Federal Election Commission

Office of Inspector General

Audit of the Federal Election Commission's Fiscal Year 2017 Financial Statements

November 2017

Assignment No. OIG-17-01

FEDERAL ELECTION COMMISSION
WASHINGTON, D.C. 20463
Office of Inspector General

MEMORANDUM

TO: The Commission

FROM: J. Cameron Thurber
Deputy Inspector General

SUBJECT: Audit of the Federal Election Commission's Fiscal Year 2017 Financial Statements

DATE: November 15, 2017

Pursuant to the Chief Financial Officers Act of 1990, as amended, this memorandum transmits the Independent Auditor's Report issued by Leon Snead & Company (LSC), P.C. for the fiscal year ending September 30, 2017. 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. 17-03, *Audit Requirements for Federal Financial Statements*.

In addition, due to the agency's determination that they are legally exempt from the *Federal Information Systems Management Act* (FISMA), the OIG requires auditing of the agency's Information Technology (IT) security against government-wide best practices at a level sufficient to express an opinion on the FEC's financial statements, and report on internal controls and assess compliance with laws and regulations as they relate to the financial operations of the FEC. LSC's report identifies a significant deficiency in internal controls related to IT security and contains recommendations to address the deficiencies noted. Management was provided a draft copy of the audit report for review and comment, and the official management comments to the report can be found in Attachment 2 of the report.

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, 2017, in conformity with accounting principles generally accepted in the United States of America.

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's 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 the OIG on (202) 694-1015.

Attachment

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

Federal Election Commission

Audit of Financial Statements

As of and for the Years Ended September 30, 2017 and 2016

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, 2017 and 2016, 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 significant 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, 2017 and 2016, 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 continues to strengthen its IT security program, and has corrective actions currently in progress to further address identified weaknesses. We also reported a significant deficiency noting that FEC's corrective action plan does not meet Office of Management and Budget's (OMB) requirements. In addition, we identified another control issue that did not rise to the level of a reportable condition which is included in a separate letter, dated November 15, 2017, for management's consideration.

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 OMB audit bulletin.

REPORT ON THE FINANCIAL STATEMENTS

We have audited the accompanying financial statements of FEC, which comprise the balance sheets as of September 30, 2017 and 2016, 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 17-03, 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, 2017 and 2016, 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, 2017 and 2016, 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 deficiencies in internal control that we consider to be significant deficiencies.

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 Needs to Formally Adopt NIST IT Security Best Practices and other Government-wide IT Security Requirements

We reported in our FY 2014 audit report that FEC Officials agreed to formally adopt the National Institute of Standards and Technology's (NIST) best practices IT security controls, and agreed to issue a policy to require a documented, fact-based, risk assessment prior to declining adoption of any government-wide IT security best practice or IT security requirement. Since then, management has made substantial efforts in addressing identified gaps in complying with best practices such as the development of a system security plan for the General Support System (GSS), along with having a signed Authorization to Operate (ATO) document for the GSS. However, our current audit disclosed that a policy has not yet been issued to mandate compliance with best practices, NIST and other government-wide security standards, that will help ensure security over the agency's information and information systems. In addition, there is disagreement from the FEC's Chief Information Officer (CIO) and Office of General Counsel that the Commission had voted[1] to adopt NIST best practices. Therefore, we have reopened prior audit recommendations that address these issues[2].

Recommendation

Adopt NIST IT security best practices and other government-wide information security requirements that are applicable to the agency's business and information systems operations, and document this policy through the issuance of a Commission Directive or a OCIO policy.

[1] The OCIO awarded a contract to SD Solutions LLC to conduct an IT GAP Analysis to obtain a system inventory, GAP analysis, and provide study results concerning the feasibility in cost of implementing NIST Guidelines. SD Solutions provided recommendations to OCIO, in which the Commissioners voted in July 2015 to approve the funding for OCIO to implement these recommendations. The SD Solutions report states that the failure to "adopt an "enterprise Risk Management Framework" (NIST best practices) has an adverse impact on the agency meeting IT security objectives.

[2] Government Auditing Standards require that auditors evaluate whether the audited entity has taken appropriate corrective action to address findings and recommendations from previous engagements that are significant within the context of the audit objectives.

Conduct and document a fact-based risk assessment prior to declining to implement government-wide IT security requirements that are applicable to FEC's business operations.

Management's Response

Management notes that OCIO has formally adopted the Commission-approved NIST 800-37 rev 1 for the FEC's critical systems. Even with the exemption the FEC has in the FISMA arena, leadership decided to adopt the NIST risk management framework (RMF) as a best practice for the FEC's major and critical systems. The Commission's adoption of the RMF, specifically NIST 800-37 rev 1, covered the agency's most critical systems, including the Enterprise General Support System (GSS). As part of the adoption of the RMF, the OCIO continuously monitors the FEC's critical systems to ensure protection of the agency's information and information systems.

The agency has developed and approved policies adopting the NIST IT Security Best Practices and Other Government-wide IT Security Requirements. OCIO has updated the 58A Information Systems Security Program Policy, signed April 4, 2017, and Policy 58-2.4 Assessment and Authorization Policy, signed January 6, 2017, which identify as one of the FEC CIO's responsibilities to "make final authorization determinations" (i.e., full authorization to operate/conditional authorization/denial of authorization). Within the same policy, "Authorization" (to operate) is defined as, "The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations based on the implementation of an agreed-upon set of security controls."

Auditor's Comments

As noted in the finding above, discussed in detail in the Notice of Findings and Recommendations (NFR) provided to FEC management on this issue, and discussed with FEC governance, our audit identified that FEC had not yet issued a policy that requires compliance with NIST best practices, and other government-wide security standards. In addition, FEC had not yet issued a policy to conduct and document a fact-based risk assessment prior to declining to implement government-wide IT security requirements that are applicable to FEC's business operations. In addition, contrary to management's response above, we were advised by the Office of General Counsel that there is disagreement from the FEC that the Commission had voted to adopt NIST best practices in FY 2015, or to fully implement NIST risk management framework. As we have reported over the last nine years, we believe that if FEC adopted such a policy it would significantly strengthen security over the agency's information and information systems by mandating that FEC security policies are aligned with government-wide standards, as appropriate.

We obtained the policies discussed in the FEC response directly from FEC officials, and we determined that neither of the two policies address recommendation number one. Therefore, this recommendation remains open.

2. Agency Corrective Action Plans

FEC's corrective action plan (CAP) for the internal control deficiencies reported in the FY 2016 financial statement audit report does not meet OMB requirements. We attributed this condition to a need for additional oversight and monitoring to ensure the agency meets Commission Directive A-50, and related OMB regulations. Without an adequate CAP, the agency is unable to track the implementation of corrective actions for reported deficiencies, ensure realistic milestones are established, and ensure targeted resolution dates are consistently met to reduce the agency's risk exposure.

OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, dated July 2016, requires each agency's CAP to address the following areas:

- Resources required to correct a control deficiency. The corrective action plan must indicate the types of resources needed (e.g., additional personnel, contract support, training, etc.), including non-financial resources, such as Senior Leadership support for correcting the control deficiency.
- Critical path milestones that affect the overall schedule for implementing the corrective actions needed to resolve the control deficiency. The milestones must lead to a date certain of the correction of the control deficiency.
- Require prompt resolution and internal control testing to validate the correction of the control deficiency.
- Procedures to ensure that accurate records of the status of the identified control deficiency are maintained and updated throughout the entire process.

To determine whether the agency met these and the agency's own requirements, we reviewed the June 2017 CAP. Our review identified the following areas where improvements were needed.

- The plan does not identify the resources required to correct a deficiency, including the types of resources needed to correct the deficiency.
- The plan does not have critical path milestones that affect the overall schedule or the corrective actions needed to resolve the deficiency, including a "date certain" that the deficiency will be corrected.
- Concerning the requirement in OMB Circular A-123 that the agency must promptly resolve and perform internal control testing to validate the correction of the control deficiency, many of the deficiencies contained in this report and in the CAP, have been outstanding for years, and some of the deficiencies have been reported outstanding since FY 2004.

We have reported problems with the agency's CAP and related areas in several prior audit reports, and corrective action has yet to be implemented for several of the recommendations. Corrective action for audit recommendations, to include the timely implementation of audit recommendations, is required by Office of Management and Budget Circular A-50, Audit Follow-up, as revised, Commission Directive 50, and OMB Circular A-

123. OMB Circular A-123, Section V, provides that agency managers are responsible for taking timely and effective action to correct deficiencies; correcting deficiencies is an integral part of management accountability and must be considered a priority by the agency; corrective action plans should be developed for all material weaknesses, and progress against plans should be periodically assessed and reported to agency management. Management should track progress to ensure timely and effective results.

Recommendation

2. Take actions to ensure that the agency's CAP includes all of the requirements of Commission Directive A-50 and OMB Circular A-123.

Agency's Response

Management generally concurred with the OIG's recommendation and has already started an action plan accordingly. In March 2017, management successfully established the Federal Election Commission Senior Management Council (SMC) for oversight of internal control and Enterprise Risk Management (ERM) activities throughout the agency. The SMC meets, at minimum, on a quarterly basis and includes senior agency officials from all divisions of FEC. Part of the mission of the SMC is to ensure that FEC implements and maintains a strong internal control framework. This includes a positive internal control environment featuring top management commitment to the values of promoting the highest ethical standards and organizing all program and administrative processes to promote accuracy, efficiency and compliance with all applicable laws. The Agency anticipates filling the vacant Director of Accounting position in FY 2018 to take the lead on Internal Control and ERM activities throughout the Agency.

Auditor's Comments

We have reviewed the documents provided by FEC relating to the actions it has taken to implement the ERM requirements of OMB Circular A-123 within the agency. Our initial reviews of these documents showed that FEC has revised its monitoring processes, and has begun to implement the circular's requirements relating to ERM.

However, our finding and recommendation relates to requirements for development, implementation and monitoring of specific corrective actions plans for past audit findings and recommendations. As discussed above, we noted that key portions of an effective corrective plan were missing from the document. FEC indicated it generally concurred with the recommendation; however, we need the specific actions the agency plans to take to address the issues noted in this report before we can determine if the actions proposed by the agency will address the findings and recommendations.

3. FEC Continues to Make Progress in Addressing Outstanding Information Technology Control Issues – However Problem Areas Remain

As required by Government Auditing Standards, we reviewed the actions taken and proposed by the FEC to address the recommendations that remained open from FY 2016. During our FY 2017 audit, we were able to close six of the audit recommendations that remained open from prior years' reports. The actions taken by FEC to enable us to close these six recommendations is a further significant step in addressing the vulnerabilities that have been identified in our prior audit reports.

Completion dates for the remaining eight are currently estimated to be implemented in FY 2018. However, as we have reported in prior audits, completion dates have changed repeatedly since the problems were first reported without any significant progress made, in some cases, since FY 2004. The following paragraphs discuss the findings and recommendations that remain open.

a. Review of User Access Authorities *(Open since FY 2004)*

FEC has not yet established a process that will provide supervisors with the necessary information to recertify user access authorities for their staff. 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. Until this control is implemented, FEC officials have reduced assurance that users only have access to information and information systems that are necessary to accomplish their specific job responsibilities.

Best practices (NIST Special Publication (SP) 800-53 and related publications) provide that an organization should review user accounts on a periodic basis. The currently approved FEC Policy 58-2.2 provides that "All user account access rights and privileges will be periodically reviewed and validated in accordance with General Support System...system security plans…."

Recommendations

3. 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

Management believes this recommendation is already completed. A complete review of privilege accounts was completed on June 17, 2017, and was submitted to the OIG. Under NIST SP 800-53 revision 4, Account Management control for moderate baseline, FEC is not required to conduct reviews of all accounts (NIST 800-53: AC-2(13). However, a review of all accounts is conducted during the on-boarding process using the FSA. Additionally, the OCIO completed updating and has implemented a stronger account management policy (58-2.2) which was published on 8/08/2017. The policy mandates that all users account access

rights and privileges be reviewed annually and validated in accordance with the GSS and major applications system security plans by the user's direct manager. The level of approval authority granted for user accounts is based on the need to know and roles of each users. As far as "process," the OCIO has developed an account management procedure which was published on 8/08/2017.

Auditor's Comments

While the FEC did conduct a review this year of users with privilege accounts, it has not yet implemented actions to provide supervisors with the ability to review and recertify access authorities for all FEC user accounts, as agreed in responses to prior years' reports. Further, based on information provided by the OIG and prior year reviews of FSA, this system is not structured to meet this outstanding security requirement and is not a reliable data source. This requirement is part of NIST best practices IT security controls, and required by FEC policies. Until an effective process is developed and implemented by FEC to address this recommendation, the finding and recommendation will remain open. In addition, we disagree with the FEC's comments that the review of user access authorities is no longer required. Our review of NIST policies showed it was moved, and is now part of a related control process.

4. Finalize the draft FEC policies that require annual recertification of users' access authorities. Ensure that the policies address privileged accounts, and require validation to actual system access records, by supervisory personnel who would have knowledge of the users' requirements for accessing FEC information and information systems.

Agency's Response

The OCIO concurred with the finding and recommendation. The CISO has completed the review of this policy and procedures. The updated policy includes specific requirements for initial and continued access to FEC data by demonstrated business need to view, add, change or delete data via supervisory approval.

Auditor's Comments

FEC concurred in the recommendation, and is moving to issue the directive. Therefore, we have no additional comments.

b. **USGCB Requirements Need to be Implemented Agency-wide *(Open since FY 2009)***

In prior audits, we reported that the FEC needed to implement the United States Government Configuration Baseline (USGCB). Our FY 2017 audit found that FEC's computer configuration was not in full compliance with these government-wide configuration standards. Until this project is completed, the agency's systems and information remain at risk. The FEC's CAP showed that the project had been deferred until the agency had completed its procurement of new laptops, estimated as "FY 2018-TBD".

In March 2007, OMB Memorandum M-07-11 announced the "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," directing agencies . . . to adopt the Federal Desktop Core Configuration (FDCC) security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense and the Department of Homeland Security. The USGCB is the security configuration and policy developed for use on Federal computer equipment, and as stated by the CIO Council, 'the USGCB initiative falls within FDCC and comprises the configuration settings component of FDCC.'

It has been over ten years since OMB first issued minimum security requirements for windows operating systems. FEC has established several final implementation dates to meet this requirement, with the last project completion date has not yet been determined. FEC attributed this latest delay in implementation to the need to purchase new computers; however, we disagree that procuring new computers is a valid reason for further delays in this long-delayed implementation of minimum security configuration requirements as all appropriate computer devices in use should be in compliance with federal government configuration standards.

Recommendation

5. Implement USGCB baseline configuration standards for all workstations regardless of the current hardware in use.

Agency's Response

Management agrees with the OIG's recommendation and plans to undertake the necessary steps to implement USGCB for all workstations. IT Operations believes that the FEC must understand IT requirements and implement USGCB in a manner which provides the best configuration for business requirements. As such, IT Operations has pushed USGCB to some workstations and not others. Our intent is to analyze and determine the best approaches in terms of functionality in meeting FEC infrastructure needs. In August 2017, the IT Operations is currently going through another round of USGCB testing before pushing settings FEC-wide.

Auditor's Comments

FEC agreed with the recommendation and plans to implement USGCB for all workstations. However, in order to consider this recommendation closed, a time-phased corrective action plan is needed, and the USGCB requirements need to be fully implemented agency-wide.

c. COOP Planning Not Completed *(Open since FY 2004)*

We reviewed the actions taken by FEC to address findings and recommendations relating to development and testing of the FEC's Continuity of Operations Plan (COOP). The FEC FY 2017 CAP did not show what progress, if any, has been made concerning this issue, and the

document contained no estimated completion date. The prior year's CAP showed that the targeted implementation date for this recommendation was the second quarter FY 2017.

The FEC has operated for 13 years without an approved and tested COOP to ensure that in the event of a disaster, the Commission would have the ability to continue normal business operations within a reasonable timeframe. Without an up-to-date COOP document that has been validated through testing and exercises, any deficiencies in the plan cannot be determined, and the agency remains at high risk with the inability to carry-out the mission of the agency in the event of local disaster.

In addition, the absence of contingency plans for the agency's general support system, and its other major applications pose a separate and material threat to the agency's mission, particularly during election cycles.

FEC provided, at our request, a COOP specific CAP related to the OIG's, *Inspection of the FEC's Disaster Recovery Plan and Continuity of Operations Plans*, released in January 2013. We reviewed this document and noted the following:

- The plan lists ten remaining OIG recommendations from a 2013,
- The original completion dates were from June to December 2013, and
- The current estimated completion date for this important project has been moved repeatedly and is now estimated to be completed by the end of December 2017.

Government-wide best practices, NIST SP 800-34, *Contingency Planning Guides for the Federal Government,* states the following:

> "Information systems are vital elements in most mission/business processes. Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. Contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level."

Recommendations

6. 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.

Agency's Response

Management concurred with the OIG's recommendations and corrective actions had been initiated to address the issues identified. Under the leadership of the Agency's Deputy Chief

Information Officer (DCIO), a number of actions have been taken to evaluate the viability of the COOP program and improve agency-wide adherence to the requirements of the Federal Continuity Directive 1 and NIST SP 800-34. The DCIO plans to distribute the final COOP plan to appropriate individuals. While devising a COOP training plan, per a previous recommendation, we have decided to follow best practice by identifying various roles within the plan for, "appropriate individuals". Our new COOP Training Plan outlines these roles along with their responsibilities. One such role is the "Executive Role" for which best practice suggests that the plan be distributed and limited to individuals that maintain this role. We plan to leverage the telework program for the Disaster Recovery Plan. Each office/division will be responsible for their individual tailored plans to resume services as quickly as possible.

Finally, NIST RMF is guided by NIST Special Publication 800-37 and not NIST SP 800-34. In accordance with the NIST RMF, FEC has selected to follow the NIST RMF at moderate for the FEC GSS, which requires FEC to implement NIST SP 800-53 CP-2 control. This control does not specifically require FEC to conduct simulated training nor automated testing. We are also not required to conduct testing of alternate site, and full recovery test (e.g., controls CP-4(2-4).

Auditor's Comments

FEC has concurred with this recommendation, and provided some information on the actions planned in this area. However, there are statements made above by management regarding required contingency planning guidance that are contradictory. FEC notes that they are adhering to Federal Continuity Directive 1 and NIST SP 800-34 for the agency's COOP program, but concludes in the same response that they are not guided by NIST SP 800-34, and not required to conduct various types of testing and training. We conclude management's response to be flawed since detailed guidance on implementing contingency controls in SP 800-53 are addressed in SP 800-34, and this linkage of the NIST IT security policies exist for all major security control categories. Further, FCD 1 issued January 17, 2017 requires that federal executive agency's "plan and conduct routine internal TT&E [Test, Training and Exercise] events in order to evaluate program readiness and ensure adequacy and viability of continuity plans and communications and IT systems." Without proper testing and training of an agency contingency plan and all its essential functions, there is no way FEC can attest that the developed plan will support the continuance of the agency's mission. We believe this management approach exemplifies the narrow the agency has on IT security control processes, and further supports the recommendation made in finding number 1 above.

In order to consider this recommendation closed, the issues noted in this document and prior audit reports need to be fully implemented.

7. Develop system specific contingency plans, as required by the NIST RMF.

Agency's Response

Management generally concurred with the OIG's recommendation. Although management does not concur that specific contingency plans are always required by the NIST RMF (NIST SP 800-37), it endorses the recommendation in principle, but believes it is inappropriate to require all FEC systems to follow NIST guidelines. NIST SP 800-53 (Control CP-2), "Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations."

As such, the FEC will mature and maintain the Authorization to Operate for systems that management identified as critical (e.g., GSS, E-Filling and Website). The OCIO continues to follow the ITD Disaster Recovery Plan dated 11/08/2010 until updated.

Auditor's Comments

FEC generally concurred with the recommendations. The Commission adopted the use of NIST RMF within FEC, and we are uncertain of what aspects of this recommendation that FEC is not in full agreement with. NIST SP 800-34, Contingency Planning Guide for Federal Information Systems, provides government-wide guidance on a seven-step contingency planning process. We did not cite which systems should or should not have contingency plans. Instead, we recommended that FEC follow the above-cited guidance in developing contingency plans.

d. Improvements Made but Issues Remain in the Remediation of Vulnerabilities *(Open since FY 2004)*

In prior audits, we reported that FEC's vulnerability scanning and remediation program did not meet best practices. Our follow-up testing found that FEC has continued to make improvements in its vulnerability scanning program, including remediation of a number of critical vulnerabilities identified by these scans; however, problems remain. In addition, critical vulnerabilities remain uncorrected and have impacted FEC systems for extended periods.

We found that detailed plans were not developed to correct long-standing critical vulnerabilities that relate to changes needed in applications which prevent FEC from addressing these problem areas. Failure to correct known vulnerabilities is a significant internal control weakness as these vulnerabilities present opportunities for intrusions into FEC's information and information systems. Also, without the proper and complete information documented in the POA&M, management cannot effectively monitor the remediation plans. For example, we noted the following areas, while identified in the POA&M, did not contain any information that would be necessary for management to effectively monitor the corrective actions planned: resources required, overall remediation plan, scheduled completion date, and key milestones with completion dates.

FEC contracted with a vendor to develop a patch management program and is working to fully implement a program that meets IT security best practices. To access the progress made in remediating long-standing problems, we obtained information from FEC personnel on the progress made in remediating critical and high vulnerabilities. The data provided showed that significant progress has been made in vulnerability remediation.

OMB Circular A-130 states that agencies "should assure that each system appropriately uses effective security products and techniques, consistent with standards and guidance from NIST." NIST SP 800-53 addresses vulnerability scanning as one of the recommended security controls and part of the risk assessment process. NIST SP-800-115 states that as part of technical security assessments and to ensure that technical security testing and examinations provide maximum value, NIST recommends that organizations: "Analyze findings, and develop risk mitigation techniques to address weaknesses. To ensure that security assessments provide their ultimate value, organizations should conduct root cause analysis upon completion of an assessment to enable the translation of findings into actionable mitigation techniques. These results may indicate that organizations should address not only technical weaknesses, but weaknesses in organizational processes and procedures as well."

Recommendations

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

Agency's Response

The OCIO agrees with the OIG's recommendation. The OCIO will continue to improve the patch management process by proactively addressing critical and high vulnerabilities. Management has recognized that there is no such thing as perfect security, and that patch management is a continuing process of detecting risks, process improvements and hardening defenses. Reasons for delayed patching can be multifaceted largely because upgrades are often costly, complex, disruptive and in some instances, unachievable, due to application dependencies. We need to accept and understand that enterprises are not in a position to constantly patch and upgrade, and apply security that meets the need of the real world. For this reason, the OCIO has successfully acquired and currently testing Micro-virtualization technology whereby individual web pages, documents and workloads can be performed in isolated containers thus protecting FEC's environment from the absence of critical patches. This tool adds to the FEC's defense in depth security strategy.

Auditor's Comments

FEC agreed to the recommendation. However, it adds a statement that "We need to accept and understand that enterprises are not in a position to constantly patch and upgrade, and apply security that meets the need of the real world." NIST SP 800-40, Guide to Enterprise

Patch Management Technologies, provides that "Patches correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they are mitigating software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation. . . . there are several challenges that complicate patch management. Organizations that do not overcome these challenges will be unable to patch systems effectively and efficiently, leading to compromises that were easily preventable." Unless FEC installs a patch management process that will ensure an ongoing and consistent process to patch and upgrade, and specifically address long outstanding vulnerabilities, it will be in jeopardy of losing what progress it has made through its current emphasis on patch management.

9. Establish Office of Chief Information Officer (OCIO) policies that require the development of POA&Ms to comply with best practices, to include key reporting areas such as: resources required; overall remediation plan; scheduled completion date; and key milestones with completion dates.

Agency's Response

Management agrees with this recommendation. The CISO will review and enhance the existing POA&M tracking management procedures to better track and mitigate critical risks.

Auditor's Comments

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

e. **Project Planning *(Open since FY 2014)***

During our FY 2017 audit, we followed up to determine the actions taken by the FEC officials to address the need for improved project planning and management, and develop policies to guide these areas. We reviewed the current CAP, and noted that the document provides that the "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." The CAP showed implementation in July 2017. To date, FEC is still working to develop appropriate guidance in this area.

Recommendations

10. Develop an Office of Chief Information Officer (OCIO) policy that requires project managers to develop a detailed project plan for all OCIO projects that require multiple resources, extended timeframes and/or have a total cost of $200,000 or more. (Revised)

Agency's Response

Management concurs with the OIG's recommendation that all projects within FEC OCIO with a budget of $200,000 and above shall adhere to the policy being developed in response to Recommendation 11. Smaller projects will be monitored but will not require formal project plans.

Auditor's Comments

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

11. 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. documentation to 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.

Agency's Response

Management concurs with the recommendation. While revisions have been made to the Project Management Plan Policy, there is still some additional language on Agile Methodology that needs to be incorporated. The OCIO is consulting with the General Services Administration (GSA), experts in changing the paradigm of federal IT projects to Agile, to finalize these revisions and publish the policy for use. Once all revisions have been completed, the policy will be routed for review and approval. The OCIO anticipates completing this action by February 1, 2018.

Auditor's Comments

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

We noted another control deficiency over financial reporting that we do not consider a significant deficiency, but still needs to be addressed by management. We have reported this matter to FEC's management, and those charged with governance in a separate letter dated November 15, 2017.

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.

Leon Snead & Company,
P.C. Rockville, MD 20850
November 15, 2017

Status of Prior Years' Audit Recommendations

Rec. No.	Open Recommendations	Status
1.	Develop an Office of Chief Information Officer (OCIO) policy that requires project managers to develop a detailed project plan for all OCIO projects that require multiple resources, extended timeframes and/or have a total cost of $200,000 or more. (Revised)	Open
2.	Develop an OCIO policy that details the necessary information required for the development of a project plan such as: identification of key tasks and/or steps; a. personnel responsible for completing the task and/or step; b. the timeframe for beginning and completing the task and/or step; c. any associated cost; d. resources required; and e. documentation to 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
3.	Promptly perform, after implementation of NIST best practice IT controls, an assessment and accreditation of the GSS.	Closed
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.	Closed
5.	Implement procedures and processes to complete periodic reviews of user access authorities after the NIST best practices implementation project is completed.	Open
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.	Open
7.	Ensure that sufficient resources are assigned to the task of periodically testing newly created system contingency plans.	Open
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.	Open
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.	Open
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. b. Implement application "white listing" on domain controllers and other critical servers. c. Implement two-factor authentication for the VPN and for webmail. d. Remove "local administrator" level privileges from end-users.	Closed
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.	Closed

Attachment 1

Status of Prior Years' Audit Recommendations

Rec. No.	Open Recommendations	Status
12.	Establish controls and process similar to those used for FEC personnel to track contractor security awareness training.	Closed
13.	Disable network access to contractors and personnel that do not complete security awareness training within a reasonable period after the required completion date.	Open
14.	Require those contractors who have not received security awareness training during FY 2016 to take required courses within the next 30 days.	Closed

Agency Response to the Draft Report

FEDERAL ELECTION COMMISSION
Washington, DC 20463

The FEC continues on the path to 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.

Findings and Recommendations

1. Adopt NIST IT security best practices and other government-wide information security requirements that are applicable to the agency's business and information systems operations, and document this policy through the issuance of a Commission Directive or an OCIO policy. Conduct and document a fact-based risk assessment prior to declining to implement government-wide IT security requirements that are applicable to FEC's business operations.

   Management's Response (Updated)

   Management notes that OCIO has formally adopted the Commission-approved NIST 800-37 rev 1 for the FEC's critical systems. Even with the exemption the FEC has in the FISMA arena, leadership decided to adopt the NIST risk management framework (RMF) as a best practice for the FEC's major and critical systems. The Commission's adoption of the RMF, specifically NIST 800-37 rev 1, covered the agency's most critical systems, including the Enterprise General Support System (GSS). As part of the adoption of the RMF, the OCIO continuously monitors the FEC's critical systems to ensure protection of the agency's information and information systems.

   The agency has developed and approved policies adopting the NIST IT Security Best Practices and Other Government-wide IT Security Requirements. OCIO has updated the 58A Information Systems Security Program Policy, signed April 4, 2017, and Policy 58-2.4 Assessment and Authorization Policy, signed January 6, 2017, which identify as one of the FEC CIO's responsibilities to "make final authorization determinations" (i.e., full authorization to operate/conditional authorization/denial of authorization). Within the same policy, "Authorization" (to operate) is defined as, "The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations based on the implementation of an agreed-upon set of security controls."

2. Take actions to ensure that the agency's CAP includes all of the requirements of Commission Directive A-50 and OMB Circular A-123.

   Agency's Response

   Management generally concurred with the OIG's recommendation and has already started an action plan accordingly. In March 2017, management successfully established the Federal Election Commission Senior Management Council (SMC) for oversight of internal control and Enterprise Risk Management (ERM) activities throughout the agency. The SMC meets, at minimum, on a quarterly basis and includes senior agency officials from all divisions of FEC. Part of the mission of the SMC is to ensure that FEC implements and maintains a strong internal control framework. This includes a positive internal control environment featuring top management commitment to the values of promoting the highest ethical standards and organizing all program and administrative processes to promote accuracy, efficiency and compliance with all applicable laws. The Agency anticipates filling the vacant Director of Accounting position in FY 2018 to take the lead on Internal Control and ERM activities throughout the Agency.

3. 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 (Updated)

   Management believes this recommendation is already completed. A complete review of privilege accounts was completed on June 17, 2017 and was submitted to the OIG. Under NIST SP 800-53 revision 4, Account Management control for moderate baseline, FEC is not required to conduct reviews of all accounts (NIST 800-53: AC-2(13). However, a review of all accounts is conducted during the on-boarding process using the FSA. Additionally, the OCIO completed updating and has implemented a stronger account management policy (58-2.2) which was published on 8/08/2017. The policy mandates that all users account access rights and privileges be reviewed annually and validated in accordance with the GSS and major applications system security plans by the user's direct manager. The level of approval authority granted for user accounts is based on the need to know and roles of each users. As far as "process," the OCIO has developed an account management procedure which was published on 8/08/2017.

4. Finalize the draft FEC policies that require annual recertification of users' access authorities. Ensure that the policies address privileged accounts, and require validation to actual system access records, by supervisory personnel who would have knowledge of the users' requirements for accessing FEC information and information systems.

   Agency's Response

   The OCIO concurred with the finding and recommendation. The CISO has completed the review of this policy and procedures. The updated policy includes specific

requirements for initial and continued access to FEC data by demonstrated business need to view, add, change or delete data via supervisory approval.

5. Implement USGCB baseline configuration standards for all workstations regardless of the current hardware in use.

   Agency's Response

   Management agrees with the OIG's recommendation and plans to undertake the necessary steps to implement USGCB for all workstations. IT Operations believes that the FEC must understand IT requirements and implement USGCB in a manner which provides the best configuration for business requirements. As such, IT Operations has pushed USGCB to some workstations and not others. Our intent is to analyze and determine the best approaches in terms of functionality in meeting FEC infrastructure needs. In August 2017, the IT Operations is currently going through another round of USGCB testing before pushing settings FEC-wide.

6. 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.

   Agency's Response (Updated)

   Management concurred with the OIG's recommendations and corrective actions had been initiated to address the issues identified. Under the leadership of the Agency's Deputy Chief Information Officer (DCIO), a number of actions have been taken to evaluate the viability of the COOP program and improve agency-wide adherence to the requirements of the Federal Continuity Directive 1 and NIST SP 800-34. The DCIO plans to distribute the final COOP plan to appropriate individuals. While devising a COOP training plan, per a previous recommendation, we have decided to follow best practice by identifying various roles within the plan for "appropriate individuals". Our new COOP Training Plan outlines these roles along with their responsibilities. One such role is the "Executive Role," for which best practice suggests that the plan be distributed and limited to individuals that maintain this role. We plan to leverage the telework program for the Disaster Recovery Plan. Each office/division will be responsible for their individual tailored plans to resume services as quickly as possible.

   Finally, NIST RMF is guided by NIST Special Publication 800-37 and not NIST SP 800-34. In accordance with the NIST RMF, FEC has selected to follow the NIST RMF at moderate for the FEC GSS, which requires FEC to implement NIST SP 800-53 CP-2 control. This control does not specifically require FEC to conduct simulated training nor automated testing. We are also not required to conduct testing of alternate site, and full recovery test (e.g., controls CP-4(2-4).

7. Develop system specific contingency plans, as required by the NIST RMF.

   Agency's Response (Updated)

Management generally concurred with the OIG's recommendation. Although management does not concur that specific contingency plans are always required by the NIST RMF (NIST SP 800-37), it endorses the recommendation in principle, but believes it is inappropriate to require all FEC systems to follow NIST guidelines. NIST SP 800-53 (Control CP-2), "Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations."

As such, the FEC will mature and maintain the Authorization to Operate for systems that management identified as critical (e.g., GSS, E-Filling and Website). The OCIO continues to follow the ITD Disaster Recovery Plan dated 11/08/2010 until updated.

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

   Agency's Response

   The OCIO agrees with the OIG's recommendation. The OCIO will continue to improve the patch management process by proactively addressing critical and high vulnerabilities. Management has recognized that there is no such thing as perfect security, and that patch management is a continuing process of detecting risks, process improvements and hardening defenses. Reasons for delayed patching can be multifaceted, largely because upgrades are often costly, complex, disruptive and in some instances, unachievable, due to application dependencies. We need to accept and understand that enterprises are not in a position to constantly patch and upgrade, and apply security that meets the need of the real world. For this reason, the OCIO has successfully acquired and currently testing Micro-virtualization technology whereby individual web pages, documents and workloads can be performed in isolated containers thus protecting FEC's environment from the absence of critical patches. This tool adds to the FEC's defense in depth security strategy.

9. Establish Office of Chief Information Officer (OCIO) policies that require the development of POA&Ms to comply with best practices, to include key reporting areas such as: resources required; overall remediation plan; scheduled completion date; and key milestones with completion dates.

   Agency's Response

   Management agrees with this recommendation. The CISO will review and enhance the existing POA&M tracking management procedures to better track and mitigate critical risks.

10. Develop an Office of Chief Information Officer (OCIO) policy that requires project managers to develop a detailed project plan for all OCIO projects that require multiple resources, extended timeframes and/or have a total cost of $200,000 or more. (Revised)

    Agency's Response (Updated)
    Management concurs with the OIG's recommendation that all projects within FEC OCIO with a budget of $200,000 and above shall adhere to the policy being developed in response to Recommendation 11. Smaller projects will be monitored but will not require formal project plans.

11. 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. documentation to 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.

    Agency's Response (Updated)
    Management concurs with the recommendation. While revisions have been made to the Project Management Plan Policy, there is still some additional language on Agile Methodology that needs to be incorporated. The OCIO is consulting with the General Services Administration (GSA), experts in changing the paradigm of federal IT projects to Agile, to finalize these revisions and publish the policy for use. Once all revisions have been completed, the policy will be routed for review and approval. The OCIO anticipates completing this action by February 1, 2018.

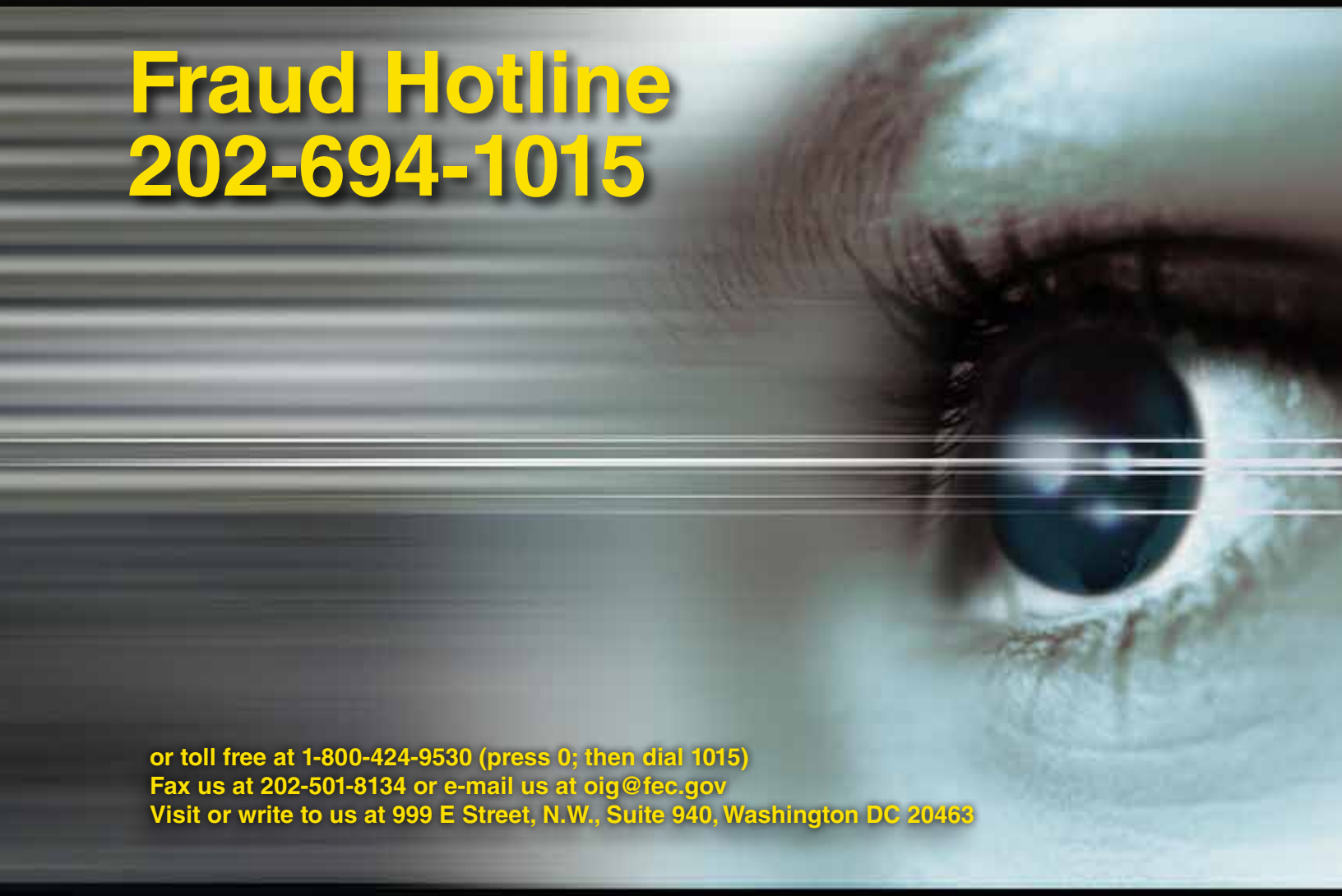
Thank you for the opportunity to once again work with the OIG and the financial statement audit team during the audit process. We look forward to continue our work with the OIG for the Fiscal Year 2018 financial statement audit.

Gilbert Ford

Digitally signed by Gilbert Ford
DN: c=US, o=U.S. Government, ou=FEC, cn=Gilbert Ford
Date: 2017.11.13 13:08:42 -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.