

FEDERAL ELECTION COMMISSION

OFFICE OF INSPECTOR GENERAL



FINAL REPORT

**Audit of the Federal Election Commission's
Fiscal Year 2007 Financial Statements**

November 2007

ASSIGNMENT No. OIG-07-01

Table of Contents

Transmittal Memorandum

Independent Auditor's Report.....1

Independent Auditor's Report on Compliance and Other Matters.....3

Independent Auditor's Report on Internal Control.....4



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 2007 Financial Statements

DATE: November 15, 2007

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 and accompanying Independent Auditor's Reports on Internal Control and Compliance and Other Matters issued by Clifton Gunderson LLP (CG-LLP) for the fiscal year ending September 30, 2007. The audit was performed by CG-LLP under a contract with and monitored by the Office of Inspector General (OIG) in accordance with *Government Auditing Standards* and Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*, as amended.

Opinion on the Financial Statements

The audit included an examination, on a test basis, of evidence supporting the amounts and disclosures in the financial statements. The audit also included assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall principal statements' presentation.

The CG-LLP report concluded that the Federal Election Commission's (FEC) financial statements present fairly, in all material respects, the financial position of the FEC as of September 30, 2007 and 2006, and its net cost, changes in net position, budgetary resources, and custodial activity for the years then ended in conformity with accounting principles generally accepted in the United States of America.

In the Independent Auditor's Report for the prior fiscal year, dated November 7, 2006, CG-LLP expressed a qualified opinion on the FY 2006 statement of net cost because the auditors were not able to obtain sufficient competent audit evidence to support the FEC's allocation of program costs. Since the FEC has changed the presentation of program

costs in its statement of net cost, the present opinion on the FY 2006 financial statements is different from that expressed in the previous report.

Report on Internal Control

CG-LLP's planning and performance of the audit included consideration of the FEC's internal control over financial reporting as a basis for designing audit procedures for the purpose of expressing an opinion on the financial statements and to comply with OMB Bulletin 07-04. The auditors did not test all internal controls relevant to operating effectiveness, such as those controls relevant to ensuring efficient operations, and consequently CG-LLP did not express an opinion on the agency's internal control over financial reporting.

The American Institute of Certified Public Accountants (AICPA) established standards on communicating deficiencies related to an entity's internal control over financial reporting identified by the auditors. As defined by the AICPA, a control deficiency exists when the design or operation of a control does not allow the agency's management or its employees, in the normal course of performing their assigned duties, to prevent or detect misstatements on a timely basis.

Auditors determine whether an internal control deficiency is a significant deficiency or a material weakness based on the factors of likelihood and magnitude. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affect the agency's ability to initiate, authorize, record, process, or report financial data reliability in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the agency's financial statements that is more than inconsequential will not be prevented or detected by the agency'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 agency's internal controls.

CG-LLP identified a significant deficiency in the area of:

- Information Technology (IT)

CG-LLP identified a material weakness in the area of:

- Integrated Financial Management System

Report on Compliance and Other Matters

FEC management is responsible for complying with laws and regulations applicable to the agency. To obtain reasonable assurance about whether the FEC's financial statements are free of material misstatements, CG-LLP performed tests of compliance with certain provisions of laws and regulations, non-compliance with which could have a direct and material effect on the determination of financial statement amounts, and certain laws and regulations specified in OMB Bulletin No. 07-04, such as the Anti-Deficiency Act and the Prompt Payment Act.

The results of CG-LLP's tests of compliance with laws and regulations described in the audit report disclosed no instances of noncompliance with the laws and regulations that are required to be reported under *Government Auditing Standards* and OMB Bulletin No. 07-04.

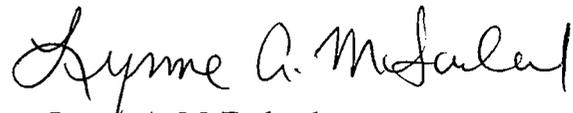
Audit Follow-up

The report on internal control contains recommendations to address weaknesses 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 Followup*, 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 Clifton Gunderson LLP's Audit Performance

In connection with the OIG's contract with CG-LLP, we reviewed CG-LLP's report and related documentation and inquired of its representatives. The OIG's review, as differentiated from an audit in accordance with U.S. generally accepted government auditing standards (GAGAS), was not intended to enable us to express, and we do not express, opinions on the FEC's financial statements or internal control or on the FEC's compliance with laws and regulations. CG LLP is responsible for the attached auditor's report and the conclusions expressed in the report. However, the OIG review disclosed no instances where CG-LLP did not comply, in all material respects, with GAGAS.

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



Lynne A. McFarland
Inspector General

Attachments

Cc: Chief Financial Officer
Staff Director
General Counsel
Chief Information Officer
Accounting Officer

Independent Auditor's Report

To the Inspector General of the
Federal Election Commission

We have audited the balance sheets of the Federal Election Commission (FEC) as of September 30, 2007 (FY 2007) and 2006 (FY 2006), and the related statements of net cost, changes in net position, budgetary resources, and custodial activity for the years then ended (hereinafter collectively referred to as the "financial statements"). These financial statements are the responsibility of the FEC's management. Our responsibility is to express an opinion on these financial statements based on our audits

We conducted our audits 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*. 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 examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statements' presentation. We believe our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of the FEC as of September 30, 2007 and 2006, and its net cost, changes in net position, budgetary resources, and custodial activity for the years then ended in conformity with accounting principles generally accepted in the United States of America.

In our report dated November 7, 2006, we expressed a qualified opinion on the FY 2006 statement of net cost because we were not able to obtain sufficient competent audit evidence to support the allocation of program costs. As described in Note 1, FEC has changed the presentation of program costs in its statement of net cost. Accordingly, our present opinion on the FY 2006 financial statements, as presented herein, is different from that expressed in our previous report.

In accordance with *Government Auditing Standards*, we have also issued our reports dated November 13, 2007 on our consideration of the FEC's internal control over financial reporting, and on our tests of the FEC's compliance with certain provisions of laws and regulations and other matters. The purpose of those reports is to describe the scope of our testing of internal

control over financial reporting and compliance and the results of that testing, and not to provide an opinion on the internal control over financial reporting or on compliance. Those reports are an integral part of our audit performed in accordance with *Government Auditing Standards* and should be considered in assessing the results of our audit.

The information in the Management Discussion and Analysis section is not a required part of the consolidated financial statements, but is supplementary information required by U.S. generally accepted accounting principles and OMB Circular No. A-136, *Financial Reporting Requirements*. We have applied certain limited procedures, which consisted principally of inquiries of management regarding the methods of measurement and presentation of this information. However, we did not audit this information and, accordingly, we express no opinion on it.

Our audits were conducted for the purpose of forming an opinion on the consolidated financial statements taken as a whole. The information in the Message from The Chairman, Performance Section, and Other Accompanying Information is presented for purposes of additional analysis and is not required as part of the consolidated financial statements. This information has not been subjected to auditing procedures and, accordingly, we express no opinion on it.

Clifton Henderson LLP

Calverton, Maryland
November 13, 2007

Independent Auditor's Report on Compliance and Other Matters

To the Inspector General of the
Federal Election Commission

We have audited the financial statements of the Federal Election Commission (FEC) as of, and for the year ended September 30, 2007, and have issued our report thereon dated November 13, 2007. We conducted our audit in accordance with the 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 07-04, *Audit Requirements for Federal Financial Statements*.

The management of FEC is responsible for complying with laws and regulations applicable to FEC. As part of obtaining reasonable assurance about whether FEC's financial statements are free of material misstatements, we performed tests of FEC's compliance with certain provisions of laws and regulations, non-compliance 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. We limited our tests of compliance to these provisions and we did not test compliance with all laws and regulations applicable to FEC. Providing an opinion on compliance with certain provisions of laws and regulations was not an objective of our audit, and, accordingly, we do not express such an opinion.

The results of our tests of compliance with laws and regulations described in the preceding paragraph disclosed no instances of reportable noncompliance or other matters that are required to be reported under U.S. generally accepted *Government Auditing Standards* or OMB Bulletin No. 07-04.

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

Clifton Gunderson LLP

Calverton, Maryland
November 13, 2007

Independent Auditor's Report on Internal Control

To the Inspector General of the
Federal Election Commission

We have audited the financial statements of the Federal Election Commission (FEC) as of and for the year ended September 30, 2007 and have issued our report thereon dated November 13, 2007. We conducted our audit in accordance with the 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*.

In planning and performing our audit, we considered FEC's internal control over financial reporting as a basis for designing our audit procedures for the purpose of expressing our opinion on the financial statements and to comply with OMB Bulletin 07-04, but not for the purpose of expressing an opinion on the effectiveness of FEC's internal control over financial reporting. We did not test all internal controls relevant to operating effectiveness as broadly defined by the *Federal Managers' Financial Integrity Act (FMFIA)* (31 U.S.C. 3512), such as those controls relevant to ensuring efficient operations. Accordingly, we do not express an opinion on the effectiveness of FEC's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and would not necessarily identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses. As discussed below, we identified certain deficiencies in internal control over financial reporting that we consider to be significant deficiencies.

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 affect the entity's ability to initiate, authorize, record, process, or report financial data reliability in accordance with generally accepted accounting principles such that there is more than a 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 controls.

Our consideration of the internal control over financial reporting was for the limited purpose described in the second paragraph of this section and would not necessarily identify all deficiencies in the internal control that might be significant deficiencies and, accordingly, would not necessarily disclose all significant deficiencies that are also considered to be material weakness. However, we believe that the significant deficiency in Integrated Financial Management System described below is a material weakness.

Finally, with respect to internal control related to performance measures reported in the FEC's Performance and Accountability Report as of September 30, 2007, we obtained an understanding of the design of significant internal controls relating to the existence and completeness assertions, as required by OMB Bulletin 07-04. Our procedures were not designed to provide assurance on internal control over reported performance measures, and, accordingly, we do not provide an opinion on such controls.

MATERIAL WEAKNESS

I. Integrated Financial Management System (Modified Repeat Finding)

A single, integrated financial management system is a unified set of financial systems linked together electronically in an efficient and effective manner to provide agency-wide financial management support. An integrated system should maintain an interrelationship between software, hardware, personnel, procedures, controls and data contained within the systems which allows users to obtain necessary information efficiently and effectively through electronic means. It does not necessarily mean having only one software application covering all financial management needs within an agency. Interfaces are acceptable as long as the supporting details are maintained and accessible to managers. Interface linkages must be electronic unless the number of transactions is so small that it is not cost beneficial to automate the interface. Easy reconciliation between systems, where interface linkage is appropriate, must be maintained to ensure data accuracy.

The FEC does not have an integrated financial management system. Its general ledger and core financial management system are housed in PeopleSoft (PS). However, significant financial activity, such as Obligations, Revenue, Accounts Receivable, Property, Plant and Equipment (PPE) and payroll transactions, originate outside of PS. Of these transactions, only the Payroll activity processed through the National Finance Center's (NFC) payroll system is automatically interfaced with the FEC's core financial system. Obligations, Revenue, Account Receivable and Property transactions are recorded in subsidiary schedules maintained in multiple excel spreadsheets and then manually posted to the general ledger. These spreadsheets support the flow of transactions throughout the year.

As a result of a lack of an integrated system, FEC goes through a process of compiling financial data in separate spreadsheets in a complex and time-consuming process to generate the financial statements. Although FEC reviews these spreadsheets, the risks of

error increase due to the inherent risk and limitations of a spreadsheet based application in an agency's financial management system. Some of these risks include:

- Substantial manual intervention is necessary, thereby increasing the risk of human error not being detected.
- Difficulty in tracking changes made to spreadsheets, including formula changes, preventing an adequate audit trail.
- Difficulty in verifying change controls and error correction changes made.
- Unique, new or non-recurring transactions are difficult to incorporate.
- Difficulty in performing automatic checks and balances on the transactions in the spreadsheets.
- Delay in recording transactions in the general ledger.
- Increase in the use of journal vouchers as a means for posting transactions to the general ledger.
- Substantial resources are spent processing transactions resulting in fewer resources for financial analysis and reporting.

These risks for errors were substantiated through our audit testing that identified the following control deficiencies:

- Accounting entries posted to the general ledger were not always sufficiently documented or documentation to support the entries was not always properly maintained.
- Accrued expenses reported on the June 30, 2007 financial statements were misstated due to a posting error.
- The change in gross accounts receivable transactions were not recorded in the interim statements of custodial activity (March 2007 and June 2007).
- Multiple budgetary accounting related issues occurred resulting in:
 - The Recoveries of Prior Year Obligations and Obligations Incurred line items of the June 30, 2007 and September 30, 2007 draft financial statements being misstated. The reconciliation between the fourth quarter SF-133 and Statement of Budgetary Resources (SBR) as of September 30, 2007 was performed using incorrect SF-133 data. Accordingly, the reconciliation did not reveal significant adjustments needed to the SBR and related financial statements, including a routine year-end adjusting entry of cancelling the 2002 fund.
 - FEC has not established the posting logic prescribed by Treasury for recording budget authority received under a continuing resolution. Furthermore, the FEC did not record apportionments in accordance with OMB Circular No. A-11, *Preparation, Submission and Execution of the Budget*. Specifically, FEC recorded the entire requested appropriation of \$54 million as budget authority in February 2007 even though the entire budget authority did not become available until April 2007. The incorrect entries increased the risk that the system's fund control may not have been effective, increasing the possibility that funds could have been obligated/expended in a manner that could have caused a violation of the Anti-Deficiency Act.
- FEC's obligating documents contained errors or were inconsistent with supporting documentation; thereby increasing the risk for disbursements to be applied to the

incorrect appropriation account or obligation. Specifically, we noted 2 out of 45 disbursements that were applied to the incorrect appropriation account.

- FEC did not prepare and submit to OMB an analysis of significant financial statement line item fluctuations between March 31, 2006 and March 31, 2007. Moreover, our review of the analyses performed in subsequent reporting quarters showed that the analyses were not performed timely and/or were not complete.
- FEC did not complete the Statement of Budgetary Resources (SBR) reconciliation to SF-133 Report on Budget Execution and Budgetary Resources for the quarters ending December 31, 2006, March 31, 2007 and June 30, 2007 as required by OMB Circular A-136.

FEC is aware of these risks and the need for an integrated financial management system. Accordingly, they plan to migrate a significant portion of their accounting function to the General Services Administration (GSA) during fiscal year 2008. In preparation for the migration, FEC is working with GSA to determine the feasibility of linking external systems not yet integrated to PeopleSoft.

Recommendations:

1. Assess the extent of financial management system integration needed for existing systems while outsourcing the accounting operations to a third party service provider.
2. Implement control activities to compensate for the lack of an integrated financial management system and to ensure that accounting transactions are recorded correctly, timely, reviewed, and with adequate supporting documentation. Some of these control activities should include, but not limited to:
 - Improving preparation and review of procurement documents, including purchase requests, purchase orders/contracts, and related supporting documentation.
 - Improving analytical and quality control review of journal vouchers, reconciliations and the financial statements, including interim financial statement.
 - Implementing proper and timely cut-off controls for processing transactions and in preparing the financial statements to allow for management's timely analysis of financial data and for audit purposes.
 - Establish a timeline for timely receipt of completed accounts receivable schedules by the finance office from the program offices.
3. Ensure that the general ledger setup and posting model definitions are in compliance with the latest transaction posting consistent with USSGL guidance and policies for recording and classifying transactions.
4. Provide employee training on procurement, appropriation law, budget execution, and financial reporting requirements, as applicable, to ensure financial reporting and fund control policies are consistently and accurately executed.
5. Ensure that FEC complies with regulatory agencies' reporting requirements.

Management Response:

Management generally concurs with the finding and recommendations. FEC management is committed to resolving the issues noted and has begun to address the recommendations. For example, FEC has entered into an agreement with GSA, an OMB-certified Line of Business provider, for financial services. FEC management has also begun to identify training opportunities for its staff to enhance awareness of sound financial management practices. FEC management will develop a corrective action plan addressing issues identified.

SIGNIFICANT DEFICIENCY

II. Information Technology (IT) (Modified Repeat Finding)

A. Commission-Wide Security Administration

An entity-wide security program should be in place to establish a framework and continuing cycle of activity to manage security risk, develop security policies, assign responsibilities, and monitor the adequacy of computer security related controls. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

During our Fiscal Year 2007 review of FEC's security program, we noted that FEC made progress in addressing prior years' findings, notably a contract was recently awarded to conduct a risk assessment of FEC's major applications and general support systems. The information obtained from this risk assessment will be used to adjust and fully implement its information classification, certification and accreditation policies.

However, at the time of this review, FEC's existing security program revealed weaknesses in controls that expose the FEC's financial management systems and data to unauthorized access and/or modification. Security weaknesses noted included:

- Risk assessments have not been performed as part of FEC's overall strategy to mitigate risks associated with its IT environment. **(Repeat Finding)**
- FEC has not fully implemented a framework of policies and standards to mitigate risks associated with the management of its information resources. Although FEC has implemented the majority of its information security policies, it has not fully implemented all of the related procedures and standards. FEC has not finalized and implemented an information classification policy, as well as its certification and accreditation policy. **(Repeat Finding)**
- FEC has created security plans for all of its major applications and mission critical general support systems. However, these security plans are not consistent with best practices "Risk Management Cycle", as they are not based on an assessment of the risks to FEC systems. **(Repeat Finding)**

- Major applications and mission critical general support systems have not been certified and accredited to ensure that they are operating according to FEC's security requirements. **(Repeat Finding)**.
- FEC could not provide evidence to show that background investigations were performed timely for 3 out of the 10 newly hired employees that we sampled (30%). **(New Finding)**.

Recommendations:

6. Perform risk assessments, as part of FEC's overall strategy to mitigate risks associated with its IT environment.
7. Finalize and implement FEC's information classification policy and certification and accreditation policy along with any accompanying standards.
8. Incorporate the results of risk assessments into FEC security plans.
9. Certify and accredit all major applications and mission critical general support systems.
10. Refine procedures to ensure that all newly hired employees undergo the appropriate background investigations commensurate with the risk level of their position. FEC should also ensure these investigations are initiated within a reasonable time of employment start date.

Management Response:

FEC agrees with the majority of elements within this finding and believes that conducting a comprehensive risk assessment is a prudent course of action and consistent with its Risk Management Policy. To that end, FEC has re-issued a previous "Request for Proposal" (RFP). The contract was recently awarded to conduct a risk assessment of FEC's major applications and general support systems. The information obtained from this risk assessment will be utilized to adjust and fully implement its information classification, and certification and accreditation policies. The data sensitivity and criticality information obtained will be incorporated into the appropriate FEC system security plans. This risk assessment contract deliverables include a risk remediation plan and strategy. This remediation plan will be incorporated into the overall ITD Corrective Action Plan (CAP).

The modified system security plans, risk assessment and the resulting risk remediation plan will be included as major components of the certification and accreditation package for senior management to analyze in its decision to provide either an Authorization To Operate (ATO) or an Interim Authorization To Operate (IATO).

B. Disaster Recovery and Continuity of Operations

Losing the capability to process and protect information maintained on FEC's computer systems can significantly impact FEC's ability to accomplish its mission. The purpose

of disaster recovery and continuity of operations controls is to ensure that, when unexpected events occur, critical operations continue without interruption or critical operations are promptly resumed.

To achieve this objective, FEC should have procedures in place to protect information resources and minimize the risk of unplanned interruptions and a plan to recover critical operations should interruptions occur. These plans should consider activities performed at FEC's general support facilities (e.g. FEC's local area network, wide area network, and telecommunications facilities), as well as the activities performed by users of specific applications. To determine whether the disaster recovery plans will work as intended, FEC should establish and periodically test the capability to perform its functions in disaster simulation exercises.

Our review of the service continuity controls identified weaknesses that could affect FEC's ability to respond to a disruption in business operations after a disaster or other interruption. Details of the matter are as follows:

- FEC has not performed a business impact analysis (BIA) to formally identify and prioritize all critical data and operations on its networks and the resources needed to recover them if there was a major interruption or disaster. In addition, FEC has not established emergency processing priorities that will help manage disaster situations more effectively for the network. **(Repeat Finding)**
- FEC has not established an alternate processing site for its operations in the event of a disaster. **(Repeat Finding)**
- FEC's contingency plan is not comprehensive, as it does not include steps for recovering all FEC's major applications and mission critical general support systems. Additionally, the plan does not prioritize resources or set a timeframe for recovery. **(Repeat Finding)**
- FEC has not developed a continuity of operations plan (COOP) to support the continuation of its core mission in the event of a disaster that renders FEC's facilities unusable. **(Repeat Finding)**

Recommendations:

11. Perform a BIA to formally identify and prioritize all critical data and operations on FEC's networks and the resources needed to recover them if there is a major interruption or disaster.
12. Establish an alternate processing site and incorporate the results of the BIA into the contingency plan.
13. Develop a comprehensive contingency plan that incorporates the results of the BIA and includes the procedures and resources necessary to restore FEC systems in the event of a disaster. Ensure emergency processing priorities are established to assist in managing disaster situations, and ensure once developed, the plan is tested annually and updated based on the results of these tests.

14. Develop a COOP that addresses measures and procedures to follow in the event of a long-term interruption.

Management Response:

FEC agrees that a formal BIA would be useful and recently awarded a contract to develop a comprehensive disaster recovery plan. A component of this contract is to assist FEC in formally identifying and prioritizing all critical data and operations on its networks and the resources needed to recover them in the event of a disaster. Determine gaps in current plans and strategies to close the identified gaps on a priority basis (i.e. risk, value derived, cost, time). The vendor will then assist FEC with utilizing the data gleaned from this analysis to validate (and/or modify) its already established emergency processing priorities. FEC will ensure that all emergency processing priorities are prominently indicated in the resulting disaster recovery plan. The proposed plan will also include a testing plan and maintenance mechanism to ensure that the plan stays current.

Two additional components of this contract are to identify and prioritize those resources needed to develop a COOP and define the requirements needed to establish an alternate processing site.

C. Logical Access, System Software and Change Management Controls

Achieving an adequate level of information protection is highly dependent upon maintaining consistently effective access controls, system software and configuration management controls. Access controls limit and monitor access to computer resources (i.e., data files, application programs, and computer-related facilities and equipment) to the extent necessary to provide reasonable assurance that these resources are protected against waste, loss, unauthorized modification, disclosure, or misappropriation. Access controls include logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. Similarly, system software controls limit and monitor access to powerful programs and sensitive files that control computer processing and secure the application and data supported by the system, while change and configuration controls ensure all programs and program modifications are properly authorized, tested, and approved, and that access to and distribution of programs is carefully controlled. Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted or "turned off" or that processing irregularities or malicious code could be introduced.

Our testing of internal controls identified weaknesses related to the information protection in FEC's information systems environment. These include FEC's midrange computer systems (e.g. servers) and applications. Weaknesses noted include the following:

- The PeopleSoft application is currently running on an Oracle Release 8i Relational Database Management System that is no longer supported by the vendor.
- Audit trail parameters for the Oracle database that supports the PeopleSoft application have not been set to ensure appropriate segregation of incompatible security responsibility and to provide necessary management oversight. Although

'auditing' is activated, the audit and archive logs are written to database tables and operating system logs respectively to which the database administrators (DBAs) have full access. This implies that the DBAs have the capability to purge these logs and remove possible evidence of database activity.

- FEC does not maintain documentation supporting timely approval and testing of patches and software upgrades prior to being moved into production.
- The PeopleSoft application does not have built-in functionality to enforce FEC's password policies. Furthermore, the mitigating controls implemented by FEC do not address the following PeopleSoft weaknesses:
 - PeopleSoft does not have an account lockout policy.
 - PeopleSoft does not prevent users from using previous passwords.
 - PeopleSoft does not have the ability to enforce strong password requirements.
- FEC does not properly monitor access to its networks, systems and physical facility:
 - Six out of 10 separated employees still have active network accounts.
 - Three out of 10 LAN accounts have not logged on for more than 90 days.
 - One out of 10 LAN accounts has not changed its password in 180 days.
 - Two out of 10 LAN accounts have not logged on for more than 90 days and have not changed their passwords in 180 days.
 - Access documentation is not maintained for system administrators and database administrators. Additionally, administrator privileges are not periodically reviewed for appropriateness. FEC's current policy is to grant employees access based on their positions. Only employees hired to perform administrative functions are granted administrative access.

Recommendations:

15. Transfer processing to a service provider or update existing platform to vendor-supported versions/releases.

Management Response:

FEC has evaluated four approved agencies for a Line of Business (LOB) solution and selected the General Services Administration (GSA) as its service provider. FEC has finalized its decision regarding moving its financial, human resources, travel services and procurement activities to GSA's LOB by signing an Interagency Agreement. GSA's LOB solution will replace the FEC PeopleSoft application thus eliminating the discrepancies described in this finding.

16. Write audit trails related to DBA activity to Operating Systems logs and limit DBA's access to these logs.

Management Response:

Although the FEC has a process in place to trace any and all (attempted and successful) transactions which may occur in its Oracle databases, it concurs that implementing additional separation of duty controls will assist in eliminating the possibility that a

database administrator could purge auditing logs to hide inappropriate actions. To this end, the FEC recently implemented a process whereby database administrators have been restricted to read only access to Oracle audit log files.

17. Maintain documentation to support the testing and approval of system software changes.

Management Response:

Although FEC believes its recently issued patch management standard is sufficient, the process of maintaining supporting documentation to support the standard can be improved. In an effort to improve this process, the FEC will issue patch management standard reminders to its technical personnel. In addition, the FEC will add reviewing patch management supporting documentation to its Security Review Policy to ensure that supporting documentation is properly maintained.

18. Develop additional mitigating controls to ensure that PeopleSoft passwords are in agreement with FEC policy or ensure that if PeopleSoft processing is outsourced, the third party maintains password controls that comply with FEC password policies.

Management Response:

Although FEC has developed compensating controls to reduce the risk associated with this finding, it concurs that the PeopleSoft application does not meet the requirements specified in FEC's Password Policy. With this in mind and understanding the limitations of the current version of PeopleSoft utilized at FEC, the Password Policy is being amended to allow an exemption for the PeopleSoft application.

In addition, the FEC selection of GSA's LOB financial solution will replace the FEC PeopleSoft application thus eliminating the discrepancies described in this finding.

19. 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.
20. Utilize access request forms that identify the user's access level to document user access rights to all FEC systems and facilities. Additionally, FEC should periodically review and recertify user access to ensure current access is commensurate with job responsibilities.

Management Response:

Although the FEC has a documented process in place to terminate FEC resources for separated employees, it concurs that this process can be improved. To this end, the FEC recently awarded a contract to develop and implement an automated HR New Personnel Workflow Process.

The New Personnel Workflow Process will include full time employees, interns, and contractors and eliminate the discrepancies described in this finding. The new process will track staff from the start of their employment at FEC to exit and allow managers to request and document any changes in network and application access. This new process will enable a higher degree of coordination between HR and ITD to ensure that user accounts are disabled upon exiting per FEC policy. The new process will retain all historical information regarding account creation, changes to access rights, system resources, and termination information regarding a particular account.

OTHER MATTER

OMB Bulletin No. 07-04 requires that the auditor's report on internal control "identify those material weaknesses disclosed by the audit that were not reported in the reporting entity's Federal Managers' Financial Integrity Act (FMFIA) report." The FEC's schedule of material weaknesses and non-conformances included in the Performance and Accountability Report did not identify the material weakness noted in this report. We do not believe, however, that failure to report the material weaknesses in FMFIA constitutes a separate reportable condition or a material weakness because different criteria are used by management and the auditors in determining material weaknesses.

STATUS OF PRIOR YEAR CONDITIONS

We have reviewed the status of the FEC's corrective actions with respect to the findings and recommendations from the prior year's report on internal controls. We have attached Appendix A to our report that presents the status of prior year findings and recommendations.

FEC's response to the material weakness and significant deficiency identified in our audit is presented within the body of our report. We did not audit the FEC's response and, accordingly, we express no opinion on it.

In addition to the material weakness and significant deficiency described above, we noted certain matters involving internal control and its operation that we reported to the management of the FEC in a separate letter dated November 13, 2007.

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

Clifton Henderson LLP

Calverton, Maryland
November 13, 2007

APPENDIX A
FEDERAL ELECTION COMMISSION
STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS
September 30, 2007

PY Rec. No.	Condition/Audit Area	Recommendation	Current Status ¹
Material Weaknesses			
I. Program Cost Allocation			
1	Cost Allocation Methodology	Revise the account lockout threshold in TRS to five invalid attempts.	Closed
2	Cost Allocation Methodology	Establish written policies and procedures to ensure that employees enter their time in the cost system timely and properly and the results are supported by source data which is reviewed and approved by management	Closed
3	Cost Allocation Methodology	Ensure correct and consistent application of the cost allocation process in accordance with the cost system user manual and conceptual design document.	Closed
4	Cost Allocation Methodology	Ensure errors in TRS causing the system to allocate hours for the Information Division to the wrong program are resolved.	Closed
II. General Property and Equipment			
5	Property, Plant and Equipment	Improve analytical and quality control review of subsidiary schedules, journal vouchers and property reconciliation to ensure material errors and differences are identified and resolved timely.	Closed
6	Property, Plant and Equipment	Use correct USSGL.	Closed
7	Property, Plant and Equipment	Develop a mechanism for reconciling individual property items in the property system to the bulk purchases recorded in the general ledger to ensure completeness of the property system records. Also, ensure that the property management system has complete information, such as bar code identification, serial number and location of the asset.	Closed
8	Property, Plant and Equipment	Clearly document physical inventory procedures, results of the physical inventory, and the reconciliation performed. Maintain the documentation for audit trail and management review purposes.	Updated – reported in current year management letter

¹ Updated recommendation can be considered closed since a new recommendation has been proposed in current year's Auditor's Report on Internal Control or management letter.

APPENDIX A
FEDERAL ELECTION COMMISSION
STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS
September 30, 2007

PY Rec. No.	Condition/Audit Area	Recommendation	Current Status¹
9	Property, Plant and Equipment	Establish a standard process, mechanism or policies to ensure [offices and divisions] notify the Finance Office of the acquisition and disposition of property assets.	Updated – reported in current year management letter.
10	Property, Plant and Equipment	Perform a monthly analysis of property as part of the monthly analysis of financial activities.	Closed
Reportable Conditions			
III. Information Technology			
11	Entity-Wide Security	Complete the documentation approval and implementation of an entity-wide security program plan.	Open – reported in current year significant deficiency
12	Entity-Wide Security	Finalize and implement FEC’s information classification policy and certification and accreditation policy along with any accompanying standards.	Open – reported in current year significant deficiency
13	Entity-Wide Security	Perform risk assessments, as part of FEC’s overall strategy to mitigate risks associated with its IT environment.	Open – reported in current year significant deficiency
14	Entity-Wide Security	Incorporate the results of the risk assessments into FEC’s security plans.	Open – reported in current year significant deficiency
15	Entity-Wide Security	Classify information resources in accordance with the risk assessments.	Open – reported in current year significant deficiency
16	Entity-Wide Security	Utilize corrective action plans for all reviews of security controls whether performed internally or by a third party.	Closed

APPENDIX A
FEDERAL ELECTION COMMISSION
STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS
September 30, 2007

PY Rec. No.	Condition/Audit Area	Recommendation	Current Status¹
17	Entity-Wide Security	Ensure that corrective action plans identify the task to be completed in addition to identifying the resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.	Closed
18	Entity-Wide Security	Certify and accredit all major applications and mission critical general support systems.	Open – reported in current year significant deficiency
19	Contingency Planning	Perform a BIA to formally identify and prioritize all critical data and operations on FEC’s networks and the resources needed to recover them if there is a major interruption or disaster.	Open – reported in current year significant deficiency
20	Contingency Planning	Ensure that emergency processing priorities are established to assist in managing disaster situations more effectively for the network and include business owners in the discussion to determine how much backup data is needed on-hand to minimize the impact of a disaster.	Open – reported in current year significant deficiency
21	Contingency Planning	Establish an alternative processing site for FEC’s operations in the event of a disaster and ensure that an operational mechanism exists to update the disclosure database in the event that FEC’s database is unavailable to replicate the disclosure database resident at the off-site location.	Open – reported in current year significant deficiency
22	Contingency Planning	Develop and document a comprehensive COOP of FEC’s data centers, networks, and telecommunication facilities.	Open – reported in current year significant deficiency
23	Contingency Planning	Develop a COOP to support the continuation of FEC’s core mission in the event of a disaster that renders FEC’s facilities unusable.	Open – reported in current year significant deficiency

APPENDIX A
FEDERAL ELECTION COMMISSION
STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS
September 30, 2007

PY Rec. No.	Condition/Audit Area	Recommendation	Current Status¹
24	Controls to Protect Information	Finalize and implement FEC's process to manually review logs of users using budgetary overrides where the reviewer is an individual who does not have access to utilize the overrides.	Closed
25	Controls to Protect Information	Develop mitigating controls to ensure that PeopleSoft passwords are in agreement with FEC's policy or ensure that when PeopleSoft processing is outsourced, the third-party maintains password controls that comply with FEC's password policies.	Open – reported in current year significant deficiency
26	Controls to Protect Information	Use access request forms that identify the user's access level to document user access rights to all FEC's systems. Additionally, FEC should periodically review the appropriateness of access granted and recertify user access rights.	Closed
27	Controls to Protect Information	Investigate to determine a baseline level of auditing that can be performed without causing a detrimental impact to the performance of the Oracle databases and the applications that they support.	Closed
28	Controls to Protect Information	Periodically review data center access and remove unnecessary access rights.	Closed
29	Software Development and Change Controls	Implement formal policies and procedures for managing system software changes.	Closed
30	Software Development and Change Controls	Maintain documentation to support the testing and approval of system software changes.	Open – reported in current year significant deficiency
31	Software Development and Change Controls	Complete the migration of financial processing to a third-party service provider and verify that the service provider is utilizing vendor supported system software version.	Open – FEC has plans to migrate to a third party service provider in FY 2008.

APPENDIX A
FEDERAL ELECTION COMMISSION
STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS
September 30, 2007

PY Rec. No.	Condition/Audit Area	Recommendation	Current Status ¹
IV. Integrated Financial Management System			
32	Integrated Financial Management System	Evaluate the extent of systems integration needed for existing systems when considering the outsourcing of the FEC's accounting services to a shared service provider.	Updated – reported in current year material weakness
V. Administrative Fines, Civil Penalties and Miscellaneous Receipts			
33	Administrative Fines, Civil Penalties and Miscellaneous Receipts	Implement policies and procedures for reviewing the accounts receivable schedules for reasonableness and accuracy prior to recording related account transactions in the general ledger.	Closed
34	Administrative Fines, Civil Penalties and Miscellaneous Receipts	Formalize policies and procedures for performing accounts receivable reconciliations. While developing these procedures, the FEC should consider establishing a timeline for when the reconciliations should be finalized by the program offices and forwarded to the Finance Office.	Updated – reported in current year material weakness
35	Administrative Fines, Civil Penalties and Miscellaneous Receipts	Document all the methodologies applied in calculating allowances for uncollectible accounts. Periodically review the methodologies against actual procedures performed and revise them as necessary.	Updated – reported in current year management letter
VI. Controls Over Procurement and Disbursement Transactions			
36	Procurement and Disbursement	Issue formal guidance for performing corrective action when negative obligation balances occur. Procedures should describe the conditions when corrective action is needed, corrective actions to perform and the individuals responsible for resolving the error. The timely response and clear communication on corrective action should also be included in the procedures.	Closed
37	Procurement and Disbursement	Ensure documentation related to procurement and disbursement actions are properly approved and supported. Procurement policies and procedures should be enhanced to document, completely and clearly, operating procedures for the procurement cycle and should include procedures for documenting justification when exceptions are made to established procedures.	Updated – Reported in current year management letter

APPENDIX A
FEDERAL ELECTION COMMISSION
STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS
September 30, 2007

PY Rec. No.	Condition/Audit Area	Recommendation	Current Status¹
38	Procurement and Disbursement	Ensure reconciliations are consistently performed, reviewed and approved in a timely manner.	Closed
39	Audit Follow-up	Formalized the remediation process related to audit findings and recommendations that is consistent with OMB Circular A-50 guidelines.	Updated – reported in current year management letter