




Federal Election Commission
Office of the Inspector General

MEMORANDUM

TO: The Commission

FROM: Christopher Skinner 

SUBJECT: Transmittal of the Federal Election Commission's Fiscal Year 2020 Financial Statement Audit Report

DATE: November 16, 2020

Pursuant to the Chief Financial Officers Act of 1990, as amended, this memorandum transmits the Independent Auditor's Report issued by Brown & Company Certified Public Accountants and Management Consultants, PLLC (Brown & Company) for the fiscal year (FY) ending September 30, 2020. Enclosed you will find the Independent Auditor's final audit report on the FEC (*i.e.*, the "FEC" or "Commission") FY 2020 Financial Statements. The final audit report is additionally included in Section II of the FEC's FY 2020 Agency Financial Report

The audit was performed under a contract with, and monitored by, the OIG in accordance with generally accepted government auditing standards, the Comptroller General's *Government Auditing Standards*, and applicable provisions of Office of Management and Budget (OMB) Bulletin No. 17-03, *Audit Requirements for Federal Financial Statements*.

In Brown & Company's opinion, the financial statements present fairly, in all material respects, the financial position, net cost, changes in net position, budgetary resources, and custodial activity of the FEC as of, and for the year ending, September 30, 2020, in conformance with accounting principles generally accepted in the United States of America.

Additionally, due to the Commission's position that it is legally exempt from the Federal Information Systems Management Act (FISMA), the OIG requires an assessment of the agency's Information Technology (IT) systems security controls. Accordingly, the audit included an examination of the Commission's 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.

Brown & Company did not report any material weaknesses. However, they identified significant deficiencies with the Commission's internal controls related to IT security and documented six recommendations (four of which were repeat recommendations from the FY 2019 report) to address the deficiencies noted. The OIG acknowledges that three prior year recommendations have been closed. Management was provided a draft copy of the audit report for review and comment, and the official management comments to the report can be found in Exhibit C of the report.

The OIG reviewed Brown & Company's report and related documentation and provided the required oversight throughout the course of the audit. Our review and oversight are limited to ensuring the audit complies with applicable standards; however, we do not express an opinion regarding its results. The OIG's review determined that Brown & Company complied, in all material respects, with applicable 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, along with other detailed requirements, to implement the agreed upon recommendations. Per Commission Directive 50, Audit Follow-up, the Commission has designated the Chief Financial Officer to be the audit follow-up official (AFO) for the financial statement audit. The AFO has thirty days from the release date of the audit report to provide the OIG with a draft CAP that will address the report findings and recommendations. The OIG will review the CAP and provide any comments within fifteen days of receipt. Thereafter, the AFO will finalize the CAP and provide the final CAP 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
Lisa Stevenson, Acting General Counsel
Gilbert A. Ford, Director of Budget
Greg Baker, Deputy General Counsel
Christine McClarin, Acting Deputy Staff Director for Management and Administration





Federal Election Commission
Office of the Inspector General

Audit of the Federal Election Commission Annual Financial Statements Fiscal Year 2020

November 2020

FEDERAL ELECTION COMMISSION

INDEPENDENT AUDITOR'S REPORT

FOR THE YEARS ENDED
SEPTEMBER 30, 2020 AND 2019



Prepared By:
Brown & Company CPAs and Management Consultants, PLLC
November 16, 2020

Table of Contents

Independent Auditor's Report	1
Exhibit A - Significant Deficiencies	6
Exhibit B - Status of Prior Year's Findings and Recommendations	14
Exhibit C - Management's Response to the Auditor's Report	15



BROWN & COMPANY

CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS, PLLC

Independent Auditor's Report

Inspector General
Federal Election Commission
Washington, D.C.

In our audit of the fiscal year 2020 and 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, 2020, and 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 2020 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, 2020 and 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. 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, 2020, and 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

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, 2020, 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.

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, material weaknesses may exist that have not been identified.

During our FY 2020 audit, we identified deficiencies in FEC's internal control over financial reporting that we do not consider to be material weaknesses. Nonetheless, these deficiencies warrant FEC management's attention. We have communicated these matters to FEC's management. Below and in Exhibit A are the significant deficiencies:

1. Logical account management activities are not consistently performed for separated users.
2. Baseline configuration standards are not fully implemented for all Windows devices.
3. Continuity of Operations Plan is not implemented and tested.
4. Security awareness training was not completed by all FEC system users.
5. Corrective Action Plans are not compliant with government requirements.

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. 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 2020 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 FY 2019 Independent Auditor's Report, dated November 19, 2019. 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. There are five findings of which two are new findings and six open recommendations. FEC comments are included in their entirety in Exhibit C.

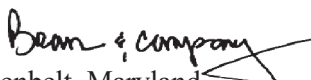

Greenbelt, Maryland
November 16, 2020

Exhibit A - Significant Deficiencies

Effectiveness of Information System Controls Over Financial Reporting

Findings and Recommendations

IT Finding 2020-01: Logical Account Management Activities Are Not Consistently Performed For Separated User (Repeat Finding)

Condition:

We identified an inconsistent implementation of FEC's account management controls for separated employees. FEC account management did not document its annual review of user accounts for the General Support System (GSS) and major application systems in accordance with their system security plan. Specifically, FEC's account management did not review user account access rights and privileges for the financial systems such as the WebTA, Pegasys and Comprizon systems. As a result, FEC management did not timely remove system user's accounts when the user separated from the agency.

Based on our review of active IT System user accounts, we identified:

- three of eleven GSS users were not removed timely; and
- one of 302 WebTA user accounts was not removed timely.

We note that upon notifying management of this finding, the three GSS user accounts were immediately removed.

Criteria:

NIST Special Publication (SP) 800-53, Revision 4 (Rev. 4), *Security and Privacy Controls for Federal Information Systems and Organizations*, Security Control AC-2 Account Management, states the following:

Control: The organization:

...

- f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
- g. Monitors the use of information system accounts;
- h. Notifies account managers:
 1. When accounts are no longer required;
 2. When users are terminated or transferred; and
 3. When individual information system usage or need-to-know changes;
- i. Authorizes access to the information system based on:
 1. A valid access authorization;
 2. Intended system usage; and
 3. Other attributes as required by the organization or associated missions/business functions;
- j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and
- k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

FEC Account Management Policy, states:

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 level of approval authority granted for user accounts should be based on the business criticality of the information or system to which the accounts are associated.

Accounts of users terminated under non-hostile circumstances should be suspended not later than the close of business (8:00 p.m.) of their final day of employment.

Cause:

FEC management has not complied with the FEC Account Management Policy or implemented sufficient monitoring controls to ensure compliance with NIST account management standards and guidelines.

Effect:

By not implementing a periodic review of all user accounts and disabling the accounts according to policy, there is an increased risk users could gain or retain unauthorized access and/or perform unauthorized functions and transactions within FEC systems.

Recommendation 1:

We recommend the FEC OCIO in conjunction with the direct managers perform and document periodic user access reviews for FEC systems according to the agency's system security plan.

IT Finding 2020-02: Baseline Configuration Standards Are Not Fully Implement For All Windows Devices.

Condition:

FEC has not fully implemented baseline configuration standards for all Windows environments in accordance with Security Technical Implementation Guide (STIG). A STIG is a cybersecurity methodology for standardizing security protocols within networks, servers, computers, and logical designs to enhance overall security. When implemented, these guides enhance security for software, hardware, physical and logical architectures to further reduce vulnerabilities.

FY 2020, FEC OCIO changed their standard configuration baseline requirements for Windows operating systems from the United States Government Configuration Baseline (USGCB) to STIG. The FEC OCIO is currently replacing Windows 7 operating systems with Windows 10 to meet the STIG requirements. However, the implementation of STIG configuration standards has not been fully implemented.

Criteria:

NIST Special Publication (SP) 800-53, Revision 4 (Rev. 4), *Security and Privacy Controls for Federal Information Systems and Organizations*, Security Control CM-2 Baseline Configuration, states the following:

Control:

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, Security Control CM-6, Configuration Settings, states the following:

Control: The organization:

- a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;
- b. Implements the configuration settings;
- c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and
- d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Cause:

The FEC OCIO postponed full implementation of the STIG baseline configuration standards last year because it was in the process of rolling out new laptops that would include Windows 10. However, this process was further delayed due to the COVID-19 environment constraints.

Effect:

FEC information systems are at increased risk by not implementing its STIG baseline configuration standards established for the agency.

Recommendation 2:

We recommend that the FEC OCIO fully implement STIG baseline configuration standards for Windows devices.

IT Finding 2020-03: Continuity Of Operations Plan Is Not Implemented And Tested (Repeat Finding)

Condition:

Based on our review of the most current FEC *Continuity of Operations Plan* (COOP) and other supporting documentation, we conclude that the COOP has not been fully implemented and tested. In FY 2020, the FEC OCIO updated the *FEC Continuity of Operation Plan*. However, FEC management has not performed test, training and exercise (TT&E) activities in accordance with the FEC COOP. TT&E aids in verifying that an organization's continuity plan is capable of supporting the continued execution of the organization's essential functions throughout the duration of a continuity event. Specifically, FEC has not fully developed, coordinated, and conducted TT&E to assess and validate its continuity plans, policies, procedures, and systems.

Also, as reported in prior periods, the FEC did not implement the agency's policy to develop system-specific contingency plans for critical information systems.

Criteria:

NIST Special Publication (SP) 800-53, Revision 4 (Rev. 4), *Security and Privacy Controls for Federal Information Systems and Organizations*, Security Control CP-2 Contingency Plan, states the following:

Control: The organization:

- a. Develops a contingency plan for the information system that:
 1. Identifies essential missions and business functions and associated contingency requirements;
 2. Provides recovery objectives, restoration priorities, and metrics;
 3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
- b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
- c. Coordinates contingency planning activities with incident handling activities;
- d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency];
- e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
- f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and
- g. Protects the contingency plan from unauthorized disclosure and modification.

NIST Special Publication (SP) 800-53, Revision 4 (Rev. 4), *Security and Privacy Controls for Federal Information Systems and Organizations*, Security Control CP-4 Contingency Plan Testing, states the following:

Control: The organization:

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

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.

Cause:

The FEC OCIO did not prioritize resources to implement and perform a routine test of its COOP to familiarize staff members with their roles and responsibilities during an emergency, ensure that systems and equipment are maintained in a constant state of readiness, and validate certain aspects of the COOP.

Effect:

Without implementing and testing a COOP before one is needed, increases the risk that the FEC's contingency plan would not include everything it needs and/or not be able to execute the plane in the most effective, efficient, and secure way

Recommendation 3:

We recommend the FEC OCIO utilize lessons learned from the COVID-19 pandemic to determine if any revisions are need to the *Continuity of Operation Plan*, and schedule periodic testing.

Recommendation 4:

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

IT Finding 2020-04: Security Awareness Training Was Not Completed By All FEC System Users

Condition:

Based on our review of FEC's security training status reports for FY 2020, all FEC system users (employees and contractors) did not complete security awareness training as required by the FEC *Federal Security Training and Awareness Policy*, Policy Number 58-1.2. The FEC Chief Information Officer (CIO) oversees the implementation and enforcement of the training policy. FEC OCIO provides training to all system users through its online training program that notifies users of training requirements and due dates. However, all system users did not complete the required training.

Specifically, based on our review of the security awareness training status reports, nine employees and one contractor of 379 system users listed did not complete training. Based on our review of the phishing training status report, one employee of 345 system users listed did not complete training.

Criteria:

National Institute of Standards and Technology (NIST) *Special Publication (SP) 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organization*, AT-2 Security Awareness Training, states the following:

Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

- a. As part of initial training for new users;
- b. When required by information system changes; and
- c. [Assignment: organization-defined frequency] thereafter.

FEC Security Training and Awareness Policy, Policy Number 58-1.2., states the following:

....

A training curriculum for each group of employees, vendors and consultants should be established and maintained; all personnel should be trained and educated in system security principles appropriate to their level of management responsibility and access.

Cause:

The FEC OCIO does not have effective procedures to enforce the *FEC Security Training and Awareness Policy* to ensure all system users complete annual training.

Effect:

Without adequate training, employee may not understand system security risks and their role in mitigating those risks.

Recommendation 5:

We recommend the FEC OCIO implement an effective procedure to enforce compliance with the security awareness training policy to ensure all system users complete security training in accordance with the *FEC Security Training and Awareness Policy*.

IT Finding 2020-05: Corrective Action Plans Are Not Compliant With Government Requirements (Repeat Finding)**Condition:**

During the fiscal year (FY) 2020 audit, the FEC Deputy Chief Information Officer updated the FEC Corrective Action Plan (CAP) and Plan of Action and Milestone (POA&M). However, the FEC CAP and POA&M need improvement to comply with government requirements. We identified the following areas where improvements are 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, 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 has not implemented 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:

The agency is unable to:

- 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 6:

We recommend that the FEC Chief Information Officer improve the plan of action and milestones report for the information system to include:

- Resources required to correct a control deficiency.
- Critical path milestones that affect the overall schedule for implementing the corrective actions are needed to resolve the control deficiency.
- Plan for prompt resolution and internal control testing to validate the correction of the control deficiency.

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

Number	Status of FY 2019 and Prior Year's Audit Recommendations	Status as of September 30, 2020
1.	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 5
2.	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 1
3.	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 1
4.	Implement USGCB baseline configuration standards for all workstations regardless of the current hardware in use.	Closed
5.	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 requires tests in a timely manner.	Open See Finding 3
6.	Develop system specific contingency plans, as required by the NIST RMF.	Open See Finding 3
7.	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.	Open See Finding 5
8.	Review information system accounts in accordance with organization-defined frequency; and the FEC initiates required actions on information system accounts based on the review.	Open See Finding 1
9.	Update the FEC's Segregation of Duties Policy to include defining information system access authorizations to support separation of duties.	Closed
10.	Implement session lockout control in accordance with organization-defined procedures.	Closed

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



FEDERAL ELECTION COMMISSION
Washington, DC 20463

November 16, 2020

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 2020 financial statements. The unmodified opinion that you rendered is reflective of the hard work and continued process improvements made by the FEC staff. The close-out of several recommendations from previous financial statement audits demonstrates significant progress in improving the FEC's IT security posture and resilience. 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 Final Draft Report

The Agency 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

IT Finding 2020-01: Logical Account Management Activities Are Not Consistently Performed for Separated User (Repeat Finding)

Auditor's recommendation: We recommend the FEC OCIO in conjunction with the direct managers perform and document periodic user access reviews for FEC systems according to the agency's system security plan.

Management response:

Management concurs with this recommendation but notes that this finding has no impact on the actual security of FEC systems.

While OCIO has implemented strict account management procedures, it recognizes the need to document these procedures, including periodic user access reviews for 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.

In regard to the three IT user accounts in the GSS that were noted in the audit finding, OCIO wishes to note for the record that these users no longer have network access.

IT Finding 2020-02: Baseline Configuration Standards Are Not Fully Implement for All Windows Devices

Auditor's recommendation: We recommend that the FEC OCIO fully implement STIG baseline configuration standards for Windows devices.

Management response:

Management concurs with the Auditor regarding the full implementation of security technical implementation guide (STIG) baseline configuration standards for Windows 10 devices. In early 2020, the OCIO began distributing Windows 10 laptops then had to suspend temporarily due to the COVID-19 pandemic. As of October 2020, Windows 10 laptop distribution has resumed and DISA STIGs are being tested with an expected implementation date of Spring 2021.

IT Finding 2020-03: Continuity of Operations Plan Is Not Implemented and Tested (Repeat Finding)

Auditor's recommendation: We recommend the FEC OCIO utilize lessons learned from the COVID-19 pandemic to determine if any revisions are need to the *Continuity of Operation Plan*, and schedule periodic testing.

Management Response:

Management concurs with the Auditor's recommendation to use lessons learned from the pandemic and schedule periodic testing.

In 2019, the OCIO awarded a contract for a complete update to the COOP plan. Phase 1 of this update was completed at the end of FY 2020, with the delivery of an updated COOP plan. Mandatory COOP training was also conducted during FY 2020.

Phase II of the implementation of the COOP plan has begun. We will look at the lessons learned during the pandemic and implement them into these updated plans and periodic testing accordingly. The OCIO is actively engaged in reviewing test plans and exercises and anticipates completion of these items by Spring 2021.

Auditor's Recommendation: We recommend that the FEC develop system-specific contingency plans, as appropriate for the agency risk level. (Repeat Recommendation)

Management Response:

Management concurs with the Auditor's recommendation and is actively engaged in Phase II of the COOP Plan to complete information system contingency plans for mission essential functions. Expected completion is September 29, 2021. We believe it is important to note that the worldwide COVID-19 pandemic has demonstrated the FEC's commitment to ensuring its continuity of operations. In March 2020, the agency went into an evacuation order and moved swiftly and successfully to a 100 percent mandatory telework scenario.

IT Finding 2020-04: Security Awareness Training Was Not Completed by All FEC Employees

Auditor's recommendation: We recommend the FEC OCIO implement an effective procedure to enforce compliance with the security awareness training policy to ensure all system users complete security training in accordance with the *FEC Security Training and Awareness Policy*.

Management Response:

Management concurs with this recommendation and is committed to continued education of all staff and contractors in information security awareness. During FY 2020, the OCIO conducted anti-phishing training in April 2020 and began its annual security training during September 2020.

While some users did not complete the required phishing training on time; the OCIO continued to prod users to complete the training. By the end of FY 2020, all staff and contractors had finished the phishing training except for two individuals.

The agency conducted annual password training in September 2020, with a due date of October 21, 2020. Based on lessons learned from the phishing training, OCIO implemented an enforcement mechanism: Users were warned to complete the training by October 21 or have their network access revoked. This newly implemented mechanism proved successful as all active users completed the password training, except for one who has received an exception due to a long-term illness and one contractor on a stop-work order due to the pandemic.

Based on the success of the enforcement mechanism in the September – October 2020 password training, OCIO believes this finding should be closed. Going forward, the OCIO intends to continue to use the penalty of network access revocation combined with intensive outreach efforts to FEC staff and contractors to ensure they are aware of their responsibilities regarding information security and complete all required training

IT Finding 2020-05: Corrective Action Plans Are Not Compliant with Government Requirements (Repeat Finding)

Auditor's Recommendation:

We recommend that the FEC Chief Information Officer improve the plan of action and milestones report for the information system to include:

- Resources required to correct a control deficiency.
- Critical path milestones that affect the overall schedule for implementing the corrective actions are needed to resolve the control deficiency.
- Plan for prompt resolution and internal control testing to validate the correction of the control deficiency.

Management Response:

Management agrees with the Auditor's recommendation to improve the POAM used for documenting and tracking the agency's planned, implemented and evaluated remedial actions to correct deficiencies noted during the assessment of security controls. During FY 2020, the CIO and CISO developed a plan of action and milestones report for information systems and management continued to update and report on corrective action plans in accordance with the timeline identified in Commission Directive 50. OCIO's Security and Operational groups have a weekly meeting to go over vulnerability of GSS systems and prioritize and fix vulnerabilities, with the critical ones fixed first. Detailed POAM sheets are used to document the work of planning, implementing and evaluating actions noted during the assessment of security controls. OCIO's Security and Operational teams are fully committed to reduce or eliminate known vulnerabilities in agency's information systems and will continue to work on including the items noted in the audit findings.