Federal Election Commission

Office of Inspector General

Audit of the Federal Election Commission's Fiscal Year 2018 Financial Statements

November 2018

Assignment No. OIG-18-01

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

MEMORANDUM

TO: The Commission

FROM: Carla A. Smith
Counsel to the Inspector General/Chief Investigator

Carla Smith
Digitally signed by Carla Smith
Date: 2018.11.15 14:26:21 -05'00'

Mia Forgy
Senior Auditor

MIA M. FORGY
Digitally signed by MIA M. FORGY
Date: 2018.11.15 14:19:15 -05'00'

SUBJECT: Audit of the Federal Election Commission's Fiscal Year 2018 Financial Statements

DATE: November 15, 2018

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, 2018. 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. 19-01, *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. In addition to the report, LSC has issued a management letter to FEC related to control issues dealing with reconciling trading partner transactions. As the issue did not rise to the level of a reportable condition to be include in the audit report, LSC believes the issue still requires corrective action from management. Management was provided a draft copy of the audit report and the separate management letter for review and comment, and the official management comments to the

report can be found in Attachment 2 of the report.

In LSC's professional 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, 2018, 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.*

Due to the current vacancies in the Inspector General (IG) and Deputy IG positions, the attached final report is being distributed on behalf of the OIG by the Counsel to the IG and the OIG's Senior Auditor, as the IG's Counsel reviews all final OIG reports prior to distribution, and the OIG's Senior Auditor contractually has primary oversight of the FY 2018 financial statement audit as the OIG's Certified Contracting Officer Representative.

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 at (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, 2018 and 2017

Submitted By

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

TABLE OF CONTENTS

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, 2018 and 2017, 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, 2018 and 2017, 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. FEC has made additional progress in addressing the findings during this fiscal year for several areas relating to its IT security program; while for other findings, we did not identify significant progress had been made. We have also reported a significant deficiency noting that FEC's corrective action plan does not meet Office of Management and Budget's (OMB) requirements.

We also identified one other control issue dealing with reconciling trading partner transactions that did not rise to the level of a reportable condition. We provide this issue to management in a separate letter dated November 15, 2018.

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, 2018 and 2017, 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 19-01, 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, 2018 and 2017, 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 of America 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), which 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, 2018 and 2017, 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 (Repeat Finding)

In our FY 2017 financial statement audit, we reported that we had re-opened[1] a prior audit finding and recommendation that dealt with the need for the Commission to: (1) formally adopt the National Institute of Standards and Technology's (NIST) best practice IT security controls and all other applicable government-wide IT security requirements, and (2) 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. The recommendations were closed based on the response from management that the Commission had voted to implement the recommendations, an official management response to our audit report agreeing to implement the recommendation, and management subsequently hiring contracting services to assist with implementation.

We followed-up with Office of the Chief Information Officer (OICO) and the Office of General Counsel (OGC) personnel during our FY 2017 audit to determine the status of this finding and recommendation. In response to an OIG request for further clarification on this matter, the Acting General Counsel in a memorandum dated, September 15, 2017, advised that the Agency could voluntarily adopt NIST 800-37 as a whole or other FISMA requirements, "…but that we do not believe the Commission has done that to date."

We met with OGC and OCIO officials during our FY 2018 audit to follow up on this prior year open recommendation and we were advised that the Commission would need to issue a policy to implement the open audit recommendation. The prior Chief Information Security Officer along with OGC staff agreed to draft a policy for review and approval by the Chief Information Officer to address the audit recommendation. As part of our standard audit requirements, we requested meetings with Governance and discussed this matter with the Vice-Chair who advised us that it was her understanding that the Commission had voted to adopt NIST best practices and she was not clear on where the breakdown in this agreement

[1] 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.

occurred. To date, no additional information has been provided by FEC, and the finding and recommendation remains open.

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 OCIO policy.
2. 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

The OCIO agrees with the recommendation in principle and will seek comment from the Commission on accepting any residual risk for the FEC which has recently and successfully adopted NIST as best practice and implemented NIST specific IT security controls into applicable systems. Over the years, the OCIO spent considerable effort implementing and executing the NIST Risk Management Framework (RMF) and applying them into FEC's critical systems. The OCIO does not believe a separate policy should be created to specifically "adopt NIST security best practices and other government-wide information security requirements" because these are indefinable requirements. The OCIO uses the following agency-wide policies to demonstrate use of NIST IT security best practices and other government-wide information security requirements: FEC Information System Security Program Policy 58A (updated April, 2017); Delegation of authority appointment of Authorizing Officials in accordance with NIST RMF (signed Feb, 2017); CISO appointment order in accordance with FISMA (signed Dec 12, 2016); and Risk Management Framework (NIST RMF) Standard Operating Procedure (signed and published March, 2017). Additionally, the OCIO has partnered with the FEC's Contracting Officer and has established a standard FEC-wide procurement and contracting process to ensure IT acquisition adheres to the policies stated above.

Auditor's Comments

While the response notes it "agrees with the recommendation in principle", it goes on to state that "the OCIO does not believe a separate policy should be created to specifically adopt NIST security best practices and other government-wide information security requirements because these are indefinable requirements."

During our audit, OGC advised us that it had determined that it was unclear that the Commission had, in fact, approved implementation of NIST best practices, and that a Commission directive would probably be needed to implement the recommendation.

As previously stated, without a policy based process to continue to strengthen weaknesses in FEC's IT security program, progress made to date can be stopped or regress to the point where implementation of IT security controls are not a priority if

changes occur in key personnel. With the recent separation of the FEC's CISO[2], who was instrumental to the CIO in the recent significant progress made to IT security, we are concerned that progress in remediating outstanding issues will become static if a formal policy is not approved that clearly states the Commission will adhere to applicable NIST security standards and all other required government-wide IT security requirements.

In addition, we are uncertain of the OCIO's position that the NIST security best practices, and other government-wide information security requirements are an "indefinable requirements". NIST has been established as the standard setting entity for all IT security requirements[3].

We continue to believe that the Commission should formally adopt NIST best practices and all other government-wide security requirements by developing a policy that mandates adherence to all standards and requirements applicable to FEC business processes, otherwise compliance with applicable security requirements will continue to be "person based" and not policy based. Such a process does not ensure the agency is consistently following the security standards set for the federal government. When changes in key personnel occur, the upward trend in addressing long standing IT security weaknesses are negatively impacted.

2. Agency Corrective Action Plans Are Not Compliant With Government Requirements

FEC's corrective action plan (CAP) for the internal control deficiencies reported in prior financial statement audit reports does not meet the Office of Management and Budget (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 that realistic milestones are established, and ensure that 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.

[2] The FEC's CISO separated from the agency in September 2018.

[3] NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems except for national security systems. The FISMA publications are consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

- 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 federal standards and their own internal requirements, we reviewed the June 2018 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 and Commission Directive 50, 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 appropriate corrective action has yet to be implemented. 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

3. 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

The OCIO continues to work towards identifying a process to evaluate government-wide IT security best practices and mandates that aligns with the OGC's established policy review processes. Partnering with OGC will enable the OCIO to track and assess government issued information security policies, mandates, and directives for their applicability to FEC systems.

Auditor's Comments

OCIO indicated that it is continuing to work on a process to review government-wide IT security requirements; however, this response does not address the recommendation in totality. As OGC may be involved in the legality portion of the assessment, they are not

responsible, nor have the expertise in information security to formally conduct a fact-based risk assessment for implementing security controls, assessing proper risk appetite, or proposing alternative security controls/approaches to addressing new security requirements.

3. Security Weaknesses in Information Technology Controls

FEC has made further progress in addressing long outstanding security control weaknesses; however, there are still areas requiring improvement and more emphasis on remediation from management. As required by Government Auditing Standards, we reviewed the actions taken and proposed by the FEC to address the recommendations that remained open from prior audits. During our current audit, we were able to close three of the audit recommendations that remained open from prior years' reports. Completion dates for the remaining open recommendations continue to be extended, even though the issues have been reported for several years and, 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. We found no corrective actions taken on this problem area during FY 2018.

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…."

Recommendation

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

Agency's Response

The OCIO agrees with the recommendation but notes that this finding has no impact on the actual security of FEC systems. In 2017, the OCIO implemented strict account management procedures that included detailed steps for users to gain and maintain access to FEC systems. However, the OCIO is in the process of researching effective ways and if an effective procedure is found for a reasonable cost it will be implemented enabling supervisors to review user access authorities annually.

Auditor's Comments

The OCIO agrees with the recommendation but added that the finding had no impact to the actual security of the FEC systems. We disagree with the FEC's comment that this issue would have no actual impact to security, as securing agency information to only those who are properly authorized is a critical function of an agency's security program. This control would identify users who have moved positions within FEC or have separated from the agency and continue to have unauthorized access to FEC information. Such a condition would have a significant impact on IT security processes.

We have reported this IT security weakness to FEC since 2009. As noted in each audit report, FEC policies, as well as NIST IT security best practices provide for an annual review of actual user access.

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

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 United States Government Configuration Baseline (USGCB)[4] 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.'

In prior audits, we reported that the FEC needed to implement the USGCB. During our FY 2018 audit, we were advised that the FEC had completed its implementation of this government-wide requirement. However, when we reviewed FEC IT security scanning reports, we identified a significant number of desktops that were not, in fact, compliant with all applicable USGCB security requirements. We discussed this issue with OCIO officials who agreed that additional actions were needed in this area.

It has been over ten years since OMB first issued minimum security requirements for windows operating systems. Until this project is completed, the agency's systems and information remain at risk.

Recommendation

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

[4] The United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. The USGCB is a Federal Government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security

Agency's Response

Management concurs with the OIG regarding the implementation of the USGCB. In 2017, the OCIO has pushed USGCB configuration settings on all Windows 7 laptops. However, recent scans indicated that USGCB is not consistently applied within the FEC environment. The OCIO will accelerate the review and testing of USGCB to analyze and determine the best approaches regarding functionality in meeting the FEC's infrastructure needs. Required USGCB settings will be applied to all workstations FEC-wide as soon as it is ready. The estimated completion date for USGCB implementation is 4th quarter FY19.

Auditor's Comments

OCIO concurs with the finding and recommendation, and provides a completion date of fourth quarter FY 2019, and we have no additional comments.

c. FEC Has Not Fully Implemented and Tested Their Agency Continuity of Operations Plan or Contingency Plans for IT Systems (*Open since FY 2004*)

We reviewed the actions taken by FEC to address findings and recommendations relating to the development and testing of the FEC's Continuity of Operations Plan (COOP). Our review of FEC's FY 2018 CAP, and discussions with OCIO officials showed that the agency is still working to complete the COOP. The current estimated completion date for this long-delayed project is now the end of calendar year 2018.

The FEC has operated for 14 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 seven remaining OIG recommendations from 2013,
- The original completion dates were from June to December 2013, and
- The current estimated completion date for this important project has been extended repeatedly and is now estimated to be completed by the end of December 2018.

Based on the level of effort, time and resources required to complete this significant agency requirement, we note that the December 2018 due date provided from management is not reasonable, which will require another date extension.

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

   Estimated completion for a table top exercise is March 2019. Management acknowledges the COOP requires updating and resources are being sought to assist in this process. Information gathered from the table top exercise will also be used to update the COOP. Estimated completion for updating is third quarter FY19.

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

   Agency's Response

   Management concurs use of NIST SP 800-34 for each system identified as a critical system. FEC will establish information system contingency plans for systems under the General Support System (GSS) boundary: Law Manager Pro, Comprizon Suite, Disclosure, Data Entry, Informatica, Kofax, ECM suite, and Presidential Matching Fund system.

   Management is currently conducting research and has been provided ISCP templates to assist in the process and working in coordination with each application owner to create each plan. Estimate completion for analysis is six months (May 2019).

   Auditor's Comments

   Management concurred with the recommendations and advised that it would have these actions completed by May 2019. We have no additional comments.

d. Further Improvements Needed in the Remediation of Vulnerabilities *(Open since FY 2004)*

In prior audits, we reported FEC's vulnerability scanning and remediation program did not meet best practices and was a significant internal control deficiency. In FY 2017, we

reported that FEC had made improvements in its scanning program, including remediation of the vulnerabilities identified by these scans, and monitoring related corrective actions.

During our FY 2018 audit, we followed up on the actions taken by FEC to determine whether the agency had fully remediated this problem area. We identified that FEC had made additional significant progress, corrected a number of long outstanding critical vulnerabilities, making further progress on others, and had established a monitoring system that met weekly to discuss progress and issues impacting the vulnerabilities. However, our review concluded that FEC had not yet established a process to allow the agency to address these areas at a "managed and measured" level – the level OMB has determined is needed to assure that an agency is meeting IT security requirements.

Our audit also determined that while tracking of identified vulnerabilities has progressed and overall are reported on POA&Ms, key required elements of effective monitoring efforts had not yet been fully addressed. The POA&Ms for several longstanding critical areas did not have key tasks identified, anticipated completion dates and other required elements of a POA&M. The prior CISO stressed the need for improvement in this area and had established a weekly meeting of all key personnel to address the issues noted in the scans and POA&Ms. We believe that this is a critical process and if continued, will enable FEC to more effectively identify needed tasks to remediate the issues, and track progress being made.

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. *(Revised)*

Agency's Response

OCIO agrees with the OIG's assessment of a need to strengthen controls around the remediation program. We remain committed to following the most effective way to mitigate software flaw vulnerabilities and effective solutions to patch management. The OCIO followed recommendations from the Department of Homeland Security (DHS) Federal Incident Response Evaluation (FIRE) program and the NIST Special Publication

800-40 Rev 3 in strengthening its patch management program. Since a number of these actions did not appear in the OIG's report, several of the more significant actions, are listed here as supplemental information.

Over the past two years, the OCIO has executed some sweeping changes to its patch management program and practices that provided more transparency and clarity to OCIO administrators responsible for the timing, prioritization, and testing of patches. In March 2018, the OCIO formalized a System Security Plan (SSP) that directed developers to mitigate high-risk vulnerabilities within thirty days (30) and moderate-risk vulnerabilities within ninety days (90). Any request for extensions must be approved of in writing by an Authorizing Official (AO). Currently, both the Deputy CIO for Enterprise Architecture and the Deputy CIO for Operations are formally appointed by the CIO as AOs for FEC's systems. Additionally, in 2018, the OCIO formed a Security and Operations (SECOPS) team to track and discuss the status of outstanding vulnerabilities and remediation plans on a weekly basis. In all cases, all vulnerabilities are documented in an FEC owned GitHub repository and POAM. All vulnerability remediation plans of actions and milestones are tracked on a weekly basis by the FEC's Information System Security Officer (ISSO). The OCIO will continue to strengthen oversight and execution control of changes already implemented above.

Auditor's Comments

As the OCIO agrees with the audit recommendations, we have no further comments.

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

OCIO agrees with the OIG's assessment and aims to implement corrective actions. The CISO is in the process of finalizing the policies and procedures to address and strengthen the vulnerability management. Estimated completion of a POA&M policy is May 2019.

Auditor's Comments

The OCIO agrees with the audit recommendations. However, we do not believe that a completion date of May 2019 is appropriate to develop a POA&M policy for these critical areas. We believe this action should be better prioritized to have this recommendation implemented immediately.

We noted another control issue that did not rise to a level of a reportable condition, and reported this in a management letter dated November 15, 2018.

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.
November 15, 2018

Status of Prior Years' Audit Recommendations

Rec	Open Recommendations	Status
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. 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.	Open[5]
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.	Open
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.	Open
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.	Open
5.	Implement USGCB baseline configuration standards for all workstations regardless of the current hardware in use.	Open
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.	Open
7.	Develop system specific contingency plans, as required by the NIST RMF.	Open
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.	Open
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.	Closed
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.	Closed
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.	Closed

[5] The FY 2018 report separates the Commission policy and the fact-based risk assessment into two separate open recommendations.

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

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 OCIO policy.
2. 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.

Agency's Response

The OCIO agrees with the recommendation in principle and will seek comment from the Commission on accepting any residual risk for the FEC, which has recently and successfully adopted NIST as a best practice and implemented NIST specific IT security controls into applicable systems. Since 2015, the OCIO has spent considerable effort implementing and executing the NIST Risk Management Framework (RMF) and applying them to the FEC's most critical systems. The OCIO does not believe a separate policy should be created to specifically "adopt NIST security best practices and other government-wide information security requirements" because these are indefinable requirements. The OCIO uses the following agency-wide policies to demonstrate use of NIST IT security best practices and other government-wide information security requirements: FEC Information System Security Program Policy 58A (updated April 2017); Delegation of authority appointment of Authorizing Officials in accordance with NIST RMF (signed February 2017); CISO appointment order in accordance with FISMA (signed December 12, 2016); and Risk Management Framework (NIST RMF) Standard Operating Procedure (signed and published March 2017). Additionally, the OCIO has partnered with the FEC's Contracting Officer and has established a standard FEC-wide procurement and contracting process to ensure IT acquisitions adhere to the policies stated above.

3. 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

The OCIO continues to work towards identifying a process to evaluate government-wide IT security best practices and mandates that aligns with the OGC's established policy review processes. Partnering with OGC will enable the OCIO to track and assess government issued information security policies, mandates, and directives for their applicability to FEC systems.

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

Agency's Response

The OCIO agrees with the recommendation, but notes that this finding has no impact on the actual security of FEC systems. In 2017, the OCIO implemented strict account management procedures that included detailed steps for users to gain and maintain access to FEC systems. However, the OCIO is in the process of researching effective ways to periodically review and recertify user access; and if an effective procedure is found for a reasonable cost, it will be implemented enabling supervisors to review user access authorities annually.

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

Agency's Response

Management concurs with the OIG regarding the implementation of the USGCB. In 2017, the OCIO pushed USGCB configuration settings on all Windows 7 laptops. However, recent scans indicated that USGCB is not consistently applied within the FEC environment. The OCIO will accelerate the review and testing of USGCB to analyze and determine the best approaches regarding functionality in meeting the FEC's infrastructure needs. Required USGCB settings will be applied to all workstations FEC-wide as soon as it is ready. The estimated completion date for USGCB implementation is fourth quarter FY19.

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

The estimated completion date for a table top exercise is March 2019. Management acknowledges the COOP requires updating and resources are being sought to assist in this process. Information gathered from the table top exercise will also be used to update the COOP. The estimated completion date for updating the COOP is third quarter FY19.

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

Agency's Response

Management concurs use of NIST SP 800-34 for each system identified as a critical system. FEC will establish information system contingency plans for systems under the General Support System (GSS) boundary: Law Manager Pro, Comprizon Suite,

Disclosure, Data Entry, Informatica, Kofax, ECM suite, and Presidential Matching Fund system.

Management is currently conducting research and has been provided ISCP templates to assist in the process and working in coordination with each application owner to create each plan. The estimated completion date for the analysis is May 2019.

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. *(Revised)*

Agency's Response

OCIO agrees with the OIG's assessment of a need to strengthen controls around the remediation program. We remain committed to following the most effective way to mitigate software flaw vulnerabilities and effective solutions to patch management. The OCIO followed recommendations from the Department of Homeland Security (DHS) Federal Incident Response Evaluation (FIRE) program and the NIST Special Publication 800-40 Rev 3 in strengthening its patch management program. Since a number of these actions did not appear in the OIG's report, several of the more significant actions, are listed here as supplemental information.

Over the past two years, the OCIO has executed some sweeping changes to its patch management program and practices that provided more transparency and clarity to OCIO administrators responsible for the timing, prioritization, and testing of patches. In March 2018, the OCIO formalized a System Security Plan (SSP) that directed developers to mitigate high-risk vulnerabilities within thirty days (30) and moderate-risk vulnerabilities within ninety days (90). Any request for extensions must be approved of in writing by an Authorizing Official (AO). Currently, both the Deputy CIO for Enterprise Architecture and the Deputy CIO for Operations are formally appointed by the CIO as AOs for FEC's systems. Additionally, in 2018, the OCIO formed a Security and Operations (SECOPS) team to track and discuss the status of outstanding vulnerabilities and remediation plans on a weekly basis. In all cases, all vulnerabilities are documented in an FEC owned GitHub repository and POAM. All vulnerability remediation plans of actions and milestones are tracked on a weekly basis by the FEC's Information System Security Officer (ISSO). The OCIO will continue to strengthen oversight and execution control of changes already implemented above.

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

OCIO agrees with the OIG's assessment and aims to implement corrective actions. The Acting CISO is in the process of finalizing the policies and procedures to address and strengthen the vulnerability management. The estimated completion date of a POA&M policy is May 2019.

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 2019 financial statement audit.

Gilbert Ford

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 1050 First Street, N.E., Suite 1010, 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.