

**FEDERAL ELECTION COMMISSION**

**OFFICE OF INSPECTOR GENERAL**



**FINAL REPORT**

**Audit of the Federal Election Commission's  
Fiscal Year 2009 Financial Statements**

**November 2009**

**ASSIGNMENT No. OIG-09-01**



## 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 2009 Financial Statements

DATE: November 13, 2009

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, 2009. 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, 2009, 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, 2008, were audited by other auditors whose report dated November 7, 2008, 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, 2009, 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 an instance of reportable noncompliance that is required to be reported under U.S. generally accepted government auditing standards or OMB guidance.

LSC identified a reportable noncompliance in the area of:

- Compliance with the Debt Collection Improvement Act

#### Audit Follow-up

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.

#### OIG Evaluation of Leon Snead & Company's Audit Performance

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  
Inspector General

Attachment

Cc: Alec Palmer, Acting Staff Director/Chief Information Officer  
Mary G. Sprague, Chief Financial Officer  
Thomasenia P. Duncan, General Counsel

---

**FEDERAL ELECTION COMMISSION**

**Audit of Financial Statements**

**As of and for the Year Ended  
September 30, 2009**

---

**Submitted By**

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

# TABLE OF CONTENTS

---

---

	<i><u>Page</u></i>
Independent Auditor's Report.....	1
Summary .....	1
Opinion on the Financial Statements .....	2
Internal Control over Financial Reporting.....	2
1. FEC Needs to Improve Internal Controls over Financial Reporting .....	3
2. IT Security Control Weaknesses.....	10
Compliance with Laws and Regulations.....	20
3. Compliance with Debt Collection Improvement Act .....	20
Appendix 1 - Status of Prior Year Recommendations.....	24
Appendix 2 - Agency Response to Draft Report .....	26



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

Inspector General  
Federal Election Commission

### Independent Auditor's Report

We have audited the balance sheet of the Federal Election Commission (FEC) as of September 30, 2009, 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 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. The financial statements of FEC as of September 30, 2008, were audited by other auditors whose report dated November 7, 2008, expressed an unqualified opinion on those statements.

#### SUMMARY

As stated in our opinion on the financial statements, we found that the FEC's financial statements as of and for the year ended September 30, 2009, 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. Our testing of internal control identified no material weaknesses in financial reporting. However, our audit identified two significant deficiencies relating to internal controls over financial reporting, and FEC's agency-wide Information Technology (IT) security program.

The results of our tests of compliance with certain provisions of laws and regulations disclosed one instance of noncompliance relating to the Debt Collection Improvement Act 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 sheet of the FEC as of September 30, 2009, and the related statements of net cost, changes in net position, budgetary resources, and custodial activity for the year then ended. The financial statements of FEC as of and for the year ended September 30, 2008, were audited by other auditors whose report dated November 7, 2008, expressed an unqualified opinion on those statements.

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 year ended September 30, 2009, in conformity with accounting principles generally accepted in the United States of America.

The information in the Management's Discussion and Analysis section is supplementary information required by accounting principles generally accepted in the United States of America or OMB Circular A-136, *Financial Reporting Requirements*. 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. 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 year ended September 30, 2009, 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 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.

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 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, we identified, as discussed below, two deficiencies in internal controls that we consider to be significant deficiencies.

## **1. FEC Needs to Improve Internal Controls over Financial Reporting**

Several of the deficiencies that impacted FEC's 2008 financial management operations either had not been fully corrected, or were not corrected until late in fiscal year 2009. We noted additional issues that impacted financial management operations during the 2009 fiscal year. These issues resulted in part because FEC did not have a permanent Chief Financial Officer (CFO), until March 2009 and the Office of the Chief Financial Officer (OCFO) was not fully staffed until late in fiscal year 2009. Taken together, these deficiencies represented a significant deficiency in internal controls over financial reporting.

### **a. FEC Needs to Improve Accruals of Accounts Payable**

OCFO personnel did not accrue certain accounts payable at the end of fiscal year 2008 and incorrectly posted these transactions as 2009 fiscal year activity. FEC did not have appropriate processes in place to accrue accounts payable for year-end financial reporting purposes. As a result, costs on FEC's 2009 Statement of Net Cost (SNC) were overstated by approximately \$200,000. Conversely, liabilities on the 2008 Balance Sheet and costs on the 2008 SNC were understated by this same amount.

Statement of Federal Financial Accounting Standards (SFFAS) No. 1 provides "for financial reporting purposes, liabilities are recognized when goods and services are received or are recognized based upon an estimate of work completed under a contract or agreement." SFFAS No. 5, *Accounting for Liabilities of the Federal Government*, requires liabilities to be recognized when goods and services are received. Under that standard, agencies are required to estimate the work completed under contracts and accrue expenses

and liabilities for goods and services received, even if the agency has not yet been billed.

We tested a sample of 2009 expense transactions and determined that FEC had not correctly accrued accounts payable at the end of the 2008 fiscal year. We analyzed the impact of these errors and determined that FEC had misstated both the 2009 and 2008 financial statements by including 2008 expenses in 2009 account balances. We expanded our tests in this area to determine if similar errors had been made at 2009 year-end, and we did not identify similar problems with the 2009 accrual process.

We discussed this matter with OCFO personnel who agreed that the transactions should have been accrued and included in the 2008 FEC financial statements. While not material, the transactions also impacted the 2009 financial statements. To address this problem, the OCFO developed additional controls and issued new accounting policies that they believe will correct this problem area.

### **Recommendations**

1. Strengthen controls over the accruals of accounts payable, and ensure that supervisory reviews of accounts payable accruals are performed.
2. Update OCFO policies to incorporate the new strengthened processes for identifying and posting accounts payable accruals.

### **Agency Response**

Management partially concurs. Management concurs that it is important to have appropriate controls over the accruals of accounts payable. However, Management notes that the referenced Statement of Federal Financial Accounting Standards (SFFAS) 5, *Accounting for Liabilities of the Federal Government*, is not the appropriate criteria to cite when discussing deficiencies with accounts payable accruals. Management recognizes that one invoice was improperly excluded from the accounts payable estimate as of September 30, 2008. However, we feel this was an isolated incident and the issue noted is not indicative of a lack of internal controls over financial reporting. In our opinion, the error noted is immaterial to the FY 2008 and FY 2009 financial statements taken as a whole.

Management believes that the appropriate controls were already in place in FY 2008. However, Management concurs that the operational documentation at the end of FY 2008 lacked clarity. Therefore, during the preparation of the FY 2009 second quarter interim statements, the Office of the Chief Financial Officer (OCFO) proactively strengthened its written procedures for this

process of identifying and posting estimated accounts payable. Management notes that the improved written procedures were in place for the remainder of the year. The accounts payable accrual process has since been added to the draft version of the Accounting Manual. Management expects to release the updated Accounting Manual within the next 180 days.

### **Auditor Comments**

We identified the deficiency in internal controls over financial reporting during our testing of 2009 transactions. Our statistical sample of 2009 transactions identified two invoices that were improperly recorded as expenses in the 2009 fiscal year. As a result of this error, the 2009 financial statements were overstated, and the 2008 financial statements were understated. Since these transactions were selected through a statistically valid method, we believe they represent a deficiency in internal controls, and do not represent “one isolated incident” as stated by FEC officials.

We disagree with FEC officials that appropriate controls were in place in 2008. In addition, the ineffective processes which were followed by FEC were in place through a significant portion of fiscal year 2009. This is evidenced by the changes made in the accrual process by FEC to address our Notice of Findings and Recommendations (NFR) issued after the June 30, 2009 interim financial statements were issued.

In our NFR provided to FEC officials, we cited SFFAS No. 1 as the criteria for our NFR. We have added this reference to our finding in this final audit report. SFFAS No. 5, paragraph 3 provides “The concept of a liability in this document is consistent with those in Statements Number 1 and 2. The definition amends the stated definition of a liability in SFFAS Number 1.” In addition, this standard provides the definition and the general principle for recognition for a liability, and is applicable to FEC.

#### **b. Internal Controls over Purchase Card Purchases**

During 2008, OCFO personnel did not follow appropriate control processes for the review and approval of purchase card invoices. In order to clear out 2008 delinquent billings, OCFO personnel researched the transactions and paid about \$7,000 to the purchase card vendor for identified transactions. To expedite the work for the remaining amounts, OCFO personnel made payments to clear the delinquent amounts because they could not identify supporting documentation.

The Treasury Financial Manual, Vol. I, Part 4, Chapter 4500, *Government Purchase Cards*, states “...the cardholder and approving official will review the cardholder statement of account received at the end of each monthly

billing cycle and follow contract procedures for identifying discrepancies. The cardholder statement must be submitted to the designated billing office within a time frame that allows them to process and pay the consolidated invoice within the Prompt Payment Act deadline.”

Our review of a statistical sample of transactions processed during fiscal year 2009 identified expenses totaling approximately \$15,000 that were for the payment of several delinquent purchase card transactions that should have been researched and corrected by the prior card holder during fiscal year 2008. While OCFO personnel certified all the transactions as valid purchases, our tests showed that approximately \$8,000 were not properly matched to purchase orders, or invoices and receiving reports that supported the payments made. The prior cardholder allowed these accounts to remain unprocessed instead of documenting and reconciling each purchase invoice timely.

We discussed this matter with OCFO personnel who agreed that the original transactions should have been reconciled by the original cardholder, and matched with proper supporting documents.

### **Recommendation**

3. Re-emphasize, in writing, to purchase cardholders and managers their responsibilities associated with managing the purchase card program payment process and the need for effective internal controls as discussed in FEC Procurement Procedures.

### **Agency Response**

Management concurs that the credit card statement should have been reconciled by the original card holder. However, Management believes that the corrections needed to address this issue have already been put in place. This was an exception to FEC’s approved processes and is not indicative of the FEC purchase card process. Additionally, as part of the corrective action plan prepared in response to the OIG audit, the OCFO is already in the process of revising and strengthening the purchase card procedures.

### **Auditor Comments**

FEC officials concur with the finding and that there was an exception to the approved processes. We continue to believe that FEC should reinforce to purchase card holders the internal control processes that should be followed in this important procurement area. This is reinforced by the problems noted by the OIG in its procurement and contract management audit released in September 2009.

**c. Prior Control Weaknesses Impacted Current Operations**

FEC officials addressed two weaknesses reported in the prior year audit report at the beginning of fiscal year 2009. In other cases, corrective actions were not implemented or completed until late in fiscal year 2009. The problems listed below continued to impact FEC financial management operations during a substantial portion of the 2009 fiscal year.

- The 2008 audit reported that FEC did not have adequate resources and employees with appropriate financial management accounting and reporting skills. The agency experienced turnover in key financial positions during fiscal year 2008 and adequate resources were not always available to fill the vacancies. As a result, the Accounting Officer had to take on some of these responsibilities leaving FEC with insufficient resources to effectively administer quality assurance procedures within their financial reporting environment.

Our review determined that the FEC did not fully correct the problem dealing with the lack of adequate human resources and personnel with the skill sets needed for an effective financial management operation until late in the 2009 fiscal year. However, by the end of the 2009 fiscal year, the FEC had hired a new CFO (March 2009), completed the restructuring of the OCFO, filled additional positions, and hired a contractor to assist with accounting operations. In addition, training was provided to OCFO officials and staff to assist in staff development throughout the 2009 fiscal year. As of the end of the fiscal year, this problem would no longer represent a significant deficiency to FEC's future financial management operations.

- FEC did not have a comprehensive policy bulletin or guidance memorandum as required by OMB Circular A-136. FEC had not established a formalized timeline for completing key processes and controls related to the financial statement process.

We reviewed the actions that FEC took to address this outstanding issue during fiscal year 2009. We found that the FEC had issued updated or new guidance addressing most of the areas where weaknesses were noted in the prior report. However, we found that a significant portion of this guidance was not issued until after March 2009, and another key policy document, the FEC Accounting Manual, was still in draft as of September 30, 2009.

## **Recommendations**

4. Update and issue the Accounting Manual within the next six months.
5. Establish a policy that requires OCFO policies and procedures to be periodically reviewed and updated, such as on a two to three year cycle.

## **Agency Response**

Management partially concurs with these recommendations, and noted that a significant amount of work to address these recommendations has already been accomplished. Management does not concur that the accounting manual was in draft as of September 30, 2009.

## **Auditor Comments**

Our finding discusses the actions that the FEC took during the 2009 fiscal year to address this 2008 deficiency. As discussed in our finding, significant portions of the overall guidance were not updated or completed until May 2009 or later. In addition, the accounting manual provided to us during the audit contained numerous proposed changes, and the OCFO acknowledges in their response to the draft report that the accounting manual would be completely updated in the next 180 days; another indication the manual has not been finalized.

### **d. Manual Systems Represent Unnecessary Risks to FEC's Financial Management Operations**

FEC uses a service provider for its general ledger and core financial management system operations. The FEC also uses spreadsheets, database applications, and PeopleSoft to perform selected accounting operations. The financial management processes that utilize significant manual operations include:

- **Collections and Accounts Receivable – Fines and Penalties.**  
Accounting for collections, accounts receivable, or fines and penalties involves a significant amount of manual operations. The OCFO must request accounts receivable information from three divisions. After the OCFO obtains the relevant information, the data is input into a database. A journal voucher is prepared quarterly and submitted to the service provider to record the accounts receivable information into the FEC's core accounting system. Collections, however, are processed to the general ledger when the payments are received. Therefore, only at the end of each quarter, after the journal voucher is posted to the general

ledger, does the custodial cash and accounts receivable reflect an accurate balance.

- **Property and Equipment and Accumulated Depreciation.**  
Our review of PP&E disclosed that FEC is using a combination of automated and manual processes to manage its property. Effective February 1, 2008, capitalized assets are recorded in the general ledger with the use of a flexible posting logic system. FEC also uses an access database to manage FEC's personal property inventory and to compute depreciation. These entries are then input into the general ledger with a journal voucher.
- **Payroll Reporting.**  
Because the payroll system does not interface with the accounting system, FEC must use a PeopleSoft application that is no longer supported by the vendor. This process also requires FEC to perform manual operations to reconcile the payroll data and prepare journal vouchers to input the payroll data into its accounting system.

OCFO officials are currently analyzing the financial management operations of FEC and assessing whether the agency should convert these operations to systems operated by its service provider. OCFO is actively working with its two service providers to interface the payroll system and the accounting system.

### **Recommendation**

6. Partner with FEC service providers to develop a time-phased plan to convert the manual systems and processes to automated systems that are integrated or interfaced with the core accounting system. Establish a goal of converting these systems by the end of 2010.

### **Agency Response**

Management concurs that agencies should consider automating manual processes whenever it is appropriate and cost-effective to do so. OCFO has implemented necessary compensating controls to minimize risks of any manual process. However, FEC will continue to evaluate the potential benefits of adopting automated systems and implementing interfaces to streamline financial processes.

### **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. This problem was also reported as part of a material weakness in the 2008 financial statement audit report.

## **2. IT Security Control Weaknesses**

The Federal Election Commission (FEC) has corrected several of the significant deficiencies that were identified in the 2008 financial statement audit report, and has developed plans of action and milestones (POA&M) to address all remaining deficiencies identified in that report. However, our 2009 audit of information technology (IT) security controls applicable to FEC's general support system (GSS) disclosed other internal control weaknesses that FEC needs to address. During our audit, we noted that FEC had contracted with an independent contractor to perform a risk assessment and analysis of controls in the GSS.

The FEC's Office of General Counsel provided us with a document that identified that FEC is exempt from all Federal Information Security Management Act (FISMA) requirements, National Institute of Standards and Technology (NIST) publications, Federal Information Processing Standards (FIPS), the E-Government Act, the Paperwork Reduction Act, the Computer Security Act of 1987, and OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, Security of Federal Automated Information Resources, among others. In effect, FEC is exempt from following most federal laws, regulations, standards, and OMB requirements dealing with IT security and related issues.

In developing standards and guidelines required by law, NIST consults with other federal agencies and offices as well as the private sector to improve information security, to avoid unnecessary and costly duplication of effort, and ensure that NIST publications are complementary with the standards and guidelines employed for the protection of national security systems. In addition to its comprehensive public review and vetting process, NIST collaborates with the Office of the Director of National Intelligence, the Department of Defense, and the Committee on National Security Systems to establish a common foundation for information security across the federal government.

NIST notes that a common foundation for information security will provide the federal government and their support contractors, more uniform and consistent ways to manage the risk to organizational operations that results from operations and use of information systems. In addition, a common foundation for information security will also provide a strong basis for reciprocal acceptance of security authorization decisions and facilitate information sharing.

Since FEC is exempt from most federal legislative and OMB directives related to IT security requirements, FEC selects and implements the security controls the agency determines are appropriate for its information system. These internal

agency selections have major implications on the FEC agency-wide IT security program and the operations and assets of the agency.

In order to determine whether the security controls (security controls are the management, operational, and technical safeguards employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information) selected and placed in operation by FEC provided “adequate security”, as it pertains to FEC’s GSS, we used the federal government’s recommended minimum security controls for non-national security systems as a “best practices” standard. These minimum security controls are contained in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*. OMB Circular A-130, Appendix III, defines “adequate security” as security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information.

We performed tests of selected minimum security controls in all seventeen security requirements identified for federal information and information systems in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. Our tests were accomplished through analysis of documents and/or data provided to us by the FEC Office of the Chief Information Officer (OCIO), interviews with OCIO personnel, including the Chief Information Security Officer (CISO), walk-through of operations, other tests and analysis, and review of the FEC’s independent contractor report on security risks identified in FEC’s GSS.<sup>1</sup>

The results of our review of IT security controls, and the corrective actions planned by FEC, if applicable, are discussed below.

**a. Actions Taken to Address Deficiencies Reported in the 2008 Financial Statement Report**

We reviewed the significant deficiencies reported in the above cited report and FEC’s plan of action and milestones (POA&M), and performed tests to determine if FEC had corrected the prior reported deficiencies. In summary, we found that FEC had corrected most of the problems reported. We determined that the OCIO had prepared a detailed POA&M for each deficiency, identified personnel responsible for the corrective actions, established target dates for key milestones, and monitored the POA&M. The table below details those areas where corrective actions are still ongoing.

---

<sup>1</sup> FEC – Local Area Network (General Support System), Risk Assessment, dated December 24, 2008, completed by an independent contractor under contract with FEC.

<b>Issue Reported</b>	<b>FEC Actions</b>	<b>LSC Testing and Conclusions</b>
Users who had left the organization retained active accounts.	FEC advised that it would strengthen controls to ensure that this area is corrected.	We found that FEC had made improvements, but had not corrected the issue completely. This issue remains open.
FEC has not yet fully developed contingency planning and Continuity of Operations Plans (COOP) processes. In discussions with OCIO personnel, we were advised that FEC had developed a multi-phased plan to address these deficiencies.	FEC has received funding to deploy phase I of its POA&M. Phase I enables FEC to complete the test plan and schedule exercises necessary to test the contingency plan. FEC estimates that the exercises and testing should begin in early 2010. The last phase of FEC's contingency planning process entails the development of a COOP plan. This part has not yet been funded and it is estimated that the COOP will not be completed until the end of fiscal year 2010.	We found that FEC had made improvements, but had not corrected the issue completely. This issue remains open.
PeopleSoft application is currently running Oracle Release 8i and this version is no longer supported.	FEC uses the system to process payroll accounting data from NFC <sup>2</sup> , and generates a journal voucher to make the accounting entries in the GSA accounting system. FEC is working with NFC and GSA to create an interface between NFC and GSA. FEC believes that this will be accomplished by the end of the fiscal year.	We discussed this matter with Director of Accounting. OCFO personnel advised that they are working with the NFC and GSA to integrate the NFC data with the GSA accounting system. While this issue is not addressed, the actions taken by FEC will result in corrective action in the near future. However, this issue remains open.

OCIO officials advised us that although the vendor no longer provides support for this version of Oracle, it does provide limited support, which includes assisting customers with “work-arounds” that may arise. OCIO officials also advised that, in addition to FEC’s considerable experience with this product, the FEC has tested and maintains Oracle 8i applications and data backups

---

<sup>2</sup> The National Finance Center, a component of the Department of Agriculture, provides payroll systems services for FEC.

allowing it to restore any database to a useable state in the event of any problem.

**b. Access Controls Need Strengthening**

Because FEC does not have the necessary software to identify a user's specific access authorities, FEC has been unable to perform periodic reviews of users' access authorities. Best practices identify periodic, (at least annual), review of access authorities granted to users as a key control practice. This process provides a key control technique to ensure access authorities remain current, since users frequently change positions and errors can occur when inputting access authorities. Without periodic re-certifications of the user's access, any improper access could continue indefinitely.

We discussed this issue with the CISO who agreed that FEC needs to perform the required review of access controls. The CISO advised that the FEC obtained the necessary software on October 20, 2009, and once the configuration and testing of the software is completed, the periodic review of access controls will begin.

We tested the FEC's current account settings against the minimum settings required by best practices and identified exceptions relating to password history enforcement, maximum password age, and minimum password age.

We also compared FEC's controls for remote access to the best practice requirements and found that FEC had not implemented sufficient controls for its dial-up access. For a moderate risk system, such as FEC's GSS, best practices require the organization to employ automated mechanisms to facilitate the monitoring and control of remote access methods; use cryptography to protect the confidentiality and integrity of remote access sessions; control all remote accesses through a limited number of managed access control points; permit remote access for privileged functions only for compelling operational needs; document the rationale for such access in the security plan for the information system; and employ multifactor authentication.

We determined that the dial-up access for FEC currently does not meet any of these benchmarks. In contrast, FEC requires personnel who access the network through connections other than dial-up access, to use multi-factor authentication, a virtual private network (VPN) connection, and full disk encryption. The CISO advised that the FEC does not believe that remote access controls discussed in best practices are applicable to FEC's dial-up access.

NIST SP 800-53 (AC-17 Remote Access) provides that “Remote access is any access to an organizational information system by a user...communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless.” As noted above, the controls, in our opinion, are applicable to FEC’s dial-up access.

**c. Continuous Monitoring**

Government Accountability Office’s (GAO) “*Standards for Internal Control in the Federal Government*” documents the five standards of internal control. One of these standards requires agencies to assure that ongoing monitoring occurs in the course of normal operations. Under the standard, monitoring is to be performed continually and is ingrained in the agency’s operations. A continuous monitoring program includes an ongoing assessment of security control effectiveness to determine if the current deployed set of security controls need to be modified or updated based on changes in the information system or its operational environment.

We reviewed the continuous monitoring program of FEC, and the independent contractor’s risk assessment of FEC’s general support system, and noted the following problems:

- Access controls – FEC was not monitoring the role of remote users who had accessed the FEC LAN.
- Audit and Accountability controls – FEC had not established routine review procedures for FEC’s general support system audit logs in order to identify inappropriate or suspicious activity.
- Risk Assessment – FEC had not established and documented the frequency of vulnerability scans throughout the enterprise, or established a continuous monitoring capability that incorporated at least quarterly vulnerability scans of FEC’s network and workstations.

FEC’s current processes call for a service provider to perform vulnerability scanning of the FEC external network quarterly. The service provider performed scans in June 2008 and December 2008; however, the agency did not maintain documentation to support correction of the weaknesses identified in the scans. Our review of these scans showed that several of the same problems were identified in both scans.

FEC does not perform scanning of workstations and devices attached to the network. Therefore, vulnerability identification, patch levels, and compliance with security configurations would not be identified through FEC’s current scanning processes. OCIO officials confirmed that FEC has not yet performed scanning in these areas.

OCIO officials have established a POA&M to address the problems noted above.

**d. Federal Desktop Core Configuration Compliance Not Implemented**

FEC has not implemented best practices and OMB mandated security requirements for its desktop workstations. These security requirements have been generally accepted as providing necessary strengthening of the federal IT systems. OMB has issued guidance, dating from March 2007 that requires all federal agencies to implement the Federal Desktop Core Configuration (FDCC) security configuration. Federal agencies are required to adopt all of the minimum settings in order to be compliant. FDCC settings are substantially more restrictive than the current FEC settings. Some security enhancements that are required by FDCC include the following:

- Running the system as a standard user and not as administrator.
- Establishing a minimum 12 character password and requiring the password to change every 60 days.
- Disabling wireless service.
- Setting the system cryptograph to use FIPS compliant algorithms for encryption, hashing, and signing.
- Disallowing drivers that are not digitally signed by Microsoft.

**e. Personnel Security Controls Strengthened but Gaps Remain**

FEC has policies and procedures in place to ensure that personnel who separated from the agency had their network accesses timely removed. For fiscal year 2009, we compared the list of personnel who separated from the agency within a three-month period to the dates that each person's network access was terminated. Network access was cancelled by the next business day for nine of the ten individuals who had separated during this period; however, network access for one individual was not removed for approximately three months after the individual had separated from FEC. OCIO personnel attributed the problem to oversight, has reviewed the circumstances surrounding the discrepancy, and advised that the OCIO has implemented compensating controls to ensure that the problem does not recur.

**f. Interconnection Agreements Not Completed**

Agencies using best practices require providers of external information system services to comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Best practices define government oversight and user

responsibilities for external information system services. They also establish requirements for monitoring security controls.

An external information system service is implemented outside of the authorization boundary of the organizational information system. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating provider maintains adequate protection for the services rendered to the organization. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

We reviewed the service providers and contractors currently used by the FEC, and noted that only one of the three entities, the National Finance Center, had an agreement with FEC that complied with the best practice requirements set out above.

FEC has established a POA&M to correct this issue.

**g. Policies and Procedures Should be Established to Meet Best Practices**

As noted above, the FEC's Office of General Counsel provided us with a document that identified that FEC is exempt from all FISMA requirements, National Institute of Standards and Technology (NIST) publications, Federal Information Processing Standards (FIPS), E-Government Act, Paperwork Reduction Act, Computer Security Act of 1987, and OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, among others.

OMB has released extensive guidance on required IT security requirements to all federal governmental entities through circulars, bulletins, and memoranda. Much of this guidance cites as authoritative sources the laws and regulations that the FEC's Office of General Counsel (OGC) has determined that FEC is exempt from compliance. These determinations cite legal authorities, and do not deal with the appropriateness of whether these requirements (controls) would further strengthen FEC's IT security program. For some areas, such as accounting requirements, OGC has noted that the FEC may use the exempted document as a model.

Currently, the FEC must analyze each document released by OMB and other authoritative sources, and determine whether FEC is required to implement the guidance, and if exempt, whether the FEC should adopt the controls. In effect, this process requires FEC to independently establish a separate IT control standard settings process for FEC.

We identified a prior OIG audit, dated December 2007, Assignment No. OIG-07-02, *Report on the 2007 Performance Audit of the Federal Election Commission's Compliance with Section 522 of the Consolidated Appropriations Act, 2005*, that reported concerns similar to ours. The report concluded that deficiencies identified in the report were attributable to two main factors, one cause was the "...lack of an overall risk-based compliance and governance framework at the FEC."

The report stated that "FEC decisions on whether to adhere to IT ... security federal government guidelines often appear to be made based on legal interpretations of laws and OMB memorandums, rather than on sound risk management." The report noted that this is supported by evaluating the significant legal resources that management assigned to decision making compared with limited resources for risk management activities. The report cited as an example, management's decision not to perform privacy impact assessments. This decision was made based on an FEC OGC opinion that the FEC did not legally have to comply with this requirement, rather than on sound risk management.

The prior report noted, and we confirmed, that other federally appropriated organizations that are exempt from FISMA and NIST guidelines have formally adopted these requirements as a matter of best practice to help ensure that sound internal controls are established and followed.

Our review of FEC's guidelines, standards and policies noted that the IT security program procedures do not reference any authoritative requirements or standards. FEC procedures are not formatted to follow federal standards, and do not address many of the specific minimum control techniques required by best practices. In addition, we noted that the FEC standards, policies and guidance are usually not dated, authenticated with a signature, or include a date when the documents will be updated.

#### **h. Configuration Management**

We reviewed the independent contractor's report on the IT security control requirement for configuration management. We noted the following configuration management deficiencies were identified: FEC does not have a formal Change Control Process in place to include proper review and sign-off from all responsible managers; and mandatory configuration settings for system components are not currently established; and hardening guidelines are not in place to ensure system components are configured to the most restrictive settings.

FEC has developed a POA&M to address these deficiencies.

## **Recommendations**

7. Formally adopt as a model for FEC 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*.
8. Perform an annual independent assessment to determine whether FEC's agency-wide IT security program meets minimum security controls established by NIST.
9. Implement a process to require users' supervisors to recertify a user's access authorities annually, and maintain documentation to support actions taken to address any changes required by the reviews.
10. Adopt Federal Desktop Core Configuration (FDCC) standards and implement these standards by the end of the 2010 fiscal year.
11. Include workstations and devices attached to the network in periodic scans performed by FEC.
12. Maintain documentation showing actions taken to address the problems identified by the vulnerability scans.
13. Implement best practice controls over FEC's dial-up access.
14. Review the circumstances surrounding the untimely removal of the separated employee's access to FEC's network, and ensure controls are in place to remove the employee's access immediately upon departure.
15. Develop an OCIO policy that requires standards, guidelines and policies to be dated, authenticated with a signature, and scheduled for review and update.
16. Prepare a detailed POA&M for items identified in the risk assessment of the GSS.

## **Agency Response**

Management concurs with recommendations 9, 10, 11, 12, 14, 15, and 16. Management did not concur with recommendations 7, 8, and 13. Concerning recommendations 7 and 8, FEC officials noted that it is already closely mirroring the NIST framework; uses the IT security controls in FIPS 200 and SP 800-53 as guidance; and deviates from the model only after careful evaluation. FEC officials noted that FEC is developing a continuous monitoring program and uses the NIST documentation as guidance. Management did not concur with

recommendation 13. FEC dial-up users make a direct connection to the FEC's modem pool when establishing a remote connection. Thus, an encrypted line is not necessary, and the cost of adding additional overhead caused by encryption outweighs the benefits to an already slow communications link.

### **Auditor Comments**

We continue to believe that FEC should implement recommendation 13. NIST SP 800-53 (AC-17 Remote Access) provides that "Remote access is any access to an organizational information system by a user...communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless." We believe that the dial-up is an external connection and the control requirements are applicable to FEC's dial-up access.

Concerning recommendations 7 and 8, we recognized in the finding that the FEC engaged an independent contractor to assess its general support system, using NIST SP 800-53 minimum security controls as a basis for the assessment. We reviewed the assessment report and related documentation; FEC's POA&M that was prepared to address the weaknesses identified by the assessment; and performed independent tests of many of the NIST SP 800-53 minimum security control requirements. Our review identified that the assessment tested 168 control areas, and concluded whether the controls were implemented, partially implemented, not implemented, planned to be implemented, or not applicable to the FEC environment. In addition, we noted that included in the independent contractor's report was a disclaimer, noting that while the risk assessment used NIST Publications as a guide, the FEC maintains its exemption from NIST and FISMA.

The independent contractor's assessment report concluded that 82 controls were implemented, 28 were partially implemented, 19 were not implemented, 20 were planned to be implemented, and 19 were not applicable to FEC's IT environment. These results indicate that approximately 44 percent of the controls applicable to FEC's IT environment were not fully implemented at the time of the review. We reviewed the FEC's POA&M prepared as part of this assessment, and noted that the document consolidated the control weaknesses identified in the contractor's report into 23 areas that needed to be corrected. Of this number, 8 were rated as high risk, 14 were rated as moderate risk, and 1 as low risk.

As noted in our audit, and in the independent contractor's assessment, FEC has not fully implemented a significant number of the minimum IT security control requirements established by best practices. During our audit, we did not locate any policies or procedures, or supporting documentation, that showed either what analytical reviews are required or were performed, to support FEC's determination that a specific control requirement should not be adopted or implemented. To illustrate, we discussed with FEC officials the lack of

compliance with FDCC requirements concerning password settings that OMB has mandated that all Federal agencies adopt. We were advised that FEC users would not support moving from the current password settings to the FDCC required settings, and FEC could not commit to implementing the substantially strengthened password settings. FEC's current password settings are substantially less rigid than the mandated FDCC settings.

In summary, we believe that unless the FEC formally adopts the NIST minimum security requirements, the FEC will continue to be at unnecessary risk.

A summary of the status of prior year recommendations is included in this report as Appendix 1.

We noted another control deficiency over financial reporting and its operation that we have reported to the management of the FEC and those charged with governance in a separate management letter dated November 13, 2009.

### **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 an instance of reportable noncompliance that is required to be reported under *Government Auditing Standards* and OMB Bulletin 07-04 (as amended).

#### **3. Compliance with Debt Collection Improvement Act**

FEC does not refer all delinquent debt to the U.S. Department of the Treasury as required by the Debt Collection Improvement Act of 1996 (DCIA). Only debts administered by the Office of Administrative Review (OAR) are referred to Treasury for collection. Receivables administered by the Office of General Counsel (OGC) and the office of Alternative Dispute Resolution (ADR) are collected within FEC. Our review identified several cases in which the delinquent debt had not been referred to Treasury or reported to credit bureaus as required. As a result, FEC is not in full compliance with the DCIA and OMB Circular A-129, *Policies for Federal Credit Programs and Non-Tax Receivables*, November 2000, as revised.

#### **Recommendation**

17. FEC should develop and enforce policies and procedures for debt collection that will ensure compliance with the DCIA and OMB A-129.

## **Agency Response**

Management concurs with this recommendation, and on November 5, it presented to the Commission's Regulations Committee the need to establish policies and procedures to ensure full compliance with the DCIA and OMB A-129.

## **Auditor Comments**

Since FEC fully concurs with this finding and recommendation, we have no additional comments.

## **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 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.

#### **AGENCY COMMENTS AND AUDITOR EVALUATION**

We have incorporated the agency's response to our audit recommendations in the report, and have attached a copy of the response, in its entirety, as Appendix 2 to this report. In addition, we have added, where appropriate, auditor comments to address the issues raised by FEC in its response.

However, the FEC's written response to the significant deficiencies identified in our audit has not been subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on whether the actions proposed will remediate the problems noted.

**DISTRIBUTION**

This report is intended solely for the information and use of the management, The Commissioners, 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.*  
Leon Snead & Company, P.C.  
November 13, 2009

## Appendix 1

### Status of Prior Year Recommendations

<b>Recommendation</b>	<b>Status as of September 30, 2009</b>
1. Fill vacant positions within the OCFO as soon as possible. Ensure that the individuals possess analytical, Federal accounting and financial reporting knowledge and experience to enhance the FEC's ability to comply with accounting and financial reporting standards.	Recommendation closed.
2. Evaluate the resources and appropriate skills needed throughout the agency to meet FEC's financial management and reporting responsibilities and implement a plan on achieving the results and recommendations of the evaluation.	Recommendation closed.
3. Ensure that appropriate and on-going training is provided to FEC employees on federal accounting and reporting and the accounting service provider's financial system. Also, ensure OCFO personnel are properly cross-trained in department activities.	Recommendation closed.
4. Formalize and periodically update policies and procedures to a) ensure segregation of duties, b) provide guidance to management and staff in recording both recurring and unique transactions, including budgetary accounts, and c) provide guidance to management and staff in executing the financial statement preparation process in a manner that enhances the timeliness of financial statement preparation and minimizes the risk of preparing inaccurate financials.	Recommendation open.
5. Implement control activities to help ensure accounting transactions are recorded correctly, timely and are properly reviewed and adequate support documentation is maintained.	Recommendation open.
6. Establish formalized policies and procedures for performing continuous assessment of risk factors associated with financial reporting, evaluating relevant controls and developing or redesigning controls to mitigate risks. These policies should include a well-defined documentation process that contains an audit trail, verifiable results, and specific retention periods so that someone not connected with the procedures can understand the assessment process.	Recommendation closed.
7. Enforce the use of the Finance Office Check List throughout the entire fiscal year.	Recommendation closed.
8. Establish a mechanism for tracking manual journal entries sent to the service provider and maintaining associated support documents.	Recommendation closed.
9. Develop or redesign controls that strengthen the accountability structure related to the process for resolving audit findings.	Recommendation closed.
10. Re-evaluate if interfacing its standalone financial management systems with the service provider's system is feasible and/or cost effective. If not feasible and/or cost effective, consider the subsystems used by the service provider's financial management systems.	Recommendation open.
11. Finalize and implement FEC's information classification policy and certification and accreditation policy along with any accompanying standards.	Recommendation closed.
12. Incorporate the results of risk assessments into FEC security plans.	Recommendation closed.
13. Utilize corrective action plans for all reviews of security controls whether performed internally or by a third-party.	Recommendation closed.

14. Certify and accredit all major applications and mission critical general support systems.	Recommendation closed.
15. Implement a process to ensure that background investigations are performed on all contractors prior to granting them access to FEC system resources.	Recommendation closed.
16. FEC should move all of its PeopleSoft financial processing capabilities to GSA or update its existing platform to vendor-supported versions/releases.	Recommendation open.
17. Develop and implement a Disaster Recovery Continuity of Operations Plan (COOP).	Recommendation open.
18. FEC should promptly terminate access to FEC resources for separated employees. Procedures should be documented and implemented to coordinate separations between Human Resources and IT management to ensure user accounts are immediately disabled upon termination.	Recommendation open.
19. Implement an exit clearance process to track separated FEC contractors and ensure that their access permissions are removed and all FEC property has been returned.	Recommendation closed.

**Audit Recommendation #1:** Strengthen controls over the accruals of accounts payable, and ensure that supervisory reviews of accounts payable accruals are performed.

**Audit Recommendation #2:** Update OCFO policies to incorporate the new strengthened processes for identifying and posting accounts payable accruals.

**Management Responses for Recommendations #1 and #2:** Management partially concurs. Management concurs that it is important to have appropriate controls over the accruals of accounts payable. However, Management notes that the referenced Statement of Federal Financial Accounting Standards (SFFAS) 5, *Accounting for Liabilities of the Federal Government*, is not the appropriate criteria to cite when discussing deficiencies with accounts payable accruals. The Scope of SFFAS #5 paragraphs 2 and 3 specifically states:

*“2. This Statement articulates a general principle that should guide preparers of general purpose federal financial reports. It also provides more detailed guidance regarding liabilities resulting from deferred compensation, insurance and guarantees (except social insurance), certain entitlements, and certain other transactions. The Statement addresses liabilities not covered in Statement of Federal Financial Accounting Standards (SFFAS) Number 1, Accounting for Selected Assets and Liabilities...*

*3. The concept of a liability in this document is consistent with those in Statements Number 1 and 2. The definition amends the stated definition of a liability in SFFAS Number 1. This Statement establishes accounting for liabilities not covered in SFFAS No. 1 and 2. Statement Number 1 addresses only those selected liabilities that routinely recur in normal operations and are due within a fiscal year. The liabilities covered in Statement Number 1 are accounts payable, interest payable, and other current liabilities, such as accrued salaries, accrued entitlement benefits payable, and unearned revenue.”*

Management recognizes that one invoice was improperly excluded from the accounts payable estimate as of September 30, 2008. However, we feel this was an isolated incident and the issue noted is not indicative of a lack of internal controls over financial reporting. In our opinion, the error noted is immaterial to the FY 2008 and FY 2009 financial statements taken as a whole.

Management believes that the appropriate controls were already in place in FY 2008. However, Management concurs that the operational documentation at the end of FY 2008 lacked clarity. Therefore, during the preparation of the FY 2009 second quarter interim statements, the Office of the Chief Financial Officer (OCFO) proactively strengthened its written procedures for this process of identifying and posting estimated accounts payable. Management notes that the improved written procedures were in place for the remainder of the year. The accounts payable accrual process has since been added to the draft version of the Accounting Manual. Management expects to release the updated Accounting Manual within the next 180 days.

**Audit Recommendation #3:** Re-emphasize, in writing, to purchase cardholders and managers their responsibilities associated with managing the purchase card program payment process and the need for effective internal controls as discussed in FEC Procurement Procedures.

**Management Response for Recommendation #3:** Management concurs that the credit card statement should have been reconciled by the original card holder. However, Management believes that the corrections needed to address this issue have already been put in place. At the time that the balance was identified, the individual no longer worked for the agency. As part of the approved procurement procedures, OCFO requires annual training through the GSA website for purchase card holders. This was an exception to FEC’s approved processes and is not indicative of the FEC purchase card process.

Additionally, as part of the corrective action plan prepared in response to an OIG procurement audit, the OCFO is already in the process of revising and strengthening the purchase card procedures.

**Audit Recommendation #4:** Update and issue the Accounting Manual within the next six months.

**Audit Recommendation #5:** Establish a policy that requires OCFO policies and procedures to be periodically reviewed and updated, such as on a two to three year cycle.

**Management Responses to Recommendations #4 and #5:** Management partially concurs. Management concurs that having current policies and procedures are an important aspect of effective financial management. However, Management believes that a significant amount of work to address these recommendations has already been accomplished.

The following is the status of OCFO Policies and Procedures:

<b>OCFO Policies and Procedures</b>					
<b>Policy Name</b>	<b>Original Date</b>	<b>Latest Revision</b>	<b>Revision Status</b>	<b>Last Approval</b>	<b>Document Type</b>
Accounting Manual	4/1/2006	6/30/2009	Regularly updated on an as-needed basis	Director of Finance	Policy
AP Accrual Process	4/13/2009	8/12/2009	Final	Director of Finance	Operational Procedure
Funds Control Document	Non-applicable	6/22/2009	Final	CFO	Policy
Financial Statement Preparation Guidance	5/28/2009	5/28/2009	Final	CFO	Policy
Fixed Asset Policy Guide	10/7/2005	5/18/2009	Final	Director of Finance	Policy

Federal Election Commission  
2009 Financial Statement Audit  
Management Responses to Audit Findings

PPE (Exhibit 3-29) of Accounting Manual	4/1/2006	5/20/2009	Final	Director of Finance	Operational Procedure
Procurement Office Policy & Procedures	6/12/2008	6/12/2008	Final	CFO	Policy
SAS 70 review policy	9/29/2009	10/9/2009	Final	Director of Finance	Policy

The above table shows that OCFO actively reviews and updates policies and procedures regularly.

Management does not concur that the Accounting Manual was in draft as of September 30, 2009. As indicated above, the Accounting Manual was first released on April 1, 2006. Only certain sections that related to the accounting system migration from PeopleSoft to GSA's Pegasys were being updated during FY 2009. Therefore, Management believes that the Accounting Manual was in place for FY 2009 and plans to complete the update in the next 180 days.

**Audit Recommendation #6:** Partner with FEC service providers to develop a time-phased plan to convert the manual systems and processes to automated systems that are integrated or interfaced with the core accounting system. Establish a goal of converting these systems by the end of 2010.

**Management Response to Recommendation #6:** Management concurs that it is important for agencies to look to automate where appropriate and cost-effective. The OCFO has worked closely with GSA, NFC and OMB in order to identify opportunities for further automation with current systems. Management notes that manual processes do not always introduce risk. The OCFO has implemented necessary compensating controls to minimize risks of any manual processes. We believe the results of our annual FMFIA assessment as well as the results of the FY 2009 financial statement audit provide us a reasonable basis for concluding that the FEC's controls are operating effectively. However, we will continue to evaluate the potential benefits of adopting automated systems and implementing interfaces to streamline financial processes.

**Audit Recommendation #7:** Formally adopt as a model for the FEC the NIST information technology (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*.

**Audit Recommendation #8:** Perform, on an annual basis, an independent assessment to determine whether the FEC's agency-wide IT security program meets minimum security controls established by NIST.

**Management Response #7 and #8:** Management does not concur with these two recommendations for the following reasons:

- The FEC is already closely mirroring the NIST framework and deviates from the NIST

model only after careful evaluation.

- The FEC is already utilizing the IT security controls specified in FIPS 200 and SP 800-53 as guidance.
- The FEC is developing a continuous monitoring program to assess whether the agency is effectively meeting its minimum security controls. This continuous monitoring program and security control assessment uses NIST documentation as guidance.
- Congress exempted the FEC from NIST, and it would be improper for the FEC's Office of Chief Information Officer to disregard the will of Congress.
- It was not the original intent of NIST to impose a set of standards to which all Federal agencies must adhere. Rather, NIST states that "the purpose of its documentation is to provide guidance." See concluding statement
- It would not be in the agency's best interest to exclude automatically other possible sources of best practice due to adherence to one standard.

The 2009 CFO audit report also discussed at length issues the FEC had already identified and developed POA&Ms to address prior to that audit. These issues were identified because the FEC contracted with an independent vendor to conduct an unbiased risk assessment and system test and evaluation (ST&E). This independent risk assessment and ST&E are components of the Commission's Certification & Accreditation program.

**Audit Recommendation #9:** Implement a process to require users' supervisors to re-certify a user's access authorities at least annually, and maintain documentation to support that actions were taken to address any changes required by the reviews.

**Management Response #9:** Management concurs with this recommendation and will include sampling user's access for re-certification by access authorities to its continuous monitoring program. The FEC has researched, tested and purchased software to perform this function.

**Audit Recommendation #10:** Adopt Federal Desktop Core Configuration (FDCC) standards, and develop a POA&M to implement these standards by end of FY 2010.

**Management Response #10:** Management concurs with this recommendation and has included it within the GSS POA&M. The FEC has formed a NIST FDCC team to evaluate, test and implement NIST FDCC's security settings. However, best practice dictates that management strive to strike a balance between security and business needs. Therefore, the FEC reserves the right to implement only those controls it deems appropriate for its computing environment.

**Audit Recommendation #11:** Include workstations and devices attached to the network in periodic scans performed by the FEC.

**Management Response #11:** Management concurs with this recommendation; however, the FEC will need to evaluate the feasibility of scanning all of the agency's workstations to determine if additional software tools and staff are required to implement this control.

**Audit Recommendation #12:** Maintain documentation showing actions taken to address the problems identified by the vulnerability scans.

**Management Response #12:** Management concurs with this recommendation and has included it within the GSS POA&M.

**Audit Recommendation #13:** Implement best practice controls over the FEC's dial-up access.

**Management Response #13:** Management does not concur with this recommendation. FEC dial-up users make a direct connection to the FEC's modem pool when establishing a remote connection. Thus, an encrypted line is not necessary.

Although the NIST standard dictates that encryption be applied for a remote dial-up connection, the requirement is based upon employing the Internet as a communications channel between the two end-points (the FEC LAN and the remote user's laptop). This premise does not take into account the possibility of simply bypassing the Internet.

In the NIST scenario, the use of encryption would be advocated because data passing through the Internet communications channel would be unsecure. However, the FEC does not utilize the Internet as a communications channel when a remote user connects to the FEC LAN during a dial-up connection. FEC dial-up users make a direct connection to the FEC's modem pool when establishing a remote connection; therefore, an encrypted line is not necessary.

The FEC remote dial-up scenario is analogous to the FEC Human Resources (HR) Office connecting to the Office of Personnel Management (OPM) over a phone to discuss a sensitive issue. When HR establishes a phone connection to OPM, it is considered relatively secure because there is a direct connection between the two. This is the same process that occurs when a remote dial-up user connects to the FEC LAN, and it is relatively secure for the same reason: there is a direct connection between the two parties.

The only time communications would pass through the Internet would be if one (or both) parties are employing Voice over Internet Protocol (VoIP). At that point, encryption is automatically applied by the VoIP technology. The cost of adding additional overhead caused by encryption outweighs the benefits to an already slow communications link.

**Audit Recommendation #14:** Review the circumstances surrounding the untimely removal of a separated employee's access to the FEC's network, and ensure controls are in place to remove employees' access immediately upon departure.

**Management Response #14:** Management concurs with this recommendation and considers this issue closed. As indicated, for nine out of ten individuals who had separated during this period, network accesses were removed by the next business day. The FEC investigated and concluded the single oversight was due to the exiting employee failing to notify the appropriate offices.

The FEC has implemented compensating manual controls (email from HR to OIT Helpdesk on departure date) to ensure this oversight does not occur again. In addition, an automatic security control will be implemented to provide better tracking of such issues in December 2009.

**Audit Recommendation #15:** Develop an OCIO policy that requires standards, guidelines and policies to be dated, authenticated with a signature and scheduled for review and update.

**Management Response #15:** Management concurs with this recommendation and will add it to the GSS LAN POA&M. However, the FEC created 58A Information Technology Program Policy, which was signed by the Chief Information Officer and dated September 17, 2004. This policy serves as a single source reference for establishing uniform policies, responsibilities and authorities for implementing the Federal Election Commission's Information System Security Program. All subsequent IT security policies, standards and guidelines gain their authority from this document, and dates and signatures are therefore not required. However, in the interest of clarity the FEC will evaluate the advantage of dating, authenticating by signature and including a date for documents to be updated.

**Audit Recommendation #16:** Prepare a detailed POA&M for items identified in the risk assessment of the GSS.

**Management Response #16:** Management concurs with this recommendation and will add it to the GSS LAN POA&M.

#### **Concluding Statement for Auditor Findings # 7-16:**

As indicated in the audit report, the FEC has corrected the majority of findings identified in the 2008 financial statement audit report and has developed plans of actions and milestones (POA&M) to address all remaining deficiencies. The FEC has also developed POA&Ms to address those deficiencies identified during the 2009 Chief Financial Officer (CFO) audit. The majority of these deficiencies were brought to our attention prior to the 2009 CFO audit because the FEC contracted an independent vendor to conduct an unbiased risk assessment and system test and evaluation (ST&E). This independent risk assessment and ST&E are components of the Commission's Certification & Accreditation program.

A large portion of the 2009 audit report focuses on the CFO auditor's assertion that the FEC should adopt Federal Information Security Act (FISMA) and National Institute of Standards and Technology (NIST) guidance as a standard. Management does not concur with this assertion for several reasons. First, it would be improper for the FEC to disregard the will of Congress. Congress exempted the FEC from numerous laws and regulations. Whether Congress took this step to allow the agency to maintain a sense of autonomy from other components of the Federal government, or for other reasons, the fact remains that it did exempt the agency and that is the law.

Second, it should be noted that it was not the original intent of NIST to impose a set of standards to which all Federal agencies must adhere. As stated in NIST, "the purpose of its documentation

is to provide guidance.” Bearing this in mind, the FEC does utilize NIST as one source of guidance when determining best practice. However, the FEC determined early in the policy development process that it would not be in the agency’s best interest to automatically exclude possible sources of knowledge due to adherence to one standard. This was demonstrated when the FEC engaged an independent contractor to perform an unbiased risk assessment and analysis of FEC security controls in its General Support System (GSS), the FEC Local Area Network (LAN). The independent contractor utilized the same NIST documentation as the CFO auditors when evaluating the FEC’s risk posture and security controls.

The FEC is already closely mirroring the NIST framework and only deviates from the NIST model after careful evaluation of a given situation and when the agency has determined that there is either a better or more cost effective method of achieving its IT security goals. It should be noted that NIST itself allows for justified deviations. One example is the FEC’s justification for not adhering to the NIST recommendation concerning remote access.

**Audit Recommendation #17:** FEC should develop and enforce policies and procedures for debt collection that will ensure compliance with the DCIA and OMB A-129.

**Management Response to Recommendation #17:** Management concurs. On November 5, Management presented to the Commission's Regulations Committee the need to establish policies and procedures to ensure full compliance with the DCIA and OMB A-129. The Commission directed the OCFO and OGC to begin work to complete this project in calendar year 2010. Management notes that this issue only impacts approximately 11% of FEC's debt.

## ***CONTACTING THE OFFICE OF INSPECTOR GENERAL***

The success of the OIG mission to prevent fraud, waste, and abuse depends on the cooperation of FEC employees (and the public). There are several ways to report questionable activity.



Call us at **202-694-1015** (a confidential or anonymous message can be left 24 hours a day/7 days a week) **or toll-free at 1-800-424-9530** (press 0; then dial 1015 - Monday - Friday 8:30am – 5:00pm).



Write or visit us - we are located at: **Federal Election Commission  
Office of Inspector General  
999 E Street, N.W., Suite 940  
Washington, D.C. 20463**

Mail is opened by OIG staff members only.



You can also fax (202-501-8134) or contact us by e-mail at: **oig@fec.gov**.  
Website address: **<http://www.fec.gov/fecig/fecig.shtml>**

Individuals may be subject to disciplinary or criminal action for knowingly making a false complaint or providing false information.