Federal Election Commission

Office of Inspector General

Audit of the Federal Election Commission's Fiscal Year 2016 Financial Statements

November 2016

Assignment No. OIG-16-01

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 2016 Financial Statements

DATE: November 15, 2016

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, 2016. 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. 15-02, *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, 2016, 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, 2015, were also audited by LSC whose report dated November 16, 2015, 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, 2016, 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. 15-02, *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 no instance of noncompliance with laws and regulations that are required to be reported under U.S. generally accepted government auditing standards or OMB guidance.

Audit Follow-up

The independent auditor's report contains recommendations to address deficiencies found by the auditors. Management was provided a draft copy of the audit report for comment and generally concurred with 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 at (202) 694-1015.

Lynne A. McFarland
Inspector General

Attachment

cc: Alec Palmer, Staff Director/Chief Information Officer
Lisa Stevenson, Acting General Counsel
Gilbert A. Ford, Acting Chief Financial Officer

Federal Election Commission

Audit of Financial Statements

As of and for the Years Ended September 30, 2016 and 2015

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, 2016 and 2015, 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, 2016 and 2015, 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. We continue to report a significant deficiency related to FEC's Information Technology (IT) security program. However, FEC has made improvements to the program, and has corrective actions underway to address open audit recommendations.

Our tests of compliance with certain provisions of laws, regulations, and significant provisions of contracts, disclosed no instance of noncompliance that is required to be reported under Government Auditing Standards and the Office of Management and Budget (OMB) audit bulletin.

FEC officials provided their response to the draft report and noted concurrence with all 14 report recommendations. FEC's detailed responses can be found in Attachment 2 of this report.

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, 2016 and 2015, 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 on Financial Statements

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of FEC as of September 30, 2016 and 2015, 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, 2016 and 2015, 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

1. FEC's IT Security Program

The FEC continues to make progress in addressing the vulnerabilities facing their IT security program. We reported in our FY 2015 audit report, the Commission voted during July 2015 to adopt the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF) (best practices) IT security controls, and to provide funding to implement these critical control processes. As we stated in our prior audit report, these actions represent a significant step in eliminating the vulnerabilities identified in our, and the Office of the Inspector General (OIG) audit reports issued since 2009. FEC has contracted with a firm to assist the agency in implementing this project, as well as taking other actions during FY 2016. FEC's current estimate for fully implementing NIST best practices is the end of FY 2017.

As required by GAS, we conducted follow-up testing to determine whether FEC had implemented corrective actions to address the recommendations in prior financial statement audit reports. We found that FEC has made progress in addressing problems reported in prior years' audits. Of the 11 open recommendations from FY 2015, one recommendation has been closed this FY, and FEC has corrective actions planned or ongoing for the remaining open recommendations. The following information discusses the open audit recommendations.

a. Planning, and Oversight of IT Projects

During our FY 2016 audit, we followed up to determine the actions taken by FEC officials to address the need for improved project planning and management. We

reviewed the FY 2016 Financial Statement Audit Corrective Action Plan (CAP) for this recommendation, and found that the plan showed the estimated completion date as "to be determined (TBD)".

We discussed this matter with the Office of the Chief Information Officer (OCIO) officials who provided us with a draft project planning policy document. From our review of this document, it appears that the policy has the potential to address the audit recommendation. However, in order to verify the sufficiency of the policy, the document must be finalized and project plans must be developed.

Recommendations:

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. If OCIO determines a particular project meeting these stated requirements would not require a project plan, OCIO officials should document this decision and reasoning as part of their project planning documentation. *(Revised)*

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: OCIO concurs that project planning is an important element in successful technological implementations. Project planning has evolved significantly over the past 5 years and as a result OCIO will support the new Agile development methodology that is consistent with GSA's new technology engagement model as dictated by the President's technology innovation agenda. The FEC is proactively leveraging the DHS Federal Network Resilience teams to augment the resources required to improve the IT Security Program management. Several of the recommendations require dedicated resources to consistently managing operations on an ongoing basis.

    Auditor's Comments: While the OCIO concurred with recommendations 1 and 2, no information was provided on how the agency planned to implement the recommendations. As a result the recommendations remain open.

b. Assessments and System Authorizations

After completion of the NIST RMF project, FEC needs to ensure its general support system, and other major systems security controls are evaluated to determine the extent to which the controls were implemented correctly; operating as intended; and producing the desired outcome with respect to meeting security requirements detailed in each systems security plan.

As we noted in prior audit reports, FEC has not followed FEC policy 58-2.4, *Certification and Accreditation Policy*, which establishes controls over the process of obtaining assurance that FEC's major applications and general support system are capable of enforcing the security policies that govern their operations.

FEC governance adopted NIST best practices, and obtained a contractor to assist the agency in developing and implementing a risk-based IT security program. The FEC currently estimates the project will be fully implemented in late FY 2017. OCIO officials advised us that after this project is fully implemented, the agency will authorize its updated systems. Assessments would be accomplished, as discussed in OMB policies, as part of an established continuous monitoring program.

Recommendations:

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

   Agency's Response: OCIO concurs with the recommendation and is currently implementing this recommendation and is on schedule for July 2017 and within the approved budget.

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. *(Revised)*

   Agency's Response: OCIO concurs with the recommendation and as the agency implements the NIST Risk Management Framework (RMF), this policy will be reviewed and updated based on the results of the RMF and will include language of when systems need to be reviewed and assessed based on changes and other determining factors.

   Auditor's Comments: Since OCIO concurred with recommendations 3 and 4, we have no additional comments.

c. Recertification of Users' Access Authorities

FEC has not established a process that will provide supervisors with the necessary information to recertify user access authorities periodically. 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.

Per the FEC's CAP, it is currently estimated that this project, in conjunction with the NIST implementation project, would be implemented in late FY 2017.

Recommendations:

5. Implement procedures and processes to complete periodic reviews of user access authorities after the NIST best practices implementation project is completed. *(Revised)*

   Agency's Response: OCIO concurs with the recommendation and will implement capabilities to allow for a review of user access authorities. FEC is participating in the DHS CDM program that will give us access to the tools and sensors, which would allow the agency to implement the recommendation made by the OIG. Phase 2 of the CDM project, will provide the agency with this capability that was awarded in July 2016. The implementation schedule is dictated by DHS as they work with the implementers to roll out the service to agencies in FY17. At the completion of the NIST contract the FEC will be implementing best practices that will improve IT policies and procedures. As part of the improvement, the review of user access authorities will be automated through the user of the DHS CDM tools following the new FEC IT policies and procedures. Subject to workload, staff and additional funding for equipment and licensing not provided by DHS CDM may extend the time required for implementation of the recommendation to several months after the completion the DHS tool deployment.

6. Update 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. *(Revised)*

   Agency's Response: OCIO concurs with the recommendation. All OCIO policies and procedures will be reviewed in the coming year as we implement NIST best practices for Information and Information Systems. FEC Policy 58-2.2 will be reviewed and updated as part of the NIST best practice implementation. The NIST project is on schedule for completion by July 2017 and within approved budget.

Auditor's Comments: Since OCIO concurred with recommendations 5 and 6, we have no additional comments.

d. Continuity of Operations Plan (COOP)

During our follow-up testing to determine whether the FEC had implemented recommendations dealing with testing a fully developed COOP plan, we noted that limited progress has been made on this issue. The CAP shows that the targeted implementation date for this recommendation is the second quarter FY 2017. The CAP notes that completion of the COOP is tied into the implementation of the NIST best practices project, which was recently awarded. The CAP further notes that "A contingency plan for all major and general support systems will be created. In addition, the COOP plan will be reviewed, updated and tested by the contractor."

FEC conducted a voluntary test of the COOP during September 23-24, 2015. The test simulated a local unavailability of the primary work site, with some designated COOP personnel working from their alternate work site. We reviewed the test plan, and related report for the September test. The following table shows what parts of the September test meets the federal testing requirements discussed below.

Federal Continuity Directive No. 1, Appendix K	Auditor's Comments
Annual testing of alert, notification, and activation procedures for continuity personnel and quarterly testing of such procedures for continuity personnel at agency headquarters.	This requirement was partially met.
Annual testing of plans for recovering vital records (both classified and unclassified), critical information systems, services, and data.	This requirement was not met.
Annual testing of primary and backup infrastructure systems and services (e.g., power, water, fuel) at alternate facilities.	This requirement was not met.
Annual testing and exercising of required physical security capabilities at alternate facilities.	This requirement was not met.
Testing and validating equipment to ensure the internal and external interoperability and viability of communications systems, through monthly testing of the continuity communications capabilities outlined in Annex H (e.g., secure and non-secure voice and data communications).	This requirement was partially met.
An annual opportunity for continuity personnel to demonstrate their familiarity with continuity plans and procedures and to demonstrate the agency's capability to continue its essential functions.	This requirement was partially met.
An opportunity to demonstrate that backup data and records required supporting essential functions at alternate facilities or locations are sufficient, complete, and current.	This requirement was not met.

Recommendation:

7. Ensure that sufficient resources are assigned to the task of periodically testing newly created system contingency plans. *(Revised)*

Agency's Response: OCIO concurs and the FEC is currently implementing NIST best practices, which include Business Continuity and Disaster Recovery Plan for each General Support Systems (GSS) and Major Applications (MA). Each system will be tested as part of the NIST guidelines. Going forward, FEC OCIO will improve its documentation of the COOP testing and test results. Through the utilization of two service providers who process and maintain FEC financial activity, the Commission has an effective COOP process for financial management and financial statement preparation and reporting. Both service providers' COOP plans are evaluated annually as part of their respective systems audits. In 2016, the service providers' COOP plans were reviewed and the auditors determined both providers have documented a comprehensive plan and set of procedures to ensure continuity of operations for information systems that support their respective operations should an unexpected interruption occur. The FEC considers the service providers COOP plans and the annual assessment of their plans as important internal controls over FEC financial reporting.

Auditor's Comments: Since OCIO concurred with the recommendation, we have no additional comments.

e. USGCB and Other Configuration Management 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 tests showed that FEC has made progress in implementing USGCB requirements, and in other configuration management controls, such as implementing automated logging of changes, and implementing a strengthened configuration review board. FEC estimates USGCB configuration security settings and other configuration management controls will be fully implemented by the end of FY 2017.

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: OCIO concurs and all agency systems will be in compliance with USGCB standards by February 2017.

Auditor's Comments: Since OCIO concurred with the recommendation, we have no additional comments.

f. Remediation of Vulnerabilities

FEC has made improvements in its scanning program, including remediation of older vulnerabilities identified by these scans. FEC has also contracted with a vendor to

develop a patching plan, and is working to fully implement a patch management program that meets IT security best practices.

However, our testing of a sample of 18 critical and high vulnerabilities identified in a FEC January 2016 scanning report showed that many of these vulnerabilities had not yet been corrected, as of July 2016. OCIO officials advised us that they are working to resolve these vulnerabilities, and many would be addressed in the near future when "a new configuration is rolled out to the users". OCIO officials agreed, however, that more needs to be done before there is a mature process for remediation of scanning vulnerabilities.

Recommendation:

9. Implement a comprehensive vulnerability scanning and remediation program. Strengthen controls to ensure that critical and high vulnerabilities identified through the vulnerability scanning are completed within 60 days of identification, or document an analysis and acceptance of risks for longer term remediation.

   Agency's Response: OCIO concurs and recently implemented a FEC vulnerability management system identifies vulnerabilities across all FEC systems and provides a mechanism to document remediation and acceptance of risk. As part of the Patch Management contract, the contractor is developing a patching process aligned with NIST that will leverage the FEC vulnerability management system for identification and documentation of vulnerabilities. The patch management process is on track to be finalized September 2017. The final process may require additional patch management solutions to improve overall effectiveness and efficiency of patch management to all FEC IT assets.

   Auditor's Comments: Since OCIO concurred with the 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).[1] 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. The contractor completed the analysis, and provided a report to FEC on October 5, 2012, and made recommendations to address the problems identified.

[1]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.

We followed-up, during our FY 2016 financial statement audit, on the seven recommendations that we considered open in the Mandiant report. We obtained information from OCIO officials on the status of FEC's corrective actions on each of the seven recommendations. From our review, we determined that FEC had taken actions to address three of the seven, and had ongoing corrective actions for the remaining four. Three of the four recommendations were related to projects that were estimated to be completed prior to the end of FY 2016. One recommendation related to a contract with DHS to provide assistance concerning the implementation of a continuous diagnostics and monitoring program that will not be implemented until FY 2017.

Recommendations:

10. Complete the implementation of the contractor's open recommendations contained in the October 2012 Threat Assessment Program report:

    a. Secure local administrator passwords by making them unique on every system or disabling the local administrator account from accessing systems over the network.

       Agency's Response: OCIO concurs with Recommendation 10a and administrators now have Privilege (PR) accounts, which are unique to each administrator.

    b. Implement application "white listing" on domain controllers and other critical servers.

       Agency's Response: OCIO concurs with Recommendation 10b and the agency is a member of the DHS CDM program. DHS made an award in July 2016 for security tools and sensors. Application White Listing is one of the capabilities the agency will be able to implement in 2017 with DHS support.

    c. Implement two-factor authentication for the VPN and for webmail.

       Agency's Response: OCIO concurs with Recommendation 10c and the FEC currently has two-factor authentication for VPN. Webmail dual factor will be implemented in April 2017.

    d. Remove "local administrator" level privileges from end-users.

       Agency's Response: OCIO concurs with Recommendation 10d and by April 2017, all local administrator privileges will be removed from user machines.

       Auditor's Comments: Since OCIO concurred with recommendations 10a-10d, we have no additional comments.

2. Security Awareness Training for Contractors

Security awareness training is a key aspect of the government's and FEC's IT security program, and is required by FEC's standards, OMB regulations, and NIST best practices. As part of our IT control testing for the FY 2016 financial statement audit, we attempted to validate that FEC's contractors who had access to the agency's network, had received security awareness training as required. OCIO personnel provided us several incomplete listings of contractors currently working for FEC and having network access, as well as printouts that listed what contractors had received security awareness training. From our review of these documents, we found that a large number of contractor personnel had not received security awareness training. After receiving additional information on several occasions from OCFO officials, we determined that all but four contractors had documentation showing security awareness training had been taken. In addition, we could find no processes or controls that would remove network access for personnel or contractors that did not complete security awareness training. We determined that FEC needs to strengthen its controls and processes in this area so that documentation of on-board contractors is accurate and readily available for physical security purposes, and contractors who access FEC's network receive required security awareness training, or network access be disabled until the training is obtained.

FEC's, Security Training Minimum Standards, provide that "Within one month of arrival, all authorized users of FEC information and information systems should receive instruction on IT Security Basics…All authorized users of FEC information and information systems should receive annual training to reinforce Rules of Behavior and Acceptable Use, receive updates on current threats and vulnerabilities, and changes in Federal legal and regulatory requirements…".

Recommendations:

11. Work with the necessary divisions/offices to establish a process that ensures the agency is able to identify all on board contractors to address this security risk to the agency.

    Agency's Response: OCIO concurs with Recommendation 11. The OCFO is working to inform the Contracting Officers Representatives (CORs) of their duties and responsibilities regarding contractor tracking in FY 17. This is in conjunction with the Office of Human Resources working with the CORs to establish on line Fingerprinting scheduling beginning in FY 17. The two measures taken together represent a process to assist the agency to identify all on board contractors and address the security risk to the agency.

12. Establish controls and process similar to those used for FEC personnel to track contractor security awareness training.

    Agency's Response: OCIO concurs with Recommendation 12 and now has in place the same system for contractors that we have for FEC personnel.

13. Disable network access to contractors and personnel that do not complete security awareness training within a reasonable period after the required completion date.

Agency's Response: OCIO concurs with Recommendation 13 and now has in place the same system for contractors that we have for FEC personnel.

14. Require those contractors who have not received security awareness training during FY 2016 to take required courses within the next 30 days.

    Agency's Response: OCIO concurs with Recommendation 14.

    Auditor's Comments: Since OCIO concurred with recommendations 11-14, 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 no instance 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.

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 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, MD 20850
November 15, 2016

Status of Prior Year Recommendations

Recommendation	Recommendation Status
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
Complete the project relating to review of user access authorities, and ensure necessary budgetary and personnel resources are provided to complete this project.	Open
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
Implement USGCB baseline configuration standards for all workstations and require documentation by the CIO to approve and accept the risk of any deviation.	Open
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
Perform within this fiscal year a new assessment and accreditation of the GSS using NIST SP 800-53 as the review criteria.	Open
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
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
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
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
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.	Closed

Attachment 2

Agency Response to Draft Report

FEDERAL ELECTION COMMISSION

Washington, DC 20463

The FEC concurs with the IT findings and recommendations identified in the audit report, and notes that the auditors recognized the progress made to remediate these conditions. We noted that 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 FEC continues to on the path remediate all findings. The OIG incorporated our detailed responses to each of the findings and recommendations into the body of the audit report. Our responses provide an overview of how we plan to remediate each of the findings.

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. If OCIO determines a particular project meeting these stated requirements would not require a project plan, OCIO officials should document this decision and reasoning as part of their project planning documentation. (Revised)

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 Response to Draft Report

Agency Response:

OCIO concurs that project planning is an important element in successful technological implementations. Project planning has evolved significantly over the past 5 years and as a result OCIO will support the new Agile development methodology that is consistent with GSA's new technology engagement model as dictated by the President's technology innovation agenda. The FEC is proactively leveraging the DHS Federal Network Resilience teams to augment the resources required to improve the IT Security Program management. Several of the recommendations require dedicated resources to consistently managing operations on an ongoing basis.

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

   Agency Response: OCIO concurs with the recommendation and is currently implementing this recommendation and is on schedule for July 2017 and within the approved budget.

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. *(Revised)*

   Agency Response: OCIO concurs with the recommendation and as the agency implements the NIST Risk Management Framework (RMF), this policy will be reviewed and updated based on the results of the RMF and will include language of when systems need to be reviewed and assessed based on changes and other determining factors.

5. Implement procedures and processes to complete periodic reviews of user access authorities after the NIST best practices implementation project is completed. (Revised)

   Agency Response: OCIO concurs with the recommendation and will implement capabilities to allow for a review of user access authorities. FEC is participating in the DHS CDM program that will give us access to the tools and sensors, which would allow the agency to implement the recommendation made by the OIG. Phase 2 of the CDM project, will provide the agency with this capability that was awarded in July 2016. The implementation schedule is dictated by DHS as they work with the implementers to roll out the service to

agencies in FY17. At the completion of the NIST contract the FEC will be implementing best practices that will improve IT policies and procedures. As part of the improvement, the review of user access authorities will be automated through the user of the DHS CDM tools following the new FEC IT policies and procedures. Subject to workload, staff and additional funding for equipment and licensing not provided by DHS CDM may extend the time required for implementation of the recommendation to several months after the completion the DHS tool deployment.

6. Update 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. (Revised)

   Agency Response: OCIO concurs with the recommendation. All OCIO policies and procedures will be reviewed in the coming year as we implement NIST best practices for Information and Information Systems. FEC Policy 58-2.2 will be reviewed and updated as part of the NIST best practice implementation. The NIST project is on schedule for completion by July 2017 and within approved budget. *Also see answer in #5*

7. Ensure that sufficient resources are assigned to the task of periodically testing newly created system contingency plans. (Revised)

Agency Response: OCIO concurs and the FEC is currently implementing NIST best practices, which include Business Continuity and Disaster Recovery Plan for each General Support Systems (GSS) and Major Applications (MA). Each system will be tested as part of the NIST guidelines. Going forward, FEC OCIO will improve its documentation of the COOP testing and test results. As we embrace cloud.gov in 2017 we will greatly enhance COOP capabilities while reducing Operational and Maintenance expenses while improving these continuity capabilities.

Through the utilization of two service providers who process and maintain FEC financial activity, the Commission has an effective COOP process for financial management and financial statement preparation and reporting. Both service providers' COOP plans are evaluated annually as part of their respective systems

audits. In 2016, the service providers' COOP plans were reviewed and the auditors determined both providers have documented a comprehensive plan and set of procedures to ensure continuity of operations for information systems that support their respective operations should an unexpected interruption occur. The FEC considers the service providers COOP plans and the annual assessment of their plans as important internal controls over FEC financial reporting.

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 Response: OCIO concurs and all agency systems will be in compliance with USGCB standards by February 2017.

9. 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.

Agency's Response OCIO concurs and recently implemented a FEC vulnerability management system identifies vulnerabilities across all FEC systems and provides a mechanism to document remediation and acceptance of risk. As part of the Patch Management contract, the contractor is developing a patching process aligned with NIST that will leverage the FEC vulnerability management system for identification and documentation of vulnerabilities. The patch management process is on track to be finalized September 2017. The final process may require additional patch management solutions to improve overall effectiveness and efficiency of patch management to all FEC IT assets.

10. Complete the implementation of the contractor's open recommendations contained in the October 2012 Threat Assessment Program report:

    a. Secure local administrator passwords by making them unique on every system or disabling the local administrator account from accessing systems over the network.

    Agency Response: OCIO concurs with Recommendation 10a and administrators now have Privilege (PR) accounts, which are unique to each administrator.

    b. Implement application "white listing" on domain controllers and other critical servers.

Agency Response to Draft Report

Agency Response: OCIO concurs with Recommendation 10b and the agency is a member of the DHS CDM program. DHS made an award in July 2016 for security tools and sensors. Application White Listing is one of the capabilities the agency will be able to implement in 2017 with DHS support.

c. Implement two-factor authentication for the VPN and for webmail.

Agency Response: OCIO concurs with Recommendation 10c and the FEC currently has two-factor authentication for VPN. Webmail dual factor will be implemented in April 2017.

d. Remove "local administrator" level privileges from end-users.

Agency Response: OCIO concurs with Recommendation 10d and by April 2017, all local administrator privileges will be removed from user machines.

11. Work with the necessary divisions/offices to establish a process that ensures the agency is able to identify all on board contractors to address this security risk to the agency.

Agency Response: OCIO concurs with Recommendation 11. The OCFO is working to inform the Contracting Officers Representatives (CORs) of their duties and responsibilities regarding contractor tracking in FY 17. This is in conjunction with the Office of Human Resources working with the CORs to establish on line Fingerprinting scheduling beginning in FY 17. The two measures taken together represent a process to assist the agency to identify all on board contractors and address the security risk to the agency.

12. Establish controls and process similar to those used for FEC personnel to track contractor security awareness training.

Agency Response: OCIO concurs with Recommendation 12 and now has in place the same system for contractors that we have for FEC personnel.

13. Disable network access to contractors and personnel that do not complete security awareness training within a reasonable period after the required completion date.

Agency Response: OCIO concurs with Recommendation 13 and now has in place the same system for contractors that we have for FEC personnel.

Agency Response to Draft Report

14. Require those contractors who have not received security awareness training during FY 2016 to take required courses within the next 30 days.

Agency Response: OCIO concurs with Recommendation 14.

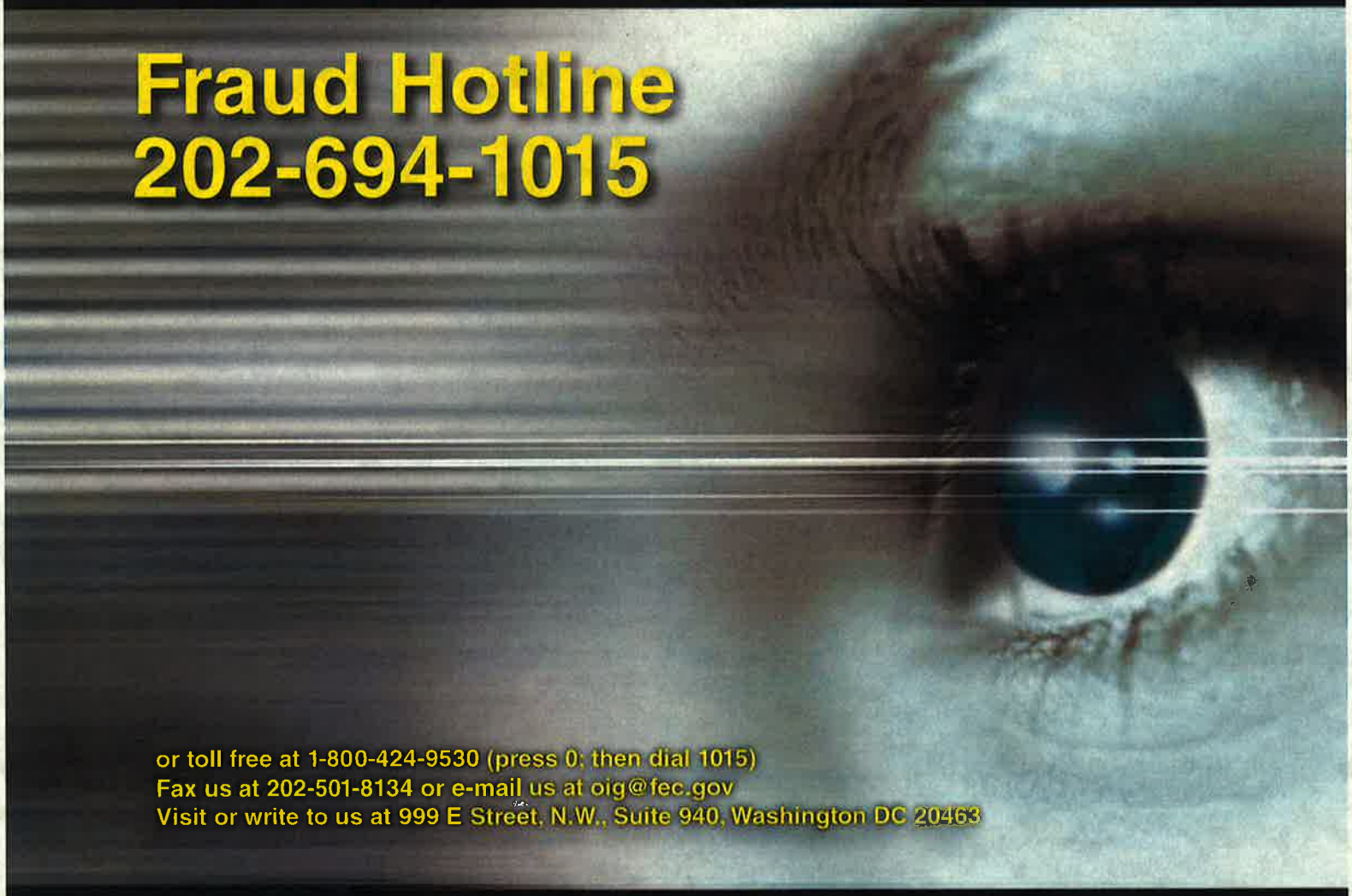
Thank you for the opportunity to be able once again to work with the financial statement audit team, and with the OIG during the audit process. We look forward to working with everyone again for the Fiscal Year 2017 financial statement audit.

Gilbert Ford

Digitally signed by Gilbert Ford
DN: cn=Gilbert Ford, o=OCFO, ou=Budget Division, email=gford@fec.gov, c=US
Date: 2016.11.10 17:11:29 -05'00'

Gilbert Ford,
Acting Chief Financial Officer

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.