Federal Election Commission

Office of Inspector General

Final Report

Audit of the Federal Election Commission's Fiscal Year 2015 Financial Statements

November 2015

Assignment No. OIG-15-01

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 2015 Financial Statements

DATE: November 16, 2015

Pursuant to the Chief Financial Officers Act of 1990, 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, 2015. 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. 14-02, *Audit Requirements for Federal Financial Statements*.

Opinion on the Financial Statements

LSC audited the balance sheet of the Federal Election Commission (FEC) as of September 30, 2015, 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, 2014, were also audited by LSC whose report dated November 14, 2014, expressed an unmodified 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, 2015, 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 **deficiency** in internal control 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 and correct, misstatements on a timely basis.
- A **significant deficiency** is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.
- A **material weakness** is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

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 did identify a significant deficiency in internal controls related to Information Technology security.

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. 14-02, *Audit Requirements for Federal Financial Statements*. 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 one instance of noncompliance with The Homeland Security Presidential Directive 23, and National Security Presidential Directive 54, *Cyber Security and Monitoring,* establishing the Comprehensive National Cyber Security Initiative, and relating

to Initiative No. 1, *Manage the Federal Enterprise Network as a Single Enterprise with a Trusted Internet Connection*. Additional details can be found on page 12 of the audit report.

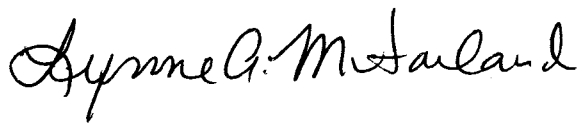
Audit Follow-up

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 some of the findings and recommendations. In accordance with OMB Circular No. A-50, *Audit Follow-up*, revised, the FEC is to prepare a corrective action plan that will set forth the specific action planned to implement the agreed upon 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: Judy Berning, Acting Chief Financial Officer
Alec Palmer, Staff Director/Chief Information Officer
Daniel Petalas, Acting General Counsel

Federal Election Commission

Audit of Financial Statements

As of and for the Years Ended
September 30, 2015 and 2014

Submitted By

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

TABLE OF CONTENTS

Page

LEON SNEAD
& COMPANY, P.C.

Certified Public Accountants
& Management Consultants

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

Independent Auditor's Report

THE COMMISSION, FEDERAL ELECTION COMMISSION
INSPECTOR GENERAL, FEDERAL ELECTION COMMISSION

We have audited the accompanying financial statements of Federal Election Commission (FEC), which comprise the balance sheet as of September 30, 2015 and 2014, and the related statements of net cost, changes in net position, budgetary resources, and custodial activity 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, regulations, and certain provisions of contracts.

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, 2015 and 2014, are presented fairly, in all material respects, in conformity with accounting principles generally accepted in the United States of America.

Our consideration of internal control would not necessarily disclose all deficiencies in internal control over financial reporting that might be material weaknesses under standards issued by the American Institute of Certified Public Accountants. Our testing of internal control identified no material weakness in internal controls over financial reporting. However, we identified a significant deficiency related to the Information Technology (IT) security program established by the FEC that continues to exist.

FEC officials responded to the draft report, and concurred with eight of the eleven recommendations. For the remaining three recommendations, relating to project planning and implementation of recommendations in a contractor's report dealing with an IT security intrusion, we have not reached agreement. In addition, while the FEC concurs with many of the IT findings identified in the audit report, FEC officials do not agree that these issues result in a significant deficiency for financial statement purposes. We disagree with the agency's comments, and have on several occasions provided authoritative guidance to FEC officials that support our professional opinion and illustrates that we have met audit standards in reporting this significant deficiency.

During this fiscal year (FY), the Commission voted to adopt the National Institute of Standards and Technology (NIST), *Risk Management Framework* (RMF), NIST IT security control "best practices," and approved funding to begin to implement this critical internal control process. We believe that the actions the Commission has agreed to take, when fully implemented, will significantly reduce the risks to the agency's information and information systems. In addition, the agency completed corrective actions on several other recommendations from our prior financial statement audit reports.

Our tests of compliance with certain provisions of laws, regulations, and significant provisions of contracts, disclosed one instance of noncompliance that is required to be reported under Government Auditing Standards and the Office of Management and Budget (OMB) audit bulletin. This issue deals with noncompliance with The Homeland Security Presidential Directive 23 and National Security Presidential Directive 54, *Cyber Security and Monitoring*, establishing the Comprehensive National Cybersecurity Initiative, and relating to Initiative No. 1, *Manage the Federal Enterprise Network as a Single Enterprise with a Trusted Internet Connection* (TIC). FEC has taken actions to meet TIC requirements, and we have been advised that the agency should be in full compliance with this security policy in the near future.

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.

REPORT ON THE FINANCIAL STATEMENTS

We have audited the accompanying financial statements of FEC, which comprise the balance sheets as of September 30, 2015 and 2014, and the related statements of net cost, statements of changes in net position, statements of budgetary resources, and custodial activity for the years then ended, and the related notes to the financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America. Such responsibility includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to error or fraud.

Auditor's Responsibility

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; standards applicable to financial statement audits contained in *Government Auditing Standards (GAS)*, issued by the Comptroller General of the United States; and OMB Bulletin 15-02, *Audit Requirements for Federal Financial Statements* (the OMB audit bulletin). Those standards and the OMB audit bulletin require that we plan and perform the audit to

obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's professional judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments in a Federal agency, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing opinions on the effectiveness of the FEC's internal control or its compliance with laws, regulations, and significant provisions of contracts. An audit also includes evaluating the appropriateness of accounting policies used, and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of FEC as of September 30, 2015 and 2014, and the related net cost, changes in net position, budgetary resources, and custodial activity for the years then ended in accordance with accounting principles generally accepted in the United States of America.

OTHER MATTERS

Required Supplementary Information

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

Other Information

Our audit was conducted for the purpose of forming an opinion on the basic financial statements taken as a whole. The performance measures and other accompanying information

are presented for the purposes of additional analysis and are not required parts 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 do not express an opinion or provide any assurance on it.

OTHER AUDITOR REPORTING REQUIREMENTS

Report on Internal Control

In planning and performing our audit of the financial statements of FEC, as of and for the years ended, September 30, 2015 and 2014, 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 audit procedures that are appropriate in the circumstances 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.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies. Therefore, material weaknesses or significant deficiencies may exist that were not identified. However, given these limitations, during our audit, we did not identify any deficiencies in internal control that we consider to be a material weakness. As discussed below, we identified a deficiency in internal control that we consider to be a significant deficiency.

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 deficiency in internal control 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 and correct, misstatements on a timely basis. A material weakness is a deficiency or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Findings and Recommendations

Notable Agency Progress

The Commission voted during July 2015 to adopt NIST's RMF and "best practice" IT security controls, and to provide funding to implement these critical control processes. These actions represent a significant step in eliminating the vulnerabilities identified in our, and the Office of the Inspector General (OIG) audit reports. FEC officials estimated that full implementation would not be completed until approximately one year after a contract is awarded to assist the agency in implementation, or approximately the end of calendar year 2016.

FY 2015 Recommendation Status

As required by GAS, we conducted follow-up testing to determine whether FEC had implemented corrective actions to address the findings and recommendations in the FY 2014 financial statement audit. The following information discusses the findings that still impact the agency's internal control processes.

a. <u>Planning, Oversight and Monitoring of FEC's Corrective Action Plan (CAP)</u>

FEC has made progress in addressing problems reported in prior years' audits. Of the 18 prior year's recommendations, seven have been closed, and our audit tests showed that the agency has corrective actions planned or ongoing on the remaining open recommendations. However, we continue to believe that effective project management is required to effectively and timely implement agreed upon corrective actions. Without appropriate project management and a project plan that includes: key tasks, assignments, timeframes, resource information, and other necessary information; the timely and effective implementation of agency IT projects are delayed, or not effectively implemented.

We worked with FEC officials during our FY 2015 audit, and provided to them guidance related to project planning and management requirements that we obtained from other federal agencies. In addition, we were notified that FEC officials added some information to the CAP relating to tasks and completion dates. However, our audit found that the agency has not issued guidance to address the deficiencies we identified in project planning, and the additional information provided in the CAP does not fully address the audit recommendation.

As noted previously, the Commission plans to obtain contractor assistance to implement NIST's best practice IT security program. The adoption of these best practice requirements will be a complex and long term project that crosses all aspects of FEC's IT operations, as well as other related agency operations. It is critical that a comprehensive project management plan be developed and monitored to ensure that this project is completed in a timely and effective manner.

<u>Recommendations:</u>

1. Develop an Office of Chief Information Officer (OCIO) policy that requires all project managers to develop a detailed project plan for all OCIO projects that require multiple resources and/or has a timeframe of completion beyond 60 days.

   <u>Agency's Response</u>
   FEC summarized the actions it has taken to attempt to address this recommendation, and adds "… We also created a draft project plan guide to provide direction in creating project plans for the OCIO. We held monthly meetings to update statuses of the CAP. The OCIO concurs to develop a project plan in areas that affect every division in the Agency. This will require a centralized Project Management Office (PMO) that would report to an Agency senior level leader and coordinate projects of a certain size and dollar value…."

Auditor's Comments

We have worked with FEC officials during the audit to assist in addressing this audit recommendation, and concur that the agency has taken certain actions. However, we are unable to agree that the proposed action to hire a Project Management Official appropriately addresses the audit recommendation. In our prior audits, we reported that inadequate project planning and management were key reasons for the significant delays in implementing agreed upon corrective actions for IT projects. Although the impact a project has on other FEC divisions is a significant element that should be included in an IT project plan, OCIO should have a project plan for all IT projects meeting the specified criteria in our recommendation, whether OCIO specific or involving other agency divisions. The OIG agrees with this conclusion, and has shown *Information Technology Project Planning and Management*, as a management challenge for FY 2015.

2. Develop an OCIO policy that details the necessary information required for the development of a project plan such as:

    a. identification of key tasks and/or steps;
    b. personnel responsible for completing the task and/or step;
    c. the timeframe for beginning and completing the task and/or step;
    d. any associated cost;
    e. resources required; and
    f. maintain documentation, as part of the project plan, to support the accomplishment of key plan tasks, issues that impacted the project, and the completion of the overall project.

Agency's Response

FEC officials advised that "The OCIO does concur to provide a project outline that covers parent tasks, resources assigned costs and start and end dates for the parent tasks. Documentation will be kept on issues that impacted the timely completion of the project. This will be applied to any project having a capital budget impact over 200K."

Auditor's Comments

We do not believe that project planning should only be done for projects that require capital expenditures. We are uncertain how the agency would determine the costs of projects that may not require the purchase of a capital item since the agency does not have a cost accounting system that could provide project costs (or estimated costs). In addition, some projects because of their critical nature and/or complexity would need a project plan, but may not have a capital budget of over $200,000.

b. Assessment and Accreditation of the General Support System (GSS)

The FEC has not completed a full assessment and accreditation of its GSS, or updated applicable policy documents as we recommended in prior financial statement audit reports. In our FY 2014, we reported that:

"FEC needs to perform an assessment of its general support system to identify vulnerabilities that could allow further network intrusions and data breaches. In addition, FEC has not followed FEC policy 58-2.4, *Certification and Accreditation Policy*, which establishes controls over the process of obtaining independent assurance that FEC major applications and general support system (GSS) are capable of enforcing the security policies that govern their operations."

Recommendations:

3. Promptly perform, after implementation of NIST best practice IT controls, an assessment and accreditation of the GSS. (*Revised)*

   Agency's Response
   FEC officials advised that "The OCIO concurs with this recommendation. The OIG is aware and has acknowledged OCIO's continuous work in this area. The OCIO is currently in the process of acquiring the service of a contractor to have the NIST Management Framework implemented (including SP 800-53r4) in the Agency… and a project plan will be created by the contractor once the contract is awarded."

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

4. Strengthen FEC Policy 58-2.4 so that it provides additional guidance on what decision points determine when a new assessment and accreditation is required; and the specific documentation requirements that need to be maintained in order for the agency to track changes so it can make informed decisions on when major changes drive the need for a new assessment and/or updated accreditation.

   Agency's Response
   FEC officials advised that "The OCIO concurs with this recommendation. All OCIO security policies will be reviewed during the implementation of the NIST Risk Management Framework and modified as needed."

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

c. Recertification of Users' Access Authorities

FEC has not yet established a process that will provide supervisors with the necessary information to recertify user access authorities for their staff. We first reported that FEC needed to develop a process to periodically review users' access authorities in 2009. While FEC officials agreed after our first report that such a control process was needed (and required by its own policies), limited progress has been made to implement this control process. This problem continues even though FEC policies contained in IT policy 58-2.2, *Account Management Policy,* and the general support system's (GSS) security plan

state that all user account access rights and privileges will be periodically reviewed and validated each six months.

Recommendations:

5. Complete the project relating to review of user access authorities, and ensure necessary budgetary and personnel resources are provided to complete this project in a timely manner.

   Agency's Response
   FEC officials advised that "The OCIO concurs with this recommendation. As we have briefed OIG, we are currently evaluating tools that can meet the needs of the Agency. OCIO expects this project to be a multi-year phase approach. The tools we are evaluating are in the range of $200K. Pending approval of the Commission we will acquire and implement the appropriate tools."

   Auditor's Comments
   Since FEC officials have agreed to implement this recommendation and are seeking funding to acquire needed software, we have no additional comments.

6. Reissue FEC Policy 58-2.2 to require annual recertification of users' access authorities by supervisory personnel who would have knowledge of the users' requirements for accessing FEC information and information systems. Ensure that the policy contains sufficient operational details to enable an effective review and update process.

   Agency's Response
   FEC officials advised that "The OCIO concurs with this recommendation. The OCIO has informed OIG that we are currently evaluating tools in order to implement the recommendations as OCIO has reported in the Corrective Action Plan. Once a tool is acquired, OCIO will provide OIG the necessary project outline for this recommendation. Because of dependencies on other module, the attestation module (user-recertification module) will be the last module to be implemented; therefore 4th quarter of FY 2017 is estimated here."

   Auditor's Comments
   Since FEC officials have agreed to implement this recommendation and are seeking funding to acquire needed software, we have no additional comments.

d. Continuity of Operations Plan (COOP)

We noted that FEC conducted a voluntary COOP testing exercise on September 23-24, 2015, to test the feasibility of using Surface tablets and the telework option as a viable method for the continuation of FEC operations in the event of a disruption to normal business. However, the COOP testing was only voluntary for COOP essential personnel, and all key COOP essential personnel had not been provided a Surface tablet at the time of this testing. Therefore, FEC has not yet fully and effectively tested and exercised the Continuity of Operations Plan (COOP) – a critical element in the development of a comprehensive and effective plan. As discussed in Federal Continuity Directive (FCD)

No. 1,[1] until the COOP plan is tested and exercised, any deficiencies in the plan cannot be determined, and the agency remains at risk of not being able to carry out the mission of the agency in the event of a disruption to normal business operations.

While the FEC currently has a draft Continuity of Operations Plan (COOP) a full test must be completed in order to validate the FEC's plan. We were advised by FEC officials that a full report of the voluntary test results is expected to be available in November 2015.

Recommendation:

7. Ensure that sufficient resources are assigned to the task of testing the COOP, a critical IT control process, in order to reduce risk to the FEC, and complete all required tests in a timely manner. Ensure that appropriate documentation is retained as required by FCD No. 1 to support that FEC has met all applicable federal requirements.

   Agency's Response
   FEC officials advised that "The OCIO concurs with this recommendation. A test of the updated COOP was performed September 23-24, 2015….A full report of the test results is available and appropriate modifications will be made to the COOP, and if additional testing is required, a project outline will be provided."

   Auditor's Comments
   Since FEC officials have agreed to implement this recommendation and are assessing the test results, we have no additional comments.

e. USGCB Configuration Requirements

We have reported in prior audits that the FEC needed to adopt the United States Government Configuration Baseline (USGCB). As discussed in OMB guidance, the implementation of these standards is critical to strengthening an agency's overall configuration management control process. Our 2015 tests showed that FEC had initiated corrective actions to implement automated logging of changes, implemented a strengthened configuration review board, and began to implement USGCB configuration security settings within FEC. However, management noted that this project has been delayed, and it is now estimated to be completed during 2017, "because it is impossible to implement (these standards) on old hardware." Until these standards are implemented, critical risks remain and could impact the agency's information and information systems.

[1] Federal Continuity Directive No.1, Federal Executive Branch National Continuity Program, Appendix K, Test, Training and Exercise, require that COOP documents must be validated through tests, training, and exercises (TT&E), and that all agencies must plan, conduct, and document periodic TT&Es to prepare for all-hazards continuity emergencies and disasters, identify deficiencies, and demonstrate the viability of their continuity plans and programs. Deficiencies, actions to correct them, and a timeline for remedy must be documented in an organization's CAP (corrective action plan). FEC Policy No. 58.2.9 provides that plans should not be considered valid until tested for practicality, executability, errors and/or omissions. The initial validation test should consist of a simulation or tactical test. Once validated, plans should be tested annually, or when substantive changes occur to the system, to the system environment, or to the plan itself. Test results should be maintained in a journal format and retained for analysis. Validated change recommendations resulting from testing activities should be incorporated into plans immediately.

Recommendation:

8. Implement USGCB baseline configuration standards for all workstations and require documentation by the CIO to approve and accept the risk of any deviation from these standards.

Agency's Response

FEC officials advised that "The OCIO concurs with this recommendation. For all the new hardware installed thus far we are 100% compliant…Because it is not possible to implement the plan on older hardware, (t)herefore, based on budget availability, the remaining machines will be compliant during FY 2016-2017…."

Auditor's Comments

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

f. Vulnerability Scanning and Timely Remediation of Vulnerabilities to Agency's Network

Vulnerability scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms is one of the most important control processes in an agency's IT security program. Without an effective scanning process, and timely remediation of identified vulnerabilities, the agency's information and information systems will remain at high risk.

Our FY 2015 audit continued to find problems in this area as follows:

- Controls needed strengthening to ensure that vulnerabilities/weaknesses identified through the vulnerability scanning tests are completed within 60 days of identification, or document an analysis and acceptance of risks for longer term remediation.

- Scanning of FEC's networks and devices were completed on a test basis, but later stopped. We were advised by FEC officials that until a decision was made as to whether to adopt NIST best practices IT security controls, scanning the network and devices served no useful purpose. In addition, the USGCB configuration management project needed to be completed prior to scanning network resources, according to FEC officials. However, the project is now scheduled to be completed during 2017, which further delays this control process for approximately two years.

Recommendation:

9. Immediately implement a comprehensive vulnerability scanning and remediation program. Strengthen controls to ensure that vulnerabilities/weaknesses identified through the vulnerability scanning are completed within 60 days of identification, or document an analysis and acceptance of risks for longer term remediation. (*Revised)*

Agency's Response

FEC officials advised that the OCIO concurs with this recommendation, and has awarded a contract to support agency scanning and remediation efforts.

Auditor's Comments

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

g. Mandiant Report Recommendations Remain Open

In May 2012, the FEC was a victim of a network intrusion by an Advanced Persistent Threat (APT).[2] The agency hired a contractor to analyze this serious intrusion on FEC's IT systems, and to provide recommended solutions to eliminating any threat discovered by the contractor. The contractor completed the analysis, and provided a report to FEC on October 5, 2012. The contractor made a significant number of recommendations, including that FEC should complete the actions by the end of October 2012.

However, our FY 2015 audit tests showed that, while the agency had taken action on several of the recommendations, other recommendations have remained open, almost three years after the report was provided to FEC officials.

Recommendation:

10. Complete the implementation of the contractor's open recommendations contained in the October 2012 Threat Assessment Program report, or provide a formal signed document accepting the risk of the remaining outstanding recommendations that FEC will not implement. Provide sufficient budgetary and personnel resources to this project to ensure that actions are properly accomplished. *(Revised)*

Agency's Response

FEC officials advised that the OCIO disagrees with the recommendation, and stated that the OCIO has implemented all the primary recommendations from the Mandiant report. FEC officials add that "The supplemental recommendations will fall under larger projects OCIO is currently working on and/or plans to implement in FY 2016. For example, as part of the USGCB project admin access from client machines will be removed as OCIO refreshes its client machines; OCIO also made a recommendation to eliminate xmail that would address this finding. The Commission instead decided to implement multi-factor authentication for "webmail" as the Agency moves from Lotus Notes to Office 365 early next year."

[2]According to NIST SP 800-39, an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of obtaining information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. The contractor also identified two additional systems that were infected, but were not shown as APT type threats.

Auditor's Comments

Since FEC officials have agreed to implement this recommendation via other planned projects, we will review the agency's detailed plans for resolving the remaining recommendations during the FY 2016 audit. Thus, we have no additional comments.

A summary of the status of prior year recommendations is included as Attachment 1.

REPORT ON COMPLIANCE

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. 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.

In connection with our audit, we noted one instance described below of noncompliance that is required to be reported according to *Government Auditing Standards* and the OMB audit bulletin guidelines. No other matters came to our attention that caused us to believe that FEC failed to comply with applicable laws, regulations, or significant provisions of laws, regulations, and contracts that have a material effect on the financial statements insofar as they relate to accounting matters. Our audit was not directed primarily toward obtaining knowledge of such noncompliance. Accordingly, had we performed additional procedures, other matters may have come to our attention regarding the FEC's noncompliance with applicable laws, regulations, or significant provisions of laws, regulations, and contracts insofar as they relate to accounting matters.

Noncompliance with Comprehensive National Cyber Security Initiative (*Repeat Finding)*

We first reported that the FEC was noncompliant with The Homeland Security Presidential Directive 23, and National Security Presidential Directive 54, *Cyber Security and Monitoring*, in our FY 2012 audit report. Trusted Internet Connection (TIC) was introduced in OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections*, dated November 20, 2007. The initiative was described in the memorandum as an effort to develop "a common [network] solution for the federal government" that would reduce the number of external Internet connections for the entire government. The memorandum stated that "each agency will be required to develop a comprehensive POA&M (Plan of Action and Milestones)" to implement TIC, but it neither defined "agency" nor referred to any legal authority supporting the initiative.

FEC's Office of General Counsel (OGC) analyzed this document and initially determined that the FEC was exempt from implementing TIC. However, at our request, OGC reassessed this determination, and in an August 2012 memorandum to the Staff Director, the OGC stated that

"…we conclude that FEC must comply with all requirements of…TIC." Based upon this OGC opinion, FEC officials agreed in 2012 to implement TIC.

Our 2015 audit tests found that the agency has just contracted with a vendor to implement TIC requirements. FEC officials advised that TIC would be fully implemented in the near future.

Recommendation:

11. Develop a time-phased corrective action plan to address the prompt implementation of Homeland Security Presidential Directive 23, and National Security Presidential Directive 54, Cyber Security and Monitoring.

    Agency's Response
    FEC officials advised that "The OCIO concurs with this recommendation…The contracting officer awarded a contract for the TIC service at the end of September. We are currently in the planning phase with the winning vendor. The estimated completion date is the second quarter of FY 2016…."

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

Restricted Use Relating to Reports on Internal Control and Compliance

The purpose of the communication included in the sections identified as "Report on Internal Control" and "Report on Compliance" is solely to describe the scope of our testing of internal control over financial reporting and compliance, and to describe any material weaknesses, significant deficiencies, or instances of noncompliance we noted as a result of that testing. Our objective was not to provide an opinion on the design or effectiveness of the FEC's internal control over financial reporting or its compliance with laws, regulations, or provisions of contracts. The two sections of the report referred to above are integral parts of an audit performed in accordance with *Government Auditing Standards* in considering the FEC's internal control over financial reporting and compliance. Accordingly, those sections of the report are not suitable for any other purpose.

AGENCY'S RESPONSE

The FEC's November 9, 2015 response to the audit report, which has been summarized in the body of this report, is included in its entirety as Attachment 2. The FEC's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Leon Snead & Company, P.C.

Rockville, Maryland
November 16, 2015

Status of Prior Year Recommendations

Rec. No.	Recommendation	Recommendation Status
1.	Formally adopt as a model for FEC, the NIST IT security controls established in FIPS 199, FIPS 200, SP 800-53, and other applicable guidance that provides best practice IT security control requirements.	Closed
2.	Revise FEC policies and procedures to require a documented, fact-based, risk assessment prior to declining adoption of any government-wide IT security best practice, or IT security requirement. Require the Chief Information Officer (CIO) to approve, and accept the risk of any deviation from government-wide IT security best practices that are applicable to the FEC business operations. Retain documentation of these decisions.	Closed
3.	Complete the implementation of the open contractor's recommendations contained in the October 2012 Threat Assessment Program report. Provide sufficient budgetary and personnel resources to this project to ensure that actions are properly accomplished.	Open
4.	Revise all pertinent FEC policies and procedures to ensure that they address proper prevention and detection controls, and provide a current and authoritative control structure for addressing Advance Persistent Threat (APT), and other types of intrusions.	Closed
5.	Complete the project relating to review of user access authorities, and ensure necessary budgetary and personnel resources are provided to complete this project.	Open
6.	Reissue FEC Policy 58-2.2 to require annual recertification of users' access authorities by supervisory personnel who would have knowledge of the users' requirements for accessing FEC information and information systems. Ensure that the policy contains sufficient operational details to enable an effective review and update process.	Open
7.	Revise FEC policies and operating procedures to require the minimum best practices controls contained in the United States Government Configuration Baseline (USGCB).	Closed
8.	Implement USGCB baseline configuration standards for all workstations and require documentation by the CIO to approve and accept the risk of any deviation.	Open
9.	Undertake a comprehensive review of user accounts that have been granted non-expiring passwords. Require detailed information from account owners on the need for non-expiring accounts, including the development of other alternatives, before reauthorizing the accounts' access. Develop FEC policies and operating procedures to implement this recommendation.	Closed
10.	Whenever possible, require accounts with non-expiring passwords to be changed at least annually. Establish substantially more robust password requirements for accounts granted non-expiring passwords. Develop FEC policies and operating procedures to implement this recommendation.	Closed
11.	Immediately terminate those accounts with non-expiring passwords that have not accessed their accounts within the last 12 months. Develop FEC policies and operating procedures to implement this recommendation to include a data retention policy for historical data.	Closed

12.	Strengthen controls to ensure that vulnerabilities/weaknesses identified through the vulnerability scanning tests are completed within 60 days of identification, or document an analysis and acceptance of risks for longer term remediation.	Open
13.	Perform within this fiscal year a new assessment and accreditation of the GSS using NIST SP 800-53 as the review criteria.	Open
14.	Strengthen FEC Policy 58-2.4 so that it provides additional guidance on what decision points determine when a new assessment and accreditation is required; and the specific documentation requirements that need to be maintained in order for the agency to track changes so it can make informed decisions on when major changes drive the need for a new assessment and/or updated accreditation.	Open
15.	Ensure that sufficient resources are assigned to the task of testing the COOP, a critical IT control process, in order to reduce risk to the FEC, and complete all required tests in a timely manner. Ensure that appropriate documentation is retained as required by FCD No. 1 to support that FEC has met all applicable federal requirements.	Open
16.	Develop a detailed Plan of Action and Milestone (POA&M) to ensure that required COOP testing and exercises are completed as soon as possible.	Open
17.	Issue a FEC policy that requires project managers to prepare project plans that address FEC Directive 50 requirements for projects that are implemented to address audit recommendations. Require that the project plan includes information, such as: identification of key tasks and/or steps; personnel responsible for completing the task and/or step; the timeframe for beginning and completing the task and/or step; resources required; and that documentation be maintained, as part of the project plan, to support the accomplishment of key plan tasks, issues that impacted the project, and the completion of the overall project.	Open
18.	Develop a time-phased corrective action plan to address the prompt implementation of Homeland Security Presidential Directive 23, and National Security Presidential Directive 54, Cyber Security and Monitoring.	Open

Agency Response to Report[3]

While the FEC concurs with many of the IT findings identified in the audit report, we do not agree that these issues result in a significant deficiency for financial statement purposes. All IT findings are solely related to the FEC's general support system (GSS) rather than the financial system of record, which is outsourced. The likelihood of a material misstatement occurring due to the weakness in the FEC GSS environment is extremely low. The current levels of IT controls do not impact the fair presentation of the Agency's financial statements such that it would rise to the level of a significant deficiency in the scope of the financial statement audit.

In FY 2015, the Agency has taken steps to adopt the National Institute of Standards and Technology (NIST), *Risk Management Framework* (RMF), NIST IT security control "best practices," and approved funding to begin to implement this critical internal control process. In addition, the Agency completed corrective actions on several other recommendations from our prior financial statement audit reports. Furthermore, the Agency has taken actions to meet TIC requirements, and should be in full compliance with this security policy in the near future.

1. Develop an Office of Chief Information Officer (OCIO) policy that requires all project managers to develop a detailed project plan for all OCIO projects that require multiple resources and/or has a timeframe of completion beyond 60 days.

   Agency's Response

   In the FY 2014 financial statement audit report, the auditors recommended that FEC issue a policy that requires project managers to prepare project plans that addresses Directive 50 requirements. These additional items consisted of identifying information such as: identification of key tasks and/or steps; personnel responsible for completing the task and/or step; the time frame for beginning and completing the task and/or step; resources required; and that documentation be maintained, as part of the project plan, to support the accomplishment of key plan tasks, issues that impacted the project, and the completion of the overall project.

   Directive 50 requires that for all audit follow up, management officials are responsible for receiving and analyzing audit reports, providing timely responses, and taking corrective action for all audit follow-up. It further outlines the need to develop a written corrective action plan (CAP) to present to the Commission after receiving the audit report, conduct regular meetings with the Inspector General to follow-up on outstanding findings, respond in a timely manner to all audit reports, and produce semi-annual reports that are submitted to Agency head.

   In FY 2015, the OCIO continued its efforts to enhance the CAP to adhere to Directive 50 and the auditor's recommendation. We focused on creating project

[3] The acting Chief Financial Officer provided the agency response via email, and the response is attached in its entirety.

plans for some CAP items. We enhanced the CAP to include updates, key tasks, accomplishments, key personnel and timelines. Additionally, we created a separate document to serve as project plan for specific CAP items. We also created a draft project plan guide to provide direction in creating project plans for the OCIO. We held monthly meetings to update statuses of the CAP.

The OCIO concurs to develop a project plan in areas that affect every division in the Agency. This will require a centralized Project Management Office (PMO) that would report to an Agency senior level leader and coordinate projects of a certain size and dollar value. Because Project Management Book of Knowledge (PMBOK) is a massive bureaucratic framework that may not fit in this small Agency, this change will require the Commission to support staffing a PMO and whether new project methodologies are feasible, such as implemented by the Digital Services Innovation Team at GSA.

2. Develop a OCIO policy that details the necessary information required for the development of a project plan such as:
    a. identification of key tasks and/or steps;
    b. personnel responsible for completing the task and/or step;
    c. the timeframe for beginning and completing the task and/or step;
    d. any associated cost;
    e. resources required; and
    f. maintain documentation, as part of the project plan, to support the accomplishment of key plan tasks, issues that impacted the project, and the completion of the overall project.

Agency's Response

The OCIO does concur to provide a project outline that covers parent tasks, resources assigned costs and start and end dates for the parent tasks. Documentation will be kept on issues that impacted the timely completion of the project. This will be applied to any project having a capital budget impact over 200K.

3. Promptly perform, after implementation of NIST best practice IT controls, an assessment and accreditation of the GSS. (*Revised)*

Agency's Response

The OCIO concurs with this recommendation. The OIG is aware and has acknowledged OCIO's continuous work in this area. The OCIO is currently in the process of acquiring the service of a contractor to have the NIST Management Framework implemented (including SP 800-53r4) in the Agency. The OCIO already provided OIG with a copy of the SOW for their review. As previously stated above, a project plan will be created by the contractor once the contract is awarded.

4. Strengthen FEC Policy 58-2.4 so that it provides additional guidance on what decision points determine when a new assessment and accreditation is required; and the specific documentation requirements that need to be maintained in order for the agency to track changes so it can make informed decisions on when major changes drive the need for a new assessment and/or updated accreditation.

   Agency's Response

   The OCIO concurs with this recommendation. All OCIO security policies will be reviewed during the implementation of the NIST Risk Management Framework and modified as needed.

   The OIG is aware and has acknowledged OCIO's continuous work in this area. The OCIO is currently in the process of acquiring the service of a contractor to have the NIST Management Framework implemented (including SP 800-53r4) in the Agency. The OCIO already provided OIG with a copy of the SOW for their review. As previously stated above, a project plan will be created by the contractor once the contract is awarded.

5. Complete the project relating to review of user access authorities, and ensure necessary budgetary and personnel resources are provided to complete this project in a timely manner.

   Agency's Response

   The OCIO concurs with this recommendation. As we have briefed OIG, we are currently evaluating tools that can meet the needs of the Agency. OCIO expects this project to be a multi-year phase approach. The tools we are evaluating are in the range of $200K. Pending approval of the Commission we will acquire and implement the appropriate tools.

6. Reissue FEC Policy 58-2.2 to require annual recertification of users' access authorities by supervisory personnel who would have knowledge of the users' requirements for accessing FEC information and information systems. Ensure that the policy contains sufficient operational details to enable an effective review and update process.

   Agency's Response

   The OCIO concurs with this recommendation. The OCIO has informed OIG that we are currently evaluating tools in order to implement the recommendations as OCIO has reported in the Corrective Action Plan. Once a tool is acquired, OCIO will provide OIG the necessary project outline for this recommendation. Because of dependencies on other module, the attestation module (user-recertification module) will be the last module to be implemented; therefore 4th quarter of FY 2017 is estimated here.

7. Ensure that sufficient resources are assigned to the task of testing the COOP, a critical IT control process, in order to reduce risk to the FEC, and complete all required tests in a timely manner. Ensure that appropriate documentation is retained as required by FCD No. 1 to support that FEC has met all applicable federal requirements.

   Agency's Response

   The OCIO concurs with this recommendation. A test of the updated COOP was performed September 23-24, 2015. The test simulated a local unavailability of the primary work site, with all designated COOP personnel working from their alternate work site. A full report of the test results is available and appropriate modifications will be made to the COOP, and if additional testing is required, a project outline will be provided.

8. Implement USGCB baseline configuration standards for all workstations and require documentation by the CIO to approve and accept the risk of any deviation from these standards.

   Agency's Response

   The OCIO concurs with this recommendation. For all the new hardware installed thus far we are 100% compliant. Currently, we have 90 compliant machines. Because it is not possible to implement the plan on older hardware, the OCIO implementation plan is linked to the desktop hardware refresh cycle. Therefore, based on budget availability, the remaining machines will be compliant during FY 2016-2017 during new hardware implementation.

   The OCIO has provided OIG with the project plan of what we have accomplished thus far as an example, of which the IG's office has accepted.

9. Immediately implement a comprehensive vulnerability scanning and remediation program. Strengthen controls to ensure that vulnerabilities/weaknesses identified through the vulnerability scanning are completed within 60 days of identification, or document an analysis and acceptance of risks for longer term remediation. (*Revised)*

   Agency's Response

   The OCIO concurs with this recommendation. The procurement officer awarded a contract to support the scanning and remediation efforts. This effort will help with documentation and acceptance of risks for longer term remediation. OIG is aware of the SOW for this service. It is important to note that when the scanning tool was configured we ran our first set of scans in April of this year.

10. Complete the implementation of the contractor's open recommendations contained in the October 2012 Threat Assessment Program report, or provide a

formal signed document accepting the risk of the remaining outstanding recommendations that FEC will not implement. Provide sufficient budgetary and personnel resources to this project to ensure that actions are properly accomplished. *(Revised)*

Agency's Response

The OCIO disagrees with the recommendation for this activity. The OCIO has implemented all the primary recommendations from the Mandiant report. The supplemental recommendations will fall under larger projects OCIO is currently working on and/or plans to implement in FY 2016. For example, as part of the USGCB project admin access from client machines will be removed as OCIO refreshes its client machines; OCIO also made a recommendation to eliminate xmail that would address this finding. The Commission instead decided to implement multi-factor authentication for "webmail" as the Agency moves from Lotus Notes to Office 365 early next year.

11. Develop a time-phased corrective action plan to address the prompt implementation of Homeland Security Presidential Directive 23, and National Security Presidential Directive 54, Cyber Security and Monitoring.

Agency's Response

The OCIO concurs with this recommendation. The OCIO personnel reviewed the MTIPs vendors' proposals on the 17th through the 21st of September. The contracting officer awarded a contract for the TIC service at the end of September. We are currently in the planning phase with the winning vendor. The estimated completion date is the second quarter of FY 2016. A project schedule will be available to the IG in the next 3 weeks.

The FEC concurs with many of the IT findings identified in the audit report. However, none of the findings were related to financial reporting. Therefore, we do not agree that these issues result in a significant deficiency for financial statement purposes. The levels of IT controls do not impact the fair presentation of the Agency's financial statements for it to be considered a significant deficiency in the scope of the financial statement audit.

Federal Election Commission
Office of Inspector General

Fraud Hotline
202-694-1015

or toll free at 1-800-424-9530 (press 0; then dial 1015)
Fax us at 202-501-8134 or e-mail us at oig@fec.gov
Visit or write to us at 999 E Street, N.W., Suite 940, Washington DC 20463

Individuals including FEC and FEC contractor employees are encouraged to alert the OIG to fraud, waste, abuse, and mismanagement of agency programs and operations. Individuals who contact the OIG can remain anonymous. However, persons who report allegations are encouraged to provide their contact information in the event additional questions arise as the OIG evaluates the allegations. Allegations with limited details or merit may be held in abeyance until further specific details are reported or obtained. Pursuant to the Inspector General Act of 1978, as amended, the Inspector General will not disclose the identity of an individual who provides information without the consent of that individual, unless the Inspector General determines that such disclosure is unavoidable during the course of an investigation. To learn more about the OIG, visit our Website at: http://www.fec.gov/fecig/fecig.shtml

Together we can make a difference.