

OFFICE OF INSPECTOR GENERAL



*Audit of the Federal Election Commission's  
FY 19 Financial Statement Audit Report  
Assignment No. OIG-19-01*

Prepared by: **Brown and Company**

**November 2019**


Federal Election Commission - Office of Inspector General  
1050 First Street, N.E., Suite 1010, Washington, D.C. 20463



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

**TRANSMITTAL MEMORANDUM**

**TO:** The Commission

**FROM:** Christopher Skinner   
Inspector General

**SUBJECT:** The Federal Election Commission's (FEC) Fiscal Year (FY) 2019 Financial Statement Audit Report

**DATE:** November 19, 2019

**ENCLOSURE:** Independent Audit of the U.S. Federal Election Commission's Fiscal Year 2019 Financial Statement Audit Report

Pursuant to the Chief Financial Officers Act of 1990, as amended, this memorandum transmits the subject audit report issued by Brown & Company Certified Public Accountants and Management Consultants, PLLC (Brown & Company).<sup>1</sup> Enclosed you will find the Independent Auditor's final audit report on the FEC FY 2019 Financial Statements. The final audit report is additionally included in Section II of the FEC's FY 2019 Agency Financial Report.

The audit was performed under a contract with, and monitored by the 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.<sup>2</sup>

In Brown & Company's opinion, the FEC 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, 2019, in conformity with accounting principles generally accepted in the United States of America.

Additionally, due to the agency's position 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. Therefore, the audit included an examination of FEC IT security in comparison to government-wide best practices. The OIG acknowledges that the independent auditors are only required to explicitly opine on internal controls that have a material impact on agency financial statement reporting.

The audit report identified internal control deficiencies related to IT security and as a result, documented seven (7) recommendations<sup>3</sup> to address the internal control deficiencies.

---

<sup>1</sup> The FEC Office of Inspector General (OIG) contracted with Brown & Company, an Independent Auditor, to perform the FEC FY 2019 Financial Statement Audit.

<sup>2</sup> And applicable provisions of Office of Management and Budget (OMB) Bulletin No. 17-03, Audit Requirements for Federal Financial Statements.

<sup>3</sup> Five (5) recommendations were repeated from prior years' Financial Statement Audit Reports.

The OIG acknowledges that corrective actions by management resulted in the closure of two (2) recommendations from the FY 2018 Financial Statement Audit Report. The OIG provided FEC management a draft copy of the audit report for review and comment. The official management response to the report can be found in Exhibit C of the enclosed report.

The OIG reviewed Brown & Company's report and related documentation and provided the required oversight throughout the course of the audit. Our review is permitted to ensure the accuracy of the audit conclusions but not to express an opinion of its results. The OIG's review indicated that Brown & Company complied, in all material respects, with Government Auditing Standards.

In accordance with *OMB Circular No. A-50, Audit Follow-up*, revised, the FEC is to prepare a corrective action plan (CAP) that will set forth the specific actions planned, as well as other detail requirements, to implement the agreed upon recommendations. Per Commission Directive 50, *Audit Follow-up*, the Commission has designated the Chief Financial Officer as the audit follow-up official (AFO) for FEC financial statement audits. The AFO has thirty (30) days from the issuance of the final audit report release date to provide the OIG with a draft CAP that outlines the agencies strategy to address the report findings and recommendations. The OIG will review the CAP and provide any comments within fifteen (15) days of receipt. Then, the AFO will finalize the CAP and provide it to the Commissioners with a courtesy copy to the OIG.

We appreciate the collaboration and support from FEC staff and the professionalism that Brown & Company exercised throughout the course of the audit. If you have any questions concerning the enclosed report, please contact my office at (202) 694-1015.

Thank you.

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

**FEDERAL ELECTION COMMISSION**

**INDEPENDENT AUDITOR'S REPORT**

**FOR THE YEARS ENDED  
SEPTEMBER 30, 2019 AND 2018**



**Prepared By:  
Brown & Company CPAs and Management Consultants, PLLC  
November 19, 2019**

## Table of Contents

Independent Auditor's Report .....	1
Exhibit A - Significant Deficiencies .....	7
Exhibit B - Status of Prior Year's Findings and Recommendations .....	17
Exhibit C - Management's Response to the Auditor's Report .....	18



## **Independent Auditor's Report**

Inspector General  
Federal Election Commission  
Washington, D.C.

In our audit of the fiscal year 2019 financial statements of the Federal Election Commission (FEC), we found:

- FEC's financial statements as of and for the fiscal year ended September 30, 2019, are presented fairly, in all material respects, in accordance with U.S. generally accepted accounting principles;
- no material weaknesses in internal control over financial reporting based on the limited procedures we performed; and
- no reportable noncompliance for fiscal year 2019 with provisions of applicable laws, regulations, contracts, and grant agreements we tested.

The following sections discuss in more detail (1) our report on the financial statements, which includes required supplementary information (RSI) and other information included with the financial statements; (2) our report on internal control over financial reporting; and (3) our report on compliance with laws, regulations, contracts, and grant agreements.

### **Report on the Financial Statements**

In accordance with the provisions of Accountability of Tax Dollars Act of 2002 (ATDA) (Pub. L. No. 107-289), we have audited FEC's financial statements. FEC's financial statements comprise the balance sheets as of September 30, 2019, the related statements of net cost, changes in net position, budgetary resources, and custodial activity for the fiscal years then ended; and the related notes to the financial statements.

We conducted our audit in accordance with U.S. generally accepted government auditing standards and the provisions of Office of Management and Budget (OMB) Bulletin No. 19-03, *Audit Requirements for Federal Financial Statements*. We believe that the audit evidence we obtained is sufficient and appropriate to provide a basis for our audit opinions.

### Management's Responsibility

FEC's management is responsible for (1) the preparation and fair presentation of these financial statements in accordance with U.S. generally accepted accounting principles; (2) preparing, measuring, and presenting the RSI in accordance with U.S. generally accepted accounting principles; (3) preparing and presenting other information included in documents containing the audited financial statements and auditor's report, and ensuring the consistency of that information with the audited financial statements and the RSI; and (4) maintaining effective internal control over financial reporting, including 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 fraud or error.

### Auditor's Responsibility

Our responsibility is to express an opinion on these financial statements based on our audit. U.S. generally accepted government auditing standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement. We are also responsible for applying certain limited procedures to RSI and other information included with the financial statements.

An audit of financial statements involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the auditor's assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, 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 an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit of financial statements also involves evaluating the appropriateness of the accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements. Our audit also included performing such other procedures as we considered necessary in the circumstances.

### Opinion on Financial Statements

In our opinion, FEC's financial statements present fairly, in all material respects, FEC's financial position as of September 30, 2019, and its net cost of operations, changes in net position, budgetary resources, and custodial activity for the fiscal years then ended in accordance with U.S. generally accepted accounting principles.

### **Other Matters**

#### Prior Period Financial Statements Audited by a Predecessor Auditor

The FEC's financial statements as of and for the period ending September 30, 2018 were audited by a predecessor auditor, Leon Snead & Company, P.C. The predecessor auditor expressed an unmodified opinion on the financial statements. The audit report was dated November 15, 2018.

#### Required Supplementary Information

U.S. generally accepted accounting principles issued by the Federal Accounting Standards Advisory Board (FASAB) require that the RSI be presented to supplement the financial statements. Although the RSI is not a part of the financial statements, FASAB considers this information to be an essential part of financial reporting for placing the financial statements in appropriate operational, economic, or historical context. We have applied certain limited procedures to the RSI in accordance with U.S. generally accepted government auditing standards, which consisted of inquiries of management about the methods of preparing the RSI and comparing the information for consistency with management's responses to the auditor's inquiries, the financial statements, and other knowledge we obtained during the audit of the financial statements, in order to report omissions or material departures from FASAB guidelines, if any, identified by these limited procedures.

We did not audit and we do not express an opinion or provide any assurance on the RSI because the limited procedures we applied do not provide sufficient evidence to express an opinion or provide any assurance.

#### Other Information

FEC's other information contains a wide range of information, some of which is not directly related to the financial statements. This information is presented for purposes of additional analysis and is not a required part of the financial statements or the RSI. We read the other information included with the financial statements in order to identify material inconsistencies, if any, with the audited financial statements. Our audit was conducted for the purpose of forming an opinion on FEC's financial statements. We did not audit and do not express an opinion or provide any assurance on the other information.

#### **Report on Internal Control over Financial Reporting**

In connection with our audit of FEC's financial statements, we considered FEC's internal control over financial reporting, consistent with our auditor's responsibility discussed below. We performed our procedures related to FEC's internal control over financial reporting in accordance with U.S. generally accepted government auditing standards.

#### Management's Responsibility

FEC management is responsible for maintaining effective internal control over financial reporting, including 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 fraud or error.

#### Auditor's Responsibility

In planning and performing our audit of FEC's financial statements as of and for the year ended September 30, 2019, in accordance with U.S. generally accepted government auditing standards, we considered the FEC's internal control over financial reporting 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 FEC's internal control over financial reporting. Accordingly, we do not express an opinion on FEC's internal control over financial reporting. We are required to report all deficiencies that are considered to be significant deficiencies or material weaknesses. We did not consider all internal controls relevant to operating objectives, such as those controls relevant to preparing performance information and ensuring efficient operations.

*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 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.



## Definition and Inherent Limitations of Internal Control over Financial Reporting

An entity's internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, the objectives of which are to provide reasonable assurance that (1) transactions are properly recorded, processed, and summarized to permit the preparation of financial statements in accordance with U.S. generally accepted accounting principles, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition, and (2) transactions are executed in accordance with provisions of applicable laws, including those governing the use of budget authority, regulations, contracts, and grant agreements, noncompliance with which could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct, misstatements due to fraud or error.

## Results of Our Consideration of Internal Control over Financial Reporting

Our consideration of internal control was for the limited purpose described above, and was not designed to identify all deficiencies in internal control that might be material weaknesses and significant deficiencies or to express an opinion on the effectiveness of FEC's internal control over financial reporting. Therefore, material weaknesses or significant deficiencies may exist that have not been identified. Given these limitations, during our audit, we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. However, we identified certain deficiencies in internal control, described below and in Exhibit A that we consider to be significant deficiencies.

1. Agency corrective action plans are not compliant with government requirements.
2. FEC shall review information system accounts.
3. FEC needs to update the separation of duties policy.
4. USGCB<sup>1</sup> requirements need to be implemented Agency-wide.
5. FEC has not fully implemented and tested their Agency Continuity of Operations Plan and Disaster Recovery Plan for IT systems.
6. FEC shall develop system-specific Contingency Plans.
7. FEC needs to apply session lock requirements to all workstations.

## Intended Purpose of Report on Internal Control over Financial Reporting

The purpose of this report is solely to describe the scope of our consideration of FEC's internal control over financial reporting and the results of our procedures, and not to provide an opinion on the effectiveness of the FEC's internal control over financial reporting. This report is an integral part of an audit performed in accordance with U.S. generally accepted government auditing standards in considering internal control over financial reporting. Accordingly, this report on internal control over financial reporting is not suitable for any other purpose.

## **Report on Compliance with Laws, Regulations, Contracts, and Grant Agreements**

In connection with our audit of FEC's financial statements, we tested compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements consistent with our auditor's responsibility discussed below. We caution that noncompliance may occur and not be detected by these tests.

---

<sup>1</sup> United States Government Configuration Baseline (USGCB).

We performed our tests of compliance in accordance with U.S. generally accepted government auditing standards.

#### Management's Responsibility

FEC management is responsible for complying with laws, regulations, contracts, and grant agreements applicable to FEC.

#### Auditor's Responsibility

Our responsibility is to test compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements applicable to FEC that have a direct effect on the determination of material amounts and disclosures in FEC's financial statements, and perform certain other limited procedures. Accordingly, we did not test compliance with all laws, regulations, contracts, and grant agreements applicable to FEC.

#### Results of Our Tests for Compliance with Laws, Regulations, Contracts, and Grant Agreements

Our tests for compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements disclosed no instances of noncompliance for FY 2019 that would be reportable under U.S. generally accepted government auditing standards. However, the objective of our tests was not to provide an opinion on compliance with laws, regulations, contracts, and grant agreements applicable to FEC. Accordingly, we do not express such an opinion.

#### Intended Purpose of Report on Compliance with Laws, Regulations, Contracts, and Grant Agreements

The purpose of this report is solely to describe the scope of our testing of compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements, and the results of that testing, and not to provide an opinion on compliance. This report is an integral part of an audit performed in accordance with U.S. generally accepted government auditing standards in considering compliance. Accordingly, this report on compliance with laws, regulations, contracts, and grant agreements is not suitable for any other purpose.

#### **Status of Prior Year's Findings and Recommendations**

We have reviewed the status of open recommendations from the prior year's Independent Auditor's Report, dated November 15, 2018. The status of prior year recommendations is presented in Exhibit B.

#### **Management's Response to the Auditor's Report**

Management has presented a response to the findings identified in our report. Management's response to the report is presented in Exhibit C. We did not audit FEC's response and, accordingly, we express no opinion on it.

#### **Evaluation of Management's Response to the Auditor's Report**

In response to the draft report, FEC provided its plans to address the findings, and agreed with the recommendations to improve information system security controls. FEC comments are included in their entirety in Exhibit C.

This report is intended solely for the information and use of the management of FEC, OMB, and the U.S. Congress, and is not intended for any other purpose.

*Brown & Company*  
Greenbelt, Maryland  
November 19, 2019

# Exhibit A - Significant Deficiencies

## Findings and Recommendations

### IT Finding 2019-01: Agency Corrective Action Plans Are Not Compliant With Government Requirements (Repeat Finding)

#### Condition:

During the fiscal year (FY) 2019 audit, the FEC Deputy Chief Information Officer informed the auditor that the agency has not implemented the FY 2018 recommendation to update the corrective action plans (CAP). As stated in FY 2018 audit report, FEC's corrective action plan for the internal control deficiencies reported in prior financial statement audit reports does not meet the OMB requirements. Also, FEC was not able to provide an updated plan of action and milestone report as of June 30, 2019.

To determine whether the agency met federal standards and their own internal requirements, the auditor reviewed the June 2018 CAP. The 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.

#### Criteria:

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 are 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.

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.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision (Rev.) 2, *Risk Management Framework (RMF) for Information Systems and Organizations*, December 2018, states the following in regard to plan of action and milestones:

*Plan of Action and Milestones, Task A-6:* Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports.

Discussion: The plan of action and milestones is included as part of the authorization package. The plan of action and milestones describes the actions that are planned to correct deficiencies in the controls identified during the assessment of the controls and during continuous monitoring. The plan of action and milestones includes tasks to be accomplished with a recommendation for completion before or after system authorization; resources required to accomplish the tasks; milestones established to meet the tasks; and the scheduled completion dates for the milestones and tasks.

NIST SP 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, - Building Effective Assessment Plans*, December 2014, Security Control CA-5, Plan of Action and Milestones, states the following:

Determine if the organization:

- Develops a plan of action and milestones for the information system to:
  - document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls;
  - reduce or eliminate known vulnerabilities in the system;
- Defines the frequency to update the existing plan of action and milestones;
- Updates the existing plan of action and milestones with the organization-defined frequency based on the findings from:
  - security controls assessments;
  - security impact analyses; and
  - continuous monitoring activities

**Cause:**

FEC lacks procedures to comply with the requirements for a plan of actions and milestones that meet federal requirements. This condition is also caused by a need for additional oversight and monitoring to ensure the agency meets Commission Directive A-50 and related OMB regulations.

**Effect:**

Without an adequate CAP, the agency is unable to:

- Track the implementation of corrective actions for reported deficiencies;
- Ensure that realistic milestones are established;
- Ensure that targeted resolution dates are consistently met to reduce the agency's risk exposure; and
- Determine if risks are not accepted, mitigated or responded to with actionable plans and decisions.

**Recommendation 1:**

We recommend that the FEC Chief Information Officer develop and update, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated

remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

**Finding 2019-02: FEC Shall Review Information System Accounts (Repeat Finding)**

**Condition:**

The *FEC Account Management Policy*, Policy Number 58-2.2 was adopted in September 2004 and updated in February 2017. The policy states the following:

It is FEC policy that: All user account access rights and privileges should be reviewed annually and validated in accordance with General Support System and Major Application system security plans by the user's Direct Manager.

The FEC relies on the effectiveness of account management controls for users to gain and maintain access to FEC's systems, and does not enforce the requirement for the Direct Manager to annually review information system accounts.

**Criteria:**

NIST *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)*, Version 1.1, April 2018, states the following in regard to segregation of duties:

*Access Control (PR.AC):* Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.

NIST Special Publication (SP) 800-53A, Revision 4 (Rev. 4), *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, - Building Effective Assessment Plans*, December 2014, Security Control AC-5, Separation of Duties, states the following:

Determine if the organization:

- Defines the frequency to review accounts for compliance with account management requirements;
- Reviews accounts for compliance with account management requirements with the organization-defined frequency.

**Cause:**

Due to lack of resources, FEC has not provided the Direct Manager with information required to review information system accounts on a periodic basis.

**Effect:**

The lack of review of information system accounts increases the risk of unauthorized access to FEC's information and information systems.

## **Recommendation 2:**

We recommend that the FEC review information system accounts in accordance with organization-defined frequency; and the FEC initiates required actions on information system accounts based on the review.

## **Finding 2019-03: FEC Needs to Update the Separation of Duties Policy**

### **Condition:**

The *FEC Segregation of Duties Policy*, Policy Number 58-2.7 was adopted in September 2004 and updated in February 2010. The policy states the following:

As resources permit, a division of roles and responsibilities relating to electronic information and computing resources should be implemented to exclude the possibility for a single individual to subvert a critical process.

In particular, a segregation of duties should be maintained between the following functions:

- Information systems use,
- Data entry,
- Computer operation,
- Network management,
- System administration,
- Systems development and maintenance,
- Change management,
- Security administration, and
- Security audit.

As stated above, FEC's policy defines duties of individuals to be separated as recommended by federal guidelines. However, FEC's policy does not "define information system access authorizations to support separation of duties between users," which is also recommended for federal agencies. Information system access authorization is the function of specifying access rights/privileges to resources related to information security and computer security in general and to access control in particular. Separation of duties includes, for example, ensuring security personnel administering access control functions do not also administer audit functions.

### **Criteria:**

NIST Special Publication (SP) 800-37, Revision (Rev.) 2, *Risk Management Framework (RMF) for Information Systems and Organizations*, December 2018, states the following in regard to segregation of duties:

*Risk Management Roles, Task P-1:* Identify and assign individuals to specific roles associated with security and privacy risk management.

NIST *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)*, Version 1.1, April 2018, states the following in regard to segregation of duties:

*Access Control (PR.AC):* Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties

NIST SP 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, - Building Effective Assessment Plans*, December 2014, Security Control AC-5, Separation of Duties, states the following:

Determine if the organization:

- Defines duties of individuals to be separated;
- Separates organization-defined duties of individuals;
- Documents separation of duties; and
- Defines information system access authorizations to support separation of duties.

**Cause:**

FEC is in the process of re-assessing FEC's information system security controls. Due to competing priorities and lack of resources, FEC has not updated the *Separation of Duties Policy* to include information system access authorizations.

**Effect:**

The lack of defining information system access authorizations as part of the *Segregation of Duties Policy* increases the risk of agency's intended policy and procedures not being implemented and monitored. Lack of compliance with agency's procedures increases the risk of unauthorized or unintentional modification or misuse of the organization's information assets.

**Recommendation 3:**

We recommend that the FEC update the FEC's *Segregation of Duties Policy* to include defining information system access authorizations to support separation of duties.

**IT Finding 2019-04: USGCB Requirements Need to be Implemented Agency-wide (Repeat Finding)**

**Condition:**

During the FY 2019 audit, the FEC Deputy Chief Information Officer informed the auditor that the FEC has not fully implemented The United States Government Configuration Baseline (USGCB)<sup>2</sup> configuration standards for all workstations. The agency is currently conducting tests and reviews to install Windows 10 on agency laptops and workstations. Since the FEC is in the process of replacing Windows 7 with Windows 10, the agency did not take action to implement USGCB on all Windows 7 laptops and workstations.

**Criteria:**

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 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 Chief Information Officers Council, "the USGCB initiative falls within FDCC and comprises the configuration settings component of FDCC."

---

<sup>2</sup> 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 effective configuration settings focusing primarily on security.



NIST Special Publication (SP) 800-53A, Revision 4 (Rev. 4), *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, - Building Effective Assessment Plans*, December 2014, Security Control CA-6, Configuration Settings, states the following:

Determine if the organization:

- Establishes and documents configuration settings for information technology products employed within the information system using organization-defined security configuration checklists;
- Implements the configuration settings;
- Identifies any deviations from established configuration settings for organization-defined information system components based on organizational-defined operational requirements; and
- Monitors changes to the configuration settings in accordance with organizational policies and procedures.

**Cause:**

FEC's implementation of Windows 10 is expected to be completed in January 2020 and to include the USGCB configuration requirements. Therefore, the agency did not apply resources to ensure USGCB configuration settings are installed on all laptops and workstations that have Windows 7.

**Effect:**

The FEC's systems and information remain at risk until full implementation of the USGCB configuration requirements.

**Recommendation 4:**

We recommend that the FEC implement USGCB baseline configuration standards for all workstations regardless of the current hardware in use.

**IT Finding 2019-05: FEC Has Not Fully Implemented and Tested Their Agency Continuity of Operations Plan and Disaster Recovery Plan for IT Systems (Repeat Finding)**

**Condition:**

During the FY 2019 audit, the FEC Deputy Chief Information Officer informed the auditor that the agency has not tested the Continuity of Operations Plan (COOP) or Disaster Recovery Plan. The FEC *Continuity of Operations and Disaster Recovery Policy*, Policy Number 58-2.9, was adopted in September 2004, and updated in February 2010. The FEC policy states:

Business continuity and disaster recovery plans should be tested/re-assessed on a regular basis.

- Plans should not be considered valid until tested for practicality, executability, errors and/or omissions. The initial validation test should consist of a simulation or tactical test.
- Once validated, plans should be tested annually, or when substantive changes occur to the system, to the system environment, or to the plan itself.
- Test results should be maintained in a journal format and retained for analysis.
- Validated change recommendations resulting from testing activities should be incorporated into plans immediately.

However, the FEC did not comply with standard business continuity plans. For example, the FEC has operated for 15 years without an approved and tested COOP and Disaster Recovery Plan to ensure that in the event of a disaster, the Commission would have the ability to continue normal business operations within a reasonable timeframe. FEC provided a COOP specific Corrective Action Plan related to the Office Inspector General's, *Inspection of the FEC's Disaster Recovery Plan and Continuity of Operations Plans*, released in January 2013. The auditor 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 was estimated to be completed by the end of December 2018.

The FEC held a meeting to develop a strategy for testing the plans, but the FEC has not formulated a plan to test the COOP and Disaster Recovery plan.

**Criteria:**

NIST Special Publication (SP) 800-34, Revision (Rev.) 1, *Contingency Planning Guide for Federal Information Systems*, dated May 2010, 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.

NIST SP 800-84, *Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities*, September 2006, provides guidelines on designing, developing, conducting, and evaluating test, training, and exercise (TT&E) events so that organizations can improve their ability to prepare for, respond to, manage, and recover from adverse events.

NIST SP 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, - Building Effective Assessment Plans*, December 2014, Security Control CP-4, Contingency Plan Testing, states the following:

Determine if the organization:

- Tests the contingency plan for the information system with the organization-defined frequency, using organization-defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan;
- Reviews the contingency plan test results; and
- Initiates corrective actions, if needed.

**Cause:**

FEC has not made it a high priority to apply resources to test the COOP and Disaster Recovery Plan and determine the agency's readiness to execute the plans.

**Effect:**

The disaster recovery plans could fail because they were not tested, maintained or re-assessed. 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.

**Recommendation 5:**

We recommend that the FEC update, reassess, test, and maintain the COOP and Disaster Recovery Plan regularly to determine that they are up to date and effective.

**IT Finding 2019-06: FEC Shall Develop System-Specific Contingency Plans  
(Repeat Finding)**

**Condition:**

The FEC has not developed system specific contingency plans. The FEC *Continuity of Operations and Disaster Recovery Policy*, Policy Number 58-2.9, was adopted in September 2004, and updated in February 2010. The FEC policy states:

Business continuity and disaster recovery plans should be developed within a common framework; each plan should contain the following minimum elements:

- Application-specific or system-specific definitions of outages, emergencies, crises and disasters;
- Identification of the person (or persons) by functional title who are authorized to declare information system outages, emergencies, crises and disasters;
- Resumption, recovery, and restoration objectives and options, including the information systems' resumption and restoration priorities, operational and monetary costs, escalation criteria and key decision-points;
- Team assignments, to include the names, functional titles, and current contact data for primary and alternate personnel who make up the response team. As appropriate, similar information will be provided for alternate processing/recovery site team members; and
- Contact and coordination information for federal emergency management authorities.

However, the FEC did not implement the agency's policy to develop system-specific contingency plans for critical information systems.

**Criteria:**

NIST Special Publication (SP) 800-34, Revision (Rev.) 1, *Contingency Planning Guide for Federal Information Systems*, dated May 2010, 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.

NIST SP 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations - Building Effective Assessment Plans*, December 2014, Security Control CP-2, Contingency Plan, states the following:

Determine if the organization:

- Develops a contingency plan for the information system that:
  - Identifies essential missions and business functions and associated contingency requirements;
  - Provides recovery objectives, restoration priorities, and metrics;
  - Addresses contingency roles, responsibilities, assigned individuals with contact information;
  - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; and
  - Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.

**Cause:**

FEC has not made it a high priority to apply resources to develop system-specific contingency plans and determine the agency's readiness to execute the plans.

**Effect:**

Without system-specific contingency plans, the FEC increases the risk of not implementing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level.

**Recommendation 6:**

We recommend that the FEC develop system-specific contingency plans, as appropriate for the agency risk level.

**Finding 2019-07: FEC Needs to Apply Session Lock Requirements to All Workstations**

**Condition:**

We examined FEC's group policy for session lock after invalid attempts by privilege users and non-privilege users and noted the setting for "account lockout duration" is 30 minutes. The agency's Group Policy is computer-based (as opposed to user-based) and therefore the settings are the same for non-privilege and privilege accounts.

The FEC *Account Management Procedures*, was adopted in September 2004 and updated in February 2017. The document, which includes LAN Account Procedures for Disable/Suspend Account, states that "FEC will automatically terminate session after sixty (60) minutes of inactivity."

We noted that FEC needs to update the account management procedures to agree with the group policy.

We also noted that FEC does not apply the session lock group policy consistently across all workstations. We tested the effectiveness of this control at the workstation assigned to the auditor, and found that group policy was not assigned to the workstation. Therefore, the session continued for over an hour without any activity.

**Criteria:**

NIST Special Publication (SP) 800-53A, Revision 4 (Rev. 4), *Assessing Security and Privacy Controls in Federal Information Systems and Organizations - Building Effective Assessment Plans*, December 2014, Security Control AC-11, Session Lock states the following:

Determine if:

- The organization defines the time period of user inactivity after which the information system initiates a session lock;
- The information system prevents further access to the system by initiating a session lock after organization-defined time period of user inactivity or upon receiving a request from a user; and
- The information system retains the session lock until the user reestablishes access using established identification and authentication procedures.

**Cause:**

Due to lack of monitoring and oversight, FEC has not consistently implemented policies for session lockout.

**Effect:**

The lack of review of session lockout controls increases the risk of unauthorized access to FEC's information and information systems.

**Recommendation 7:**

We recommend that the FEC implement session lockout control in accordance with organization-defined procedures.

## Exhibit B - Status of Prior Year's Findings and Recommendations

Number	Status of FY 2018 and Prior Year's Audit Recommendations	Status as of September 30, 2019
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.	Closed in FY 2019
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 See Finding 1
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 See Finding 2
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 See Finding 2
5.	Implement USGCB baseline configuration standards for all workstations regardless of the current hardware in use.	Open See Finding 4
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 See Finding 5
7.	Develop system specific contingency plans, as required by the NIST RMF.	Open See Finding 6
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.	Closed in FY 2019

# Exhibit C - Management's Response to the Auditor's Report



FEDERAL ELECTION COMMISSION  
Washington, DC 20463

November 18, 2019

On behalf of Federal Election Commission (FEC) Management, I would like to thank the FEC Office of the Inspector General and Brown & Company for their diligent work auditing the FEC's FY 2019 financial statements. The unmodified opinion you rendered is reflective of the hard work and continued process improvements made by the FEC staff. The close-out of two reoccurring recommendations from the FY 2018 financial statement audit demonstrates significant progress in improving the FEC's IT security posture. We also note that the financial statement audit made several other recommendations related to IT systems and corrective action plan reporting. Enclosed herein is responses to those recommendations, as provided by the FEC Chief Information Officer.

On behalf of Management,

A handwritten signature in black ink, appearing to read "John Quinlan".

John Quinlan  
Chief Financial Officer

## Agency Response to the Draft Report



**FEDERAL ELECTION COMMISSION**  
Washington, DC 20463

The FEC continues on the path to remediate all findings. Our responses provide an overview of how we plan to remediate each of the findings.

### **Findings and Recommendations**

#### **Recommendations**

1. We recommend the FEC Chief Information Officer develop and update, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

#### **Management's Response**

Management continued to update and report on corrective action plans throughout FY 2019, in accordance with the timeline identified in Commission Directive-50, and remains fully committed to reducing or eliminating known vulnerabilities in the agency's information system. However, Management agrees with the Auditor's recommendation to improve the process for documenting and tracking the agency's planned, implemented and evaluated remedial actions to correct deficiencies noted during the assessment of security controls. The agency was challenged in its efforts to complete these documentation improvements during FY 2019, in part by time and staff resources lost during the lapse in appropriations from December 22, 2018 to January 25, 2019, and by vacancies in the Information Security Office, which have now been filled.

2. We recommend the FEC reviews information system accounts in accordance with organization-defined frequency; and the FEC initiates required actions on information system accounts based on the review.

#### **Management'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. In 2019, the OCIO additionally implemented strict account management



## **Agency Response to the Draft Report**

procedures for Active Directory Domain Administrators and Office 365 Global Administrators by enforcing multi-factor authentication. These Administrators are now required to provide an additional level of authentication to access their respective systems. OCIO also began work on a multi-phase project to redevelop the current FEC System Access system to improve steps for users to gain and maintain access to FEC systems. OCIO continues to research effective ways to review account management procedures. If an effective procedure is found for a reasonable cost, it will be implemented to enable supervisors to review user access authorities annually.

3. We recommend the FEC updates the FEC's *Segregation of Duties Policy* to include defining information system access authorizations to support separation of duties.

### **Management's Response**

Management concurs with this finding. The OCIO will work to update the *Separation of Duties Policy* to include information access authorizations, with a target completion date of June 2020. The final adoption of any proposed policy change is contingent up the restoration of a quorum of four FEC Commissioners.

4. We recommend the FEC implement USGCB baseline configuration standards for all workstations regardless of the current hardware in use.

### **Management's Response**

Management concurs with the Auditor regarding the implementation of the USGCB as applied to the Windows 7 environment used by the agency in past years. As a result, the OCIO initially accelerated the review and testing of USGCB to analyze and determine the best approaches in meeting the FEC's infrastructure needs. However, following the announcement that Windows 7 was nearing end-of-life, the OCIO determined that the best use of internal resources in 2018 would be to focus on enterprise system and application compatibility running on the Windows 10 platform. In 2019, the OCIO actively started the process of replacing the Windows 7 operating system with Windows 10 for all users and contractors, which includes a hardware refresh. USGCB does not apply to the Windows 10 platform, so these settings will not be applied.

NIST has published a security technical implementation guide (STIG) for Windows 10 to improve the security of DoD systems to be used by other government agencies in conjunction with browser, antivirus and other third-party tools. In an effort to remove Windows 7 from our infrastructure as soon as possible, the OCIO has not finalized testing of these STIGs but has successfully implemented various security tools on the desktop level which include antivirus, 24-hr security operations center and virtualization-based security.

5. We recommend the FEC updates, reassesses, tests, and maintains the COOP and Disaster Recovery Plan regularly to determine that they are up to date and effective.

### **Management's Response**

In 2019, Management received funding approval to seek consulting services to update the

### **Agency Response to the Draft Report**

agency's COOP Plan. As part of the update to our plan, Management anticipates reviewing, with the assistance of the consultant, best practice for table top exercises, taking into consideration FEC's culture and infrastructure. To date, an award has been issued for these consulting services, and the OCIO is actively engaged in updating the COOP Plan as well as reviewing test plans and exercises.

6. We recommend the FEC develop system-specific contingency plans, as appropriate for the agency risk level.

#### **Management's Response**

The OCIO completed an ISCP for the Presidential Matching funds system; however Management has ceased work on the remaining systems. In 2019, Management received funding approval to seek consulting services to update the COOP Plan and has since issued an award. As part of the update process, existing DRPs will be reviewed and, if possible, incorporated into ISCPs after a completed BIA is performed. Work is planned to resume on completing ISCPs after the list of critical systems has been updated, per the BIA.

7. We recommend the FEC implement session lockout control in accordance with organization-defined procedures

#### **Management's Response**

Management agrees with this recommendation. The OCIO has a group policy object (GPO) that defines the time period of user inactivity enforced at the domain level. Management, in coordination with the OCIO team, will review this GPO to ensure it is applied to all active directory organizational units and not blocked by a competing policy.