by quantity licenses to purchased licenses is dependent upon evaluating the cost versus risk of purchasing quantity licenses or purchased licenses per software package.

Auditor Recommendation #17: Restrict network folders & subfolders containing copyright applications and software to only authorized users based on the operational policies developed and implemented.

Management Response to Recommendation #17: Management concurs, in part, with recommendation #17. Access to network folders & subfolders containing copyright applications and software is already restricted; however, management will evaluate the impact on operational effectiveness of further restricting access to userinstall and adjust its methods accordingly.

Auditor Recommendation #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.

Management Response to Recommendation #18: Management concurs with recommendation #18.

Auditor Recommendation #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.

Management Response to Recommendation #19: Management does not concur with recommendation #19 for several reasons. Although the FEC is exempted from the Paperwork Reduction Act (PRA), which requires federal agencies to adhere to the National Institute of Standards and Technology (NIST) standards for information technology security, it continues to use these standards as guidance. As a small agency, the FEC would be especially burdened by the additional overhead expenses associated with adhering to all NIST standards. Instead, the agency retains the flexibility to adopt NIST guidelines as appropriate, which was the original intent of these standards, and to consider best practices identified from other sources where those standards will best serve the FEC's needs. NIST standards nevertheless form the basis for the FEC's security program. Utilizing this guidance, the FEC has identified 29 best practices and implemented policies based upon them. The FEC is currently evaluating additional best practices to determine whether incorporating them into its security program will support the agency's overall IT security needs. In addition, the agency's 2009 third party, independent Certification and Accreditation project was based upon NIST standards. These policies and the Certification and Accreditation process not only describe the FEC's minimum security controls, but also affirm its decision not to rely upon a single source of guidance for best practices. Instead, the FEC draws upon other sources and tailors those best practices to its unique computing environment.

Auditor Recommendation #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.

Management Response to Recommendation #20: Management does not concur with recommendation #20. The FEC already requires contractors to comply with its IT security policies and best practices.

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.