

**FEDERAL ELECTION COMMISSION**

**OFFICE OF INSPECTOR GENERAL**



**FINAL REPORT**

**Audit of the Federal Election Commission's  
Fiscal Year 2010 Financial Statements**

**November 2010**

**ASSIGNMENT No. OIG-10-01**



## 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 2010 Financial Statements

DATE: November 12, 2010

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, 2010. 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, 2010, 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, 2009, were also audited by LSC whose report dated November 13, 2009, 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, 2010, 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.

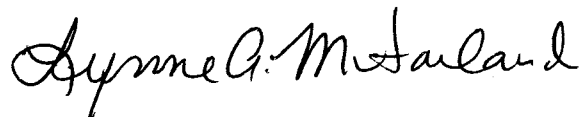
#### Audit Follow-up

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  
Christopher P. Hughey, Acting General Counsel

---

**FEDERAL ELECTION COMMISSION**

**Audit of Financial Statements**

**As of and for the Years Ended  
September 30, 2010 and 2009**

---

**Submitted By**

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

# TABLE OF CONTENTS

---

	<u>Page</u>
Independent Auditor’s Report.....	1
Summary .....	1
Opinion on the Financial Statements .....	2
Internal Control over Financial Reporting.....	2
1. Improvements Needed in Controls over Financial Reporting .....	3
2. IT Security Control Weaknesses.....	7
Compliance with Laws and Regulations.....	17
Appendix 1 - Status of Prior Year Recommendations.....	20
Appendix 2 - Agency Response to Draft Report .....	22



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, 2010 and 2009, 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, 2010 and 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. 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, 2010 and 2009, 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, 2010 and 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 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*. 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, 2010 and 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 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. Improvements Needed in Controls over Financial Reporting**

#### **a. Accrual of Accounts Payable in Error**

The FEC's controls over the accrual of payables for financial statement presentation and the posting of these entries to the general ledger were not effectively implemented. Our review of September 30, 2010 financial statements, and a sample of transactions processed during Fiscal Year 2010 identified a duplicate accrual of \$139,969.99 posted to the general ledger by Office of the Chief Financial Officer (OCFO) personnel. We attributed this problem to the need for more effective implementation of controls over the accounts payable accrual process.

The error we identified occurred when an accounting clerk did not follow OCFO policy to ensure that the invoice payment was not pending in Pegasys prior to recording the accrual transaction. In addition, while the OCFO's supervisory review process detected this error, actions were not taken to ensure that the error was, in fact, corrected. When discovered during the audit, OCFO personnel adjusted the financial statements to correct the error. If left uncorrected, liabilities on FEC's 2010 Balance Sheet and costs on the 2010 Statement of Net Cost (SNC) would have been overstated by approximately \$140,000. Conversely, had this error not been corrected, costs on the 2011 SNC would have been understated by this same amount.

OCFO officials advised they plan to review the current accounts payable accrual process, and determine if there is a better approach to calculating the accrual estimate. They have agreed that once the OCFO ensures that the appropriate process is in place, the OCFO will train staff.

Statement of Federal Financial Accounting Standards (SFFAS) No. 1, *Accounting for Selected Assets and Liabilities*, provides that for financial reporting purposes, liabilities are recognized when goods and services are received or are recognized

based on an estimate of work completed under a contract or agreement. Paragraph 77 states “When an entity accepts title to goods, whether the goods are delivered or in transit, the entity should recognize a liability for the unpaid amount of the goods. If invoices for those goods are not available when financial statements are prepared, the amounts owed should be estimated.”

### **Recommendation**

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.

### **Agency Response**

Management concurs that controls over the accounts payable accrual process should be strengthened to ensure that potential misstatements are identified and corrected in a timely manner. However, FEC management does not concur that the \$140 thousand misstatement noted in the auditor’s report contributes to a significant deficiency in internal control over financial reporting.

During FY 2011, management will perform the following to strengthen controls over the accounts payable accrual process:

- Perform a comprehensive review of the accounts payable accrual processes; and
- Provide additional training to ensure that agency guidelines are followed and that transactions are processed, reviewed, and reconciled consistently, completely, timely, and accurately.

### **Auditor Comments**

We identified this error during our final testing of 2010 transactions. Our testing during FY 2009 also identified two invoices that were improperly recorded. The error in FY 2010 was identified by OCFO personnel but not corrected during supervisory review. We believe this represents a deficiency in implementation of internal controls, and does not represent “an isolated event” as stated by FEC officials since the auditors have reported problems in this area the last four years.

#### **b. FEC Needs to Convert Manual Accounting Systems**

FEC has not yet converted all manual systems and processes to automated systems that are integrated or interfaced with the core accounting system as we recommended in our prior audit. We attribute the problem in part, to: (1) difficulty in coordinating with FEC’s service providers on the development of a time-phased plan to convert the manual interface of payroll systems and processes to automated systems, and (2) the opinion of OCFO personnel that the costs to

convert the manual accounts receivable processes exceed the benefits of automating the system.

FEC uses spreadsheets and an outdated PeopleSoft platform to perform selected accounting operations. The financial management processes that still utilize significant manual operations include:

- Accounting for collections of fines and penalties. The OCFO requests accounts receivable information from three divisions. After the OCFO obtains the relevant information, the data is input into a spreadsheet. A standard voucher is prepared monthly and submitted to the service provider to record the accounting 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 month after the standard voucher is posted to the general ledger does the accounts receivable reflect an accurate balance.
- The payroll system does not interface with the accounting system; therefore, FEC must use a PeopleSoft application that is no longer supported. This process also requires FEC to perform manual operations to reconcile the payroll data and prepare standard vouchers to input the payroll data into its accounting system. OCFO is actively working with its payroll service provider to interface the payroll system and the core accounting system.

OMB Circular No. A-127, *Financial Management Systems*, 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. The core financial system is specifically used for collecting, processing, maintaining, transmitting, and reporting data regarding financial events. Other uses include supporting financial planning, budgeting activities, and preparing financial statements. Any data transfers to the core financial system must be: traceable to the transaction source; posted to the core financial system in accordance with applicable guidance from the Federal Accounting Standards Advisory Board (FASAB); and in the data format of the core financial system.

OCFO officials concurred that FEC should consider automating manual processes whenever it is appropriate and cost-effective to do so. However, OCFO officials believe that it is not cost-effective to convert its manual accounts receivable system. Concerning the continued use of the PeopleSoft application that is no longer supported, OCFO officials advised that FEC has held several meetings over the course of FY 2010 to evaluate the potential risks, benefits, and cost-effectiveness of a direct interface between the National Finance Center (NFC) Payroll and Personnel System and General Services Administration (GSA) Pegasys Financial Management System.

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.

### **Recommendation**

2. Convert FEC manual systems and processes to automated systems that are integrated or interfaced with the core accounting 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. As an example, the FEC converted its fixed assets to the General Services Administration (GSA) Fixed Asset System (Subsidiary Ledger) which has a direct interface within the GSA Financial Management System, effective in FY 2010.

Management disagrees with the recommendation that all manual processes should be automated. OMB Circular A-127, as revised, 2009, states that a financial management system *“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 FEC continues to evaluate the roles and responsibilities of all stakeholders to establish an electronic interface between NFC and GSA payroll and financial management systems and plans to complete the integration of those systems in FY 2011.

Additionally, 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. Doing so would provide little benefit to the agency or the Federal Government. This practice is consistent with the latest draft of A-127 circulated October 15, 2010.

### **Auditor Comments**

In recent testimony before the U.S. House Oversight and Government Reform Subcommittee on Government Management, Organization, and Procurement; the Controller, Office of Management and Budget, stated that the financial management environment is changing from producing annual audited financial statements to producing financial reports more frequently, at a more granular

level, and accompanied by non-financial information. The Controller further noted that agencies' financial systems are not sufficiently flexible or integrated with non-financial systems. In particular, OMB and Treasury, in coordination with the CFO Council, are working to deploy central, automated solutions that will reduce the cost and complexity of agency financial operations. The Controller concluded that federal agencies need to modernize their systems.

In addition, we noted that a recent GAO report and correspondence from OMB provide that OMB has plans underway to, "...upgrade the quality and performance of federal financial management systems by leveraging shared service solutions and implementing other government wide reforms that foster efficiencies in federal financial operations. According to OMB, the goals ... are to (1) provide timely and accurate data for decision making; (2) facilitate stronger internal controls that ensure integrity in accounting and other stewardship activities; (3) reduce costs by providing a competitive alternative for agencies to acquire, develop, implement, and operate financial management systems through shared service solutions; (4) standardize systems, business processes, and data elements; and (5) provide for seamless data exchange between and among federal agencies by implementing a common language and structure for financial information and system interfaces."

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 also reported by the predecessor auditors as part of a material weakness in the 2008 audit report, and in our 2009 financial statement audit report.

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

FEC has either implemented corrective actions or has plans developed to address most of the IT control weaknesses we reported in our 2009 financial statement audit report. However, we found in our 2010 audit that some controls were not effectively implemented, and for two areas FEC did not agree to implement our recommendations. We attributed these conditions, in part, to the complexity of issues involved, and the funding necessary to complete all planned actions. As a result, FEC information and information systems are at additional risk until these corrective actions are fully implemented. Details of the issues noted during our 2010 audit are discussed below.

### **a. Configuration Management and FDCC Security Controls**

Additional actions are necessary before FEC meets best practices for configuration control, and Federal Desktop Core Configuration (FDCC) requirements. While FEC has established baseline configuration standards for a number of its systems, these standards were not effectively implemented for the laptops we tested.

The FEC established baseline configuration security standards that identify specific services, such as Universal Plug and Play, Netmeeting Remote Desktop Sharing, Remote Desktop Help Session Manager, and Remote Registry access that should be disabled unless there is a specific business need for these services. However, our audit tests showed that these services had not been disabled, and users could manually start these services on laptop computers.

In addition, the baseline configuration security standards required that on Windows XP machines the “administrator account” be renamed, and that access to administrator authorities is limited to users requiring such access. Based on our tests, we determined that users were provided local administrator rights allowing them to change settings, as well as the ability to start “services” manually. By using these authorities, users could, among other activities, override the FEC control setting which requires re-authentication after 30 minutes of inactivity.

FEC has not yet fully implemented FDCC security control requirements that OMB established in 1997 as “best practices” security requirements for Windows computers. FEC has established a project to adopt selected control requirements and estimates that full implementation of selected controls will not be implemented until 2012. Our tests showed the following FDCC requirements have not yet been adopted by FEC.

<b>Access Control Objective</b>	<b>FEC Settings</b>	<b>FDCC Requirements</b>	<b>Meets or exceed FDCC</b>
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
Suspend inactive account	FEC activates screen saver; does not suspend session	15 minutes	No

FEC plans to implement the FDCC requirements that the agency agrees to adopt in a phased approach for new workstations. FEC estimated implementation would be completed by 2012.

NIST Special Publications 800-53, *Recommended Security Controls for Federal Information Systems*, provides the minimum controls that an agency should adopt in order to implement a configuration management control process.

We discussed these issues during our audit with Office of the Chief Information Officer (OCIO) officials who concurred with our recommendations. OCIO officials advised they meet about 75 percent of FDCC requirements, and have

plans to meet additional requirements when the FEC implementation process has been completed.

### **Recommendations**

3. Ensure that FEC baseline configuration standards are implemented in accordance with FDCC requirements for all workstations.
4. Perform periodic assessments of baseline configuration settings as part of FEC's continuous monitoring program.

### **Agency Response**

Management partially concurs with these recommendations and plans to make use of these best practices once the FEC's FDCC project is fully implemented. However, the FEC reserves the right to implement only those settings that it considers advantageous to its computing environment. As indicated, FEC is already 75 percent FDCC compliant, and has developed a plan and timetable to achieve near 93 percent compliance. Per FDCC specifications, any recommended setting not implemented will include a documented justification.

### **Auditor Comments**

FEC officials have partially concurred in our recommendations. However, FEC officials have reserved the right to implement only those settings that the agency considers advantageous to its operations. As discussed in OMB's implementing guidance, OMB has determined that the FDCC settings provide the best approach to strengthening the security over workstations that operate in a Windows environment. We continue to believe that FEC should follow OMB guidance in this important IT security area.

#### **b. Scanning Process Needs Strengthening**

While FEC has established a framework to perform periodic vulnerability scanning, including a process to address the vulnerabilities identified through its scanning processes, workstations connected to the network are currently excluded from the FEC's vulnerability scanning program. Without scanning of the individual workstations, FEC cannot detect potential vulnerabilities and assure that the devices are properly configured to meet FDCC and/or FEC security configurations.

NIST Special Publications 800-53 establishes vulnerability scanning as one of the recommended security controls in the risk assessment control area. The control requirement provides that the organization scans for vulnerabilities in the information system and hosted applications, including when new vulnerabilities potentially affecting the system/applications are identified and reported.

During our audit, we discussed this matter with OCIO officials and they advised us that they plan to perform additional workstation scanning once the FEC's FDCC project is fully implemented. OCIO officials added that they realize additional workstation scanning will help ensure continued adherence to best practices.

### **Recommendation**

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.

### **Agency Response**

Management concurs with this recommendation, and plans to make use of additional workstation vulnerability scanning once the FEC's FDCC project is fully implemented. As a proactive solution and compensating control, the FEC has implemented an automated patching process to ensure all workstation operating system vulnerabilities are properly patched. Other compensating controls the Commission employs are real-time virus and adware detection. The Commission specifically scans workstations hard-drives, CD-ROMs, and flash drives for malicious code such as viruses; worms, trojan horses, spyware, keyboard loggers etc. Additional levels of workstation security includes workstation firewalls, real-time virus and adware detection and prevention, operating system and application password standards, two factor authentication, whole hard drive encryption, and 15 minute account lock-out.

### **Auditor Comments**

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

#### **c. Termination of Separated Employees Access Authorities**

Controls established by FEC to ensure that separated employees access to the FEC network are timely removed did not function as designed. FEC policies and standards require the access authorities to be disabled within one business day, except for emergency situations when the account will be disabled immediately.

FEC implemented the FEC System Access (FSA) system to control the addition and termination of users to its systems. We performed tests of this system as part of our 2010 tests of IT controls. We sampled 11 persons who had separated from FEC during the 2010 fiscal year, and obtained information from OCIO personnel as to the date the individuals' access to the FEC network was disabled or terminated. OCIO officials advised us that operational problems occurred, and FEC did not have the dates that these employees were removed from the network.



We performed additional tests of personnel who separated after June 2, 2010, to determine if the problem impacting our original sample was corrected. We identified 14 persons who separated after June 2, 2010. Of this number, we found that seven employees' accounts were not disabled until 5 to 41 days after the employee separated.

We discussed this condition during the audit with OCIO officials who advised that they investigated the situation, and verified that there was a lack of communication between the affected offices. OCIO officials advised us that management has formed a team to resolve any residual communication issues, implement additional fail-safe methods to ensure the OCIO is notified about separations in a timely manner, and implement a policy and associated procedures to ensure consistency throughout the entire termination process.

### **Recommendation**

6. Implement additional controls to ensure that former employees' access to the network is terminated in accordance with FEC policies.

### **Agency Response**

Management concurs with this finding and recommendation. Management investigated the situation and verified that there was indeed a lack of communication between the affected offices. Since that time, the Commission has formed a management team to first resolve any residual communication issues and secondly develop and implement a policy (and associated procedures) to ensure access to FEC information resources are properly terminated.

### **Auditor Comments**

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

#### **d. Access Controls Need Further Strengthening**

FEC needs to further strengthen access controls by implementing a user access authority certification process, and by implementing best practice controls over dial-up access to the FEC network.

FEC acquired software in October 2009 to assist the agency in identifying users' specific access authorities, and had established a project to develop processes to implement this control requirement. However, because of the complexities involved with the configuration of the system, identifying the files and folders to which users have access, and ensuring the documentation provided to managers is informative and useful; the project implementation has been delayed.

We also compared FEC's controls for remote access to best practice requirements, and found that FEC had not implemented sufficient controls for its dial-up access. Best practices require, among other things, the organization to employ automated mechanisms to facilitate the monitoring and control of remote access methods, and the use of cryptography to protect the confidentiality and integrity of remote access sessions. During the period of our review, we determined that the dial-up access for FEC currently did not meet the requirements relating to the use of cryptography to protect the information transmitted. 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.

During our audit, we discussed these issues with OCIO officials. Concerning the review of user access authorities, we were advised that management is currently reassessing the resources and timeline required to provide useful network access information to users' supervisors. In addition, OCIO officials advised that after performing a cost-benefit analysis of adding encryption to an already slow and rarely used dial-up service, the Commission has concluded it will be suspending its dial-up services as of September 30, 2010.

### **Recommendations**

7. Assure sufficient resources are provided to complete the project dealing with the establishment of processes to enable periodic review of users' access authorities.
8. Require that dial-up access is properly secured as required by best practices, or terminate this type of access for users.

### **Agency Response**

Management concurs with these recommendations and is currently reassessing the resources and timeline required to overcome the complexities involved with ensuring that technical information provided to non-technical business managers is informative and useful enough to make educated decisions about system access.

After performing a cost-benefit analysis of adding encryption to an already slow and rarely used dial-up service, the Commission has concluded it would be more cost efficient to concentrate its efforts on continuing to support its more secure and reliable high speed connection. With this in mind, the Commission has suspended its dial-up services as of September 30, 2010.

### **Auditor Comments**

Since FEC officials have agreed to implement the recommendations, we have no additional comments.

#### **e. Security Awareness Training**

FEC needs to strengthen its control processes dealing with security awareness training and obtaining acknowledgement of rules of behavior for new employees and contractors. During our 2010 testing, we reviewed records detailing security awareness training provided to FEC employees and contractors. We found that for new employees and contractors the FEC does not require these personnel to receive the security awareness training, and acknowledge rules of behavior, prior to granting access to the FEC general support system. For example, we identified 10 users that received the training two weeks or longer after coming onboard, or the records showed the individuals had never completed the training.

OMB Circular A-130, Appendix III, General Support Systems, the document we used to determine best practices, requires that agencies provide security awareness training and rules of behavior to personnel prior to granting access to an agency's systems.

OCIO officials advised us that the FEC believes strengthening its Security Awareness Program would benefit the Commission. To this end, the FEC has decreased the training completion period for new employees to one business week from the date of hire. In our opinion, and as required in OMB Circular A-130, it is important that new employees and contractors become aware of privacy and security requirements prior to being allowed access to agency information and information systems.

#### **Recommendation**

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.

#### **Agency Response**

Management partially concurs with this finding and recommendation. Although six of the 10 cited were still within FEC policy of three weeks to complete security awareness training and the remaining four would have been notified of their non-compliance during the 2010 security awareness completion review, the FEC does believe strengthening its Security Awareness Program would benefit the Commission. To this end, the FEC has decreased the three week completion period for new employees to one business week.

#### **Auditor Comments**

FEC officials partially concurred with our recommendation, and agreed to reduce the period for completing the security awareness training to one business week. We concur with this alternate approach to our recommendation.

**f. Contingency Planning and COOP**

In 2009, we reported that the FEC had developed a Plan of Action and Milestones (POA&M) and made progress in developing a contingency plan and Continuity of Operations Plan (COOP) document that meets federal requirements and best practices. For 2010, we found that FEC had not yet completed the testing of the contingency plan and had not finalized the COOP. The FEC POA&M showed that the anticipated completion date for full development of the COOP and contingency plan, including testing of the plans is scheduled for November 2010. FEC officials advised us that the project was delayed due to funding issues.

**Recommendation**

10. Monitor the POA&M to ensure that the documents are completed and fully tested by the end of the 2010 calendar year.

**Agency Response**

Management concurs with this recommendation.

**Auditor Comments**

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

**g. FEC Would Further Strengthen IT Security Program by Fully Adopting Best Practices**

FEC's IT security program would be further strengthened if the agency adopted the best practices included in the NIST computer security controls publications. FEC is exempt from the Federal Information Security Management Act (FISMA)<sup>1</sup> requirements, but could voluntarily adopt these best practices as other federal entities have elected to do.

NIST is required by law to develop IT security standards and guidelines, and to consult with other federal agencies and offices, as well as the private sector to improve information security and avoid unnecessary and costly duplication of efforts in establishing security control requirements. NIST, in addition to its comprehensive public review and vetting process, 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

---

<sup>1</sup> The E-Government Act (P.L. 107-347) recognizes the importance of information security to the economic and National security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

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, NIST notes that a common foundation for information security will also provide a strong basis for reciprocal acceptance of security authorization decisions and facilitate information sharing.

During our 2010 audit, we identified four other federal entities that were also exempt from FISMA requirements. To determine how these agencies addressed the establishment of IT security standards, we reviewed selected documentation from the agencies. Details follow.

Agency	Actions Taken by Agency
Government Accountability Office	GAO’s 2009 Performance and Accountability Report notes that even though GAO is not obligated by law to comply with FISMA, GAO has adopted FISMA requirements to strengthen its information security program. GAO added 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. GAO establishes its security standards based on the federal guidance found in the National Institute of Standards and Technology (NIST) 800 series and Federal Information Processing Standards publications. GAO further noted that as existing NIST guidance is updated and new guidance disseminated, GAO has adjusted its internal information technology security policies and procedures.
The Smithsonian Institution	The Institution’s website notes that the agency voluntarily complies with FISMA requirements because they are consistent with the agency’s IT strategic goals.
Department of Defense	Employ security controls equal or higher than FISMA minimum requirements.
Central Intelligence Agency	Employ security controls equal or higher than FISMA minimum requirements.

During our audit, we discussed this matter with OCIO officials who advised that they do not concur that FEC should adopt NIST standards as best practice. OCIO officials advised that it would be improper for the FEC to disregard the will of Congress. OCIO officials noted that it was not the original intent of NIST to impose a set of standards that all federal agencies must adhere to. OCIO officials advised that FEC does utilize NIST as one source of guidance when determining best practice.

As mentioned above, other exempt federal agencies have voluntarily adopted the FISMA requirements and NIST security standards. In addition, FEC’s Office of General Counsel provided correspondence, as part of documentation to update those statues, regulations and policies that are applicable and not applicable to FEC, that indicated that if FEC elected, the agency could adopt exempted

regulations as a model. Therefore, it appears that the General Counsel has already determined it is allowable for FEC to adopt exempted regulations.

As FEC officials discussed above, organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in NIST Special Publication 800-53. NIST notes that the minimum controls could be tailored up, down, or an agency could adopt another control commensurate with risk. FEC has rated the GSS as a moderate risk system and should adopt the NIST minimum controls to address the risks to this system, or other controls commensurate with risk. Due to FEC's significant reliance on information technology to support the agency's mission, adoption of the NIST IT security standards framework would improve the agency's ability to protect IT systems from constantly changing information security threats and risks. In addition, if FEC does not adopt a set of best practice security controls, FEC will have difficulty in setting security standards for FEC IT contractors' performance and will not have benchmarks to effectively monitor contractors performing sensitive IT security operations for FEC.

FEC officials have indicated that when the "FEC deviates from the NIST model it is only after careful evaluation, and it is believed that the agency has either a better or more cost effective method of achieving its IT security goals." FEC has decided not to implement strengthened access controls due to user concerns. FEC did not provide an analysis of the risks to the system due to this lessening of minimum control requirements, establish alternative control processes, or perform any other analytical review that would support agency decisions for deviations from IT security best practices. While longer passwords, more frequent password changes, and less frequent use of the same password all add complexities to users, decisions should be primarily based on a risk-based analysis.

### **Recommendation**

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*.

### **Agency Response**

Management disagrees with this finding and recommendation except to the extent it acknowledges that the FEC may choose to voluntarily apply National Institute of Standards and Technology ("NIST") IT security standards. As the report notes, information systems security standards promulgated by NIST are derived from the *Federal Information Security Management Act* ("FISMA"), 44 U.S.C. 3541 et seq. FISMA incorporates the *Paperwork Reduction Act's* definition of "agency," which specifically excludes the Commission. See 44 U.S.C. 3502(1) (B). Accordingly, FISMA's requirement that agencies follow NIST guidelines is not

applicable to the Commission. Nevertheless, the FEC has voluntarily adopted some of these best practices on a case-by-case basis, based on its own assessment of risk, and reserves the right to implement only practices that it considers advantageous to its computing environment.

### **Auditor Comments**

We believe that FEC's IT security program would be strengthened by adopting and meeting the NIST minimum security requirements. As noted in the report, other agencies that are exempt from FISMA compliance have agreed to adopt the NIST security requirements. For example, GAO has 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." We believe that FEC would achieve the same level of assurance if it adopted the FISMA requirements.

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

We noted other control deficiencies over financial reporting and its operation that we have reported to the management of the FEC and those charged with governance in a separate letter dated November 12, 2010.

### **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).

Under OMB Bulletin 07-04, auditors are generally required to report whether the agency's financial management systems substantially comply with the federal financial management systems requirements, applicable federal accounting standards, and the United States Government Standard General Ledger at the transaction level specified in the Federal Financial Management Improvement Act (FFMIA). The Accountability of Tax Dollars Act, which requires the FEC to prepare and submit audited financial statements to Congress and the Director of OMB, did not extend to FEC the requirement to comply with FFMIA.

### **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.

#### **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, P.C.*  
Leon Snead & Company, P.C.  
November 12, 2010

**Status of Prior Year Reportable Conditions, and  
Non-Compliance with Significant Laws and Regulations**

Recommendation	Status As Of September 30, 2010
1. Strengthen controls over the accruals of accounts payable, and ensure that supervisory reviews of accounts payable accruals are performed.	Recommendation open – reported in current year significant deficiency.
2. Update OCFO policies to incorporate the new strengthened processes for indentifying and posting accounts payable accruals.	Recommendation closed.
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.	Recommendation closed.
4. Update and issue the Accounting Manual within the next six months.	Recommendation closed.
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.	Recommendation closed.
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.	Recommendation open – reported in current year significant deficiency.
7. Formally adopt as a model for FEC the NIST IT security controls established in FIPS 200, <i>Minimum Security Requirements for Federal Information and Information Systems</i> , and SP 800-53, <i>Recommended Security Controls for Federal Systems and Organizations</i> .	Recommendation open – reported in current year significant deficiency.
8. Perform an annual independent assessment to determine whether FEC’s agency-wide IT security program meets minimum security controls established by NIST.	Recommendation closed. <sup>2</sup>
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.	Recommendation open – reported in current year significant deficiency.
10. Adopt Federal Desktop Core Configuration (FDCC) standards and implement these standards by the end of the 2010 fiscal year.	Recommendation open – reported in current year significant deficiency.
11. Include workstations and devices attached to the network in periodic scans performed by FEC.	Recommendation open – reported in current year significant deficiency.
12. Maintain documentation showing actions taken to address the problems identified by the vulnerability scans.	Recommendation closed.
13. Implement best practice controls over FEC’s dial-up access.	Recommendation open – reported in current year significant deficiency.

<sup>2</sup> This recommendation is closed since the OIG has the authority to perform such an audit.

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.	Recommendation open – reported in current year significant deficiency.
15. Develop an OCIO policy that requires standards, guidelines and policies to be dated, authenticated with a signature, and scheduled for review and update.	Recommendation closed.
16. Prepare a detailed POA&M for items identified in the risk assessment of the GSS.	Recommendation closed.
17. FEC should develop and enforce policies and procedures for debt collection that will ensure compliance with the DCIA and OMB A-129.	Recommendation closed.

**Federal Election Commission  
2010 Financial Statement Audit  
Management Responses to Audit Findings**

**Auditor Recommendation #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.

**Management Response to Recommendation #1:** Management concurs that controls over the accounts payable accrual process should be strengthened to ensure that potential misstatements are identified and corrected in a timely manner. However, FEC management does not concur that the \$140 thousand misstatement noted in the auditor's report contributes to a significant deficiency in internal control over financial reporting. The results of audit testing and FEC management's own subsequent review of the accounts payable accrual indicated that this error was an isolated event and not indicative of a systemic breakdown in internal controls. In addition, the noted misstatement is immaterial to the FEC's financial statements. Total liabilities for the FEC were \$7.7 million as of September 30, 2010, and the overstatement to accounts payable of \$140 thousand represented two tenths of a percent (0.20%) of the Net Cost of Operations.

During FY 2011, management will perform the following to strengthen controls over the accounts payable accrual process:

- Perform a comprehensive review of the accounts payable accrual processes; and
- Provide additional training to ensure that agency guidelines are followed and that transactions are processed, reviewed, and reconciled consistently, completely, timely, and accurately.

**Auditor Recommendation #2:** Convert FEC manual systems and processes to automated systems that are integrated or interfaced with the core accounting system.

**Management Response to Recommendation #2:** Management concurs that it is important for agencies to consider automating manual processes whenever it is appropriate and cost-effective to do so. As an example, the FEC converted its fixed assets to the General Services Administration (GSA) Fixed Asset System (Subsidiary Ledger) which has a direct interface within the GSA Financial Management System, effective in FY 2010.

Management disagrees with the recommendation that all manual processes should be automated. OMB Circular A-127, as revised, 2009, states that a financial management system "*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 FEC continues to evaluate the roles and responsibilities of all stakeholders to establish an electronic interface between NFC and GSA payroll and financial management systems and plans to complete the integration of those systems in FY 2011.

Additionally, 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. Doing so would provide little benefit to the agency or the Federal Government. This practice is consistent with the latest draft of A-127 circulated October 15, 2010.

**Auditor Recommendation #3:** Ensure that FEC baseline configuration standards are implemented in accordance with FDCC requirements for all workstations.

**Auditor Recommendation #4:** Perform periodic assessments of baseline configuration settings as part of FEC's continuous monitoring program.

**Management Response to Recommendations #3 and #4:** Management partially concurs with these recommendations and plans to make use of these best practices once the FEC's FDCC project is fully implemented. However, the FEC reserves the right to implement only those settings that it considers advantageous to its computing environment. As indicated, FEC is already 75 percent FDCC compliant, and has developed a plan and timetable to achieve near 93 percent compliance. Per FDCC specifications, any recommended setting not implemented will include a documented justification.

**Auditor Recommendation #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.

**Management Response to Recommendation #5:** Management concurs with this recommendation, and plans to make use of additional workstation vulnerability scanning once the FEC's FDCC project is fully implemented. As a proactive solution and compensating control, the FEC has implemented an automated patching process to ensure all workstation operating system vulnerabilities are properly patched. Other compensating controls the Commission employs are real-time virus and adware detection. The Commission specifically scans workstations hard-drives, CD-ROMs, and flash drives for malicious code such as viruses; worms, trojan horses, spyware, keyboard loggers etc. Additional levels of workstation security includes workstation firewalls, real-time virus and adware detection and prevention, operating system and application password standards, two factor authentication, whole hard drive encryption, and 15 minute account lock-out.

**Auditor Recommendation #6:** Implement additional controls to ensure that former employees' access to the network is terminated in accordance with FEC policies.

**Management Response to Recommendation #6:** Management concurs with this finding and recommendation. Management investigated the situation and verified that there was indeed a

lack of communication between the affected offices. Since that time, the Commission has formed a management team to first resolve any residual communication issues and secondly develop and implement a policy (and associated procedures) to ensure access to FEC information resources are properly terminated.

**Auditor Recommendation #7:** Assure sufficient resources are provided to complete the project dealing with the establishment of processes to enable periodic review of users' access authorities.

**Auditor Recommendation #8:** Require that dial-up access is properly secured as required by best practices, or terminate this type of access for users.

**Management Response to Recommendations #7 and #8:** Management concurs with these recommendations and is currently reassessing the resources and timeline required to overcome the complexities involved with ensuring that technical information provided to non-technical business managers is informative and useful enough to make educated decisions about system access.

After performing a cost-benefit analysis of adding encryption to an already slow and rarely used dial-up service, the Commission has concluded it would be more cost efficient to concentrate its efforts on continuing to support its more secure and reliable high speed connection. With this in mind, the Commission has suspended its dial-up services as of September 30, 2010.

**Auditor Recommendation #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.

**Management Response to Recommendation #9:** Management partially concurs with this finding and recommendation. Although six of the 10 cited were still within FEC policy of three weeks to complete security awareness training and the remaining four would have been notified of their non-compliance during the 2010 security awareness completion review, the FEC does believe strengthening its Security Awareness Program would benefit the Commission. To this end, the FEC has decreased the three week completion period for new employees to one business week.

**Auditor Recommendation #10:** Monitor the POA&M to ensure that the documents are completed and fully tested by the end of the 2010 calendar year.

**Management Response to Recommendation #10:** Management concurs with this recommendation.

**Auditor Recommendation #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*.

**Management Response to Recommendation #11:** Management disagrees with this finding and recommendation except to the extent it acknowledges that the FEC may choose to

voluntarily apply National Institute of Standards and Technology (“NIST”) IT security standards. As the report notes, information systems security standards promulgated by NIST are derived from the *Federal Information Security Management Act* (“FISMA”), 44 U.S.C. 3541 et seq. FISMA incorporates the *Paperwork Reduction Act’s* definition of “agency,” which specifically excludes the Commission. See 44 U.S.C. 3502(1)(B). Accordingly, FISMA’s requirement that agencies follow NIST guidelines is not applicable to the Commission. Nevertheless, the FEC has voluntarily adopted some of these best practices on a case-by-case basis, based on its own assessment of risk, and reserves the right to implement only practices that it considers advantageous to its computing environment.

# 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](mailto: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.**