




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 2022 Financial Statement Audit Report

DATE: November 14, 2022

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, 2022. Enclosed you will find the Independent Auditor's final audit report on the FEC (*i.e.*, the "FEC" or "Commission") FY 2022 Financial Statements. The final audit report is additionally included in Section II of the FEC's FY 2022 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. 22-01, *Audit Requirements for Federal Financial Statements*.

In Brown & Company's opinion, the FEC financial statements present fairly, in all material respects, the financial position, net cost, changes in net position, and budgetary resources for the year ending September 30, 2022, in accordance with U.S. generally accepted accounting principles.

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 but did identify three significant deficiencies related to the FEC's IT security internal controls. All four open recommendations from the prior year audit report have been closed. Management was provided a draft copy of the audit report for review and comment. The official management response is included in Exhibit C.

The OIG reviewed Brown & Company's report and related documentation and provided the required oversight throughout the course of the audit. Our review ensures the accuracy of the audit conclusions but may not express an opinion of the results. The OIG's review determined that Brown & Company complied with applicable required Government Auditing Standards.

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 Ms. Shellie Purnell-Brown at (202) 694-1019.

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
Kate Higginbotham, Deputy Staff Director for Management and Administration



**FEDERAL ELECTION COMMISSION
INDEPENDENT AUDITOR'S REPORT
AND
FINANCIAL STATEMENTS
FOR THE YEARS ENDED
SEPTEMBER 30, 2022 AND 2021**



**Prepared By
Brown & Company CPAs and Management Consultants, PLLC
November 14, 2022**



INDEPENDENT AUDITOR'S REPORT

Inspector General
Federal Election Commission
Washington, D.C.

In our audits of the fiscal years 2022 and 2021 financial statements of the Federal Election Commission (FEC), we found:

- FEC's financial statements as of and for the fiscal years ended September 30, 2022, and 2021, are presented fairly, in all material respects, in accordance with United States of America (U.S.) generally accepted accounting principles;
- no material weaknesses in internal control over financial reporting based on the limited procedures we performed;
- no reportable noncompliance with provisions of applicable laws, regulations, contracts, and grant agreements for fiscal year 2022.

The following sections discuss in more detail (1) our report on the financial statements, which includes required supplementary information (RSI)¹ and other information included with the financial statements²; (2) our report on internal control over financial reporting; (3) our report on compliance with laws, regulations, contracts, and grant agreements.

Report on the Financial Statements

Opinion

In accordance with the provisions of the 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, 2022, and 2021; the related statements of net cost, changes in net position, and budgetary resources for the fiscal years then ended; and the related notes to the financial statements. In our opinion, FEC's financial statements present fairly, in all material respects, FEC's financial position as of September 30, 2022, and 2021, and its net costs of operations, changes in net position, and budgetary resources for the fiscal years then ended in accordance with U.S. generally accepted accounting principles.

Basis for Opinion

We conducted our audits in accordance with U.S. generally accepted government auditing standards. Our responsibilities under those standards are further described in the Auditor's Responsibilities for the Audit

¹ The RSI consists of Management's Discussion and Analysis and the Statement of Budgetary Resources, which are included with the financial statements.

² Other information consists of information included with the financial statements, other than the RSI, Financial section, and the auditor's report.

of the Financial Statements section of our report. We are required to be independent of FEC and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements relating to our audit. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Responsibility of Management for the Financial Statements

FEC 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 FEC's agency financial report, and ensuring the consistency of that information with the audited financial statements and the RSI; and (4) designing, implementing, and maintaining effective 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 for the Audit of the Financial Statements

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit of the financial statements conducted in accordance with U.S. generally accepted government auditing standards will always detect a material misstatement or a material weakness when it exists. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control. Misstatements, including omissions, are considered to be material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the financial statements.

In performing an audit in accordance with U.S. generally accepted government auditing standards, we:

- Exercise professional judgment and maintain professional skepticism throughout the audit.
- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, and design and perform audit procedures responsive to those risks. Such procedures include examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements in order to obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion.
- Obtain an understanding of internal control relevant to our audit 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 FEC's internal control over financial reporting. Accordingly, no such opinion is expressed.
- Evaluate the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluate the overall presentation of the financial statements.
- Perform other procedures we consider necessary in the circumstances.

We are required to communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit, significant audit findings, and certain internal control-related matters that we identified during the financial statement audit.

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. Such information is the responsibility of management and, although not a part of the financial statements, is required by FASAB, which considers it 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. Management is responsible for the other information included in FEC's agency financial report. The other information comprises the information included in the annual report but does not include the financial statements and our auditor's report thereon. Our opinion on the financial statements does not cover the other information, and we do not express an opinion or any form of assurance thereon.

In connection with our audit of the financial statements, our responsibility is to read the other information and consider whether a material inconsistency exists between the other information and the financial statements, or the other information otherwise appears to be materially misstated. If, based on the work performed, we conclude that an uncorrected material misstatement of the other information exists, we are required to describe it in our report.

Report on Internal Control over Financial Reporting

In connection with our audits of FEC's financial statements, we considered FEC's internal control over financial reporting, consistent with our auditor's responsibilities discussed below.

Results of Our Consideration of Internal Control over Financial Reporting

Our consideration of internal control was for the limited purpose described below, and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies³ or to express an opinion on the effectiveness of FEC's internal control over financial reporting. Given these limitations, during our audit, we did not identify any deficiencies in internal control over financial reporting

³ 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 over financial reporting, 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 over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

that we consider to be material weaknesses. However, material weaknesses or significant deficiencies may exist that have not been identified.

During our FY 2022 audit, we identified three findings and recommendations related to FEC's internal control over financial reporting which are considered to be significant deficiencies. For more details on these findings and recommendations see below and Exhibit A.

- Finding # 2022-01 FEC Needs to Remediate Critical-Level and High-Level Vulnerabilities
- Finding # 2022-02 FEC Needs to Improve Control over User Account Management
- Finding # 2022-03 FEC Needs to Approve Its Configuration Management Procedures

During our FY 2022 audit, we identified deficiencies in FEC's internal control over financial reporting that we do not consider to be material weaknesses or significant deficiencies. Nonetheless, these deficiencies warrant FEC's management's attention. We communicated these matters to FEC management and, where appropriate, will report on them separately.

Basis for Results of Our Consideration of Internal Control over Financial Reporting

We performed our procedures related to FEC's internal control over financial reporting in accordance with U.S. generally accepted government auditing standards.

Responsibilities of Management for Internal Control over Financial Reporting

FEC management is responsible for designing, implementing, and maintaining effective internal control over financial reporting relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibilities for Internal Control over Financial Reporting

In planning and performing our audit of FEC's financial statements as of and for the fiscal year ended September 30, 2022, in accordance with U.S. generally accepted government auditing standards, we considered FEC's internal control relevant to the financial statement audit 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 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.

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 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 audits of FEC's financial statements, we tested compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements consistent with our auditor's responsibilities discussed below.

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 fiscal year 2022 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.

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

We performed our tests of compliance in accordance with U.S. generally accepted government auditing standards. Our responsibilities under those standards are further described in the Auditor's Responsibilities for Tests of Compliance section below.

Responsibilities of Management for Compliance with Laws, Regulations, Contracts, and Grant Agreements

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

Auditor's Responsibilities for Tests of Compliance with Laws, Regulations, Contracts, and Grant Agreements

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 to perform certain other limited procedures. Accordingly, we did not test compliance with all laws, regulations, contracts, and grant agreements applicable to FEC. We caution that noncompliance may occur and not be detected by these tests.

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 2021 Independent Auditor's Report, dated November 12, 2021, and all prior year recommendations were closed. Details 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.

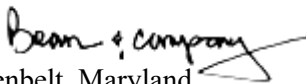

Greenbelt, Maryland
November 14, 2022

Exhibit A - Significant Deficiencies
Effectiveness of Information System Controls Over Financial Reporting
Findings and Recommendations

IT Finding # 2022-01: FEC Needs to Remediate Critical-Level and High-Level Vulnerabilities

Condition:

Brown and Company examined the FEC Office of Chief Information Officer (OCIO) Plan of Action and Milestone (POA&M) report dated September 7, 2022 and noted critical-level and high-level vulnerabilities were not remediated within the timeframe required by the FEC OCIO System Security Plan (SSP).

The FEC OCIO PO&AM showed 24 out of 47, or 49% critical-level vulnerabilities, and 43 out of 70 or 39% high-level vulnerabilities were closed in FY 22. However, 23 (51%) critical-level (ranging from 278 to 478 days outstanding) and 27 (61%) high-level (ranging from 278 to 538 days outstanding) vulnerabilities remain open past the FEC requirements. See Table-1 Vulnerability Table below.

Specifically, critical-level and high-level vulnerabilities were not timely resolved for Window STIG baseline, McAfee Antivirus detection software, unsupported software, and missing patches.

Table -1 Vulnerability Table

Vulnerabilities	Total	Open	Closed
Critical-level	47	23	24
High-level	70	27	43

Criteria:

NIST SP 800-53, Revision 5.1, *Security and Privacy Controls for Information Systems and Organization*, states the following:

“RA-5 VULNERABILITY MONITORING AND SCANNING

- a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization- defined process] and when new vulnerabilities potentially affecting the system are identified and reported;
- b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
 - 1. Enumerating platforms, software flaws, and improper configurations;
 - 2. Formatting checklists and test procedures; and
 - 3. Measuring vulnerability impact.
- c. Analyze vulnerability scan reports and results from vulnerability monitoring;
- d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;
- e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and

- f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.”

“SI-2 FLAW REMEDIATION

- a. Identify, report, and correct system flaws;
- b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
- c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and
- d. Incorporate flaw remediation into the organizational configuration management process.”

FEC OCIO FECLAN System Security Plan (SSP):

“The FEC OCIO FECLAN SSP requires staff to remediate vulnerabilities within 30 days for critical-level risk, 45 days for high-level risk, 90 days for medium-level risk, and 180-days for low-level risk.”

Cause:

FEC OCIO runs vulnerability scans weekly and monthly for its network and applications; however, flaw remediation controls were not consistently implemented to remediate known vulnerabilities due to a lack of resources and outdated equipment.

Effect:

Unmitigated vulnerabilities on FEC’s network can compromise the confidentiality, integrity, and availability of the FEC data. For example:

- An attacker may leverage known issues to execute arbitrary code.
- Foundation employees may be unable to access systems.
- Foundation data may be compromised.

Recommendation 1:

We recommend FEC OCIO remediate critical-level and high-level vulnerabilities according to the FEC System Security Plan.

IT Finding # 2022-02: FEC Needs to Improve Control over User Account Management Condition:

During FY 2022, the FEC management did not disable user accounts timely for separated employees in accordance with the agency’s account management policy and procedures.

On August 1 2022, FEC management recertified user accounts for the US Bank Purchase Card system. FEC’s recertification schedule identified two separated users who were removed from the US Bank Purchase Card system but not disabled in the FEC Microsoft Active Directory system. These two users separated from FEC in 2020, but access accounts were not deactivated until 2022.

Table 1 lists the two separated users’ names, separation dates, and deactivation dates in the FEC Microsoft Active Directory.

User Name	Separation Date	Deactivation Date
Carmen Robinson	10/29/2020	9/23/2022
Shayla Walker	4/15/2020	9/23/2022

Criteria:

NIST Special Publication (SP) 800-53, Revision 5.1 (Rev. 4), *Security and Privacy Controls for 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];”

FEC Account Management Policy, states:

“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 implemented sufficient account management controls to ensure separated employee user accounts are deactivated timely in accordance with the agency’s policy.

Effect:

FEC’s Microsoft Active Directory user accounts allow users to log on and access the FEC network resources. By not disabling the user accounts according to the agency’s account management policy and procedures, there is an increased risk a user could gain or retain unauthorized access and/or perform unauthorized functions and transactions within FEC systems.

Recommendation 2:

We recommend the FEC OCIO establish controls to ensure user accounts are deactivated timely when employees separate from the agency.

IT Finding #2022-03: FEC Needs to Approve Its Configuration Management Procedures

Condition:

The FEC OCIO Configuration Management Policy requires management to identify, document, and obtain approval of any deviations from established configuration settings for all components based on FEC policies and procedures. The FEC has established configuration settings for its laptops using Windows 10 Security Technical Implementation Guide (STIG). However, FEC OCIO failed to obtain written approval for the deviations implemented for Windows 10 laptops as required by FEC’s policy.

The FEC OCIO Security Content Automation Protocol (SCAP) Compliance Checker Report (dated July 14, 2022) showed that FEC OCIO implemented 191 (91%) out of 210 STIG configuration settings recommended for Windows 10 devices. Four of the 19 non-compliant settings were not implemented, and fifteen were compensating controls that deviated from STIG. Table 2 summarizes the FEC OCIO status of the 19 non-compliance STIG settings.

Table 2 – Window laptop non-compliance STIG settings

Windows 10 Security Technical Implementation Guide (STIG). Status of the non-compliant security controls.	Number of non-compliant security controls
Control was not implemented; FEC OCIO noted a compensating control was implemented to meet the security standards	15
Control was not implemented: FEC OCIO noted controls are currently being tested	2
Control was not implemented: FEC OCIO noted the control is being tested in its development environment	1
Control was not implemented: FEC OCIO did not provide explanation	1
Total non-compliant security controls	19

Criteria:

NIST Special Publication (SP) 800-53, Revision 5.1, *Security and Privacy Controls for Information Systems and Organizations*, Security Control CM-6 Configuration Settings, states the following:

“Control: The organization:

- a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];
- b. Implement the configuration settings;
- c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and
- d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.”

NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, states the following:

“Develop Organizational SecCM Procedures

...

Common Secure Configurations –Deviations from the common secure configurations are also addressed (e.g., identification of acceptable methods for assessing, approving, documenting, and justifying deviations to common secure configurations, along with identification of controls implemented to mitigate risk from the deviations), in the event that the configuration for a given system must diverge from the defined configuration due to mission requirements or other constraints

...”

FEC Office Of Chief Information Officer (OCIO), FECLAN System Security Plan (SSP), requires

FEC OCIO staff to identify, document, and obtain approval of any deviations from established configuration settings for all components based on FEC policies and procedures.

Cause:

FEC management does not formally document the control procedure for identifying and obtaining approval for deviations from established configuration settings.

Effect:

Implementing configuration setting deviations not approved by management increases the risk of introducing functional problems within the agency's network. For example, a deviated configuration setting may close a port or stop a service that is needed for an operating system or application functionality.

Recommendation 3:

We recommend the FEC OCIO document and maintain evidence that the controls for identifying and obtaining management's approval for deviations from its established configuration settings for Windows 10 devices is performed on a consistent basis.

Exhibit B – Status of Prior Year’s Finding and Recommendations

Status of FY 2021 Prior Year’s Audit Recommendations	Status as of September 30, 2022
2020-01 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.	Closed
2020-03: 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.	Closed
2020-04: We recommend that the FEC develop system- specific contingency plans, as appropriate for the agency risk level. (Repeat Recommendation)	Closed
2020-05: 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 <i>Security Training and Awareness Policy</i> .	Closed

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



THE FEDERAL ELECTION COMMISSION
Washington, DC 20463

November 14, 2022

On behalf of the Federal Election Commission (FEC) Management, I would like to thank the FEC Office of Inspector General and Brown and Company for their diligent work auditing the FEC's FY 2022 financial statements. The unmodified opinion that you rendered is reflective of the hard work and continued process improvements made by the FEC staff.

On Behalf of Management,

John Quinlan

John Quinlan
Chief Financial Officer

IT Finding # 2022-01 FEC Needs to Remediate Critical-Level and High-Level Vulnerabilities.

Recommendation #1:

We recommend FEC OCIO remediate critical-level and high-level vulnerabilities according to the FEC System Security Plan.

Management Response:

- Management concurs with this finding.
 Management does not concur with this finding.

Management's Response:

OCIO acknowledges the vulnerabilities shown in the plan of actions and milestones report as submitted to the auditors exist and that they have yet to be remediated but should be as soon as possible. OCIO has a plan to remediate most of these in place now; however, budgetary constraints have limited our ability to put that plan into action until recently. In the case of vulnerabilities affecting legacy application servers, OCIO has put compensating controls into place when it cannot replace the server.

In many cases, these outstanding items relate to Windows settings on 45 older laptops that are too old to accept the patches rolled out to remediate those vulnerabilities. This means that to remediate the vulnerabilities, OCIO will need to replace those laptops. Unfortunately, although OCIO has requested funding for replacement equipment for the past few fiscal years, it has not been available due to other budgetary priorities for the agency. This year, end-of-year funds became available and OCIO completed the procurement process to obtain the replacement laptops. A contract to supply the laptops was awarded in September 2022 and the new laptops were received in late October 2022. Currently, OCIO is working on configuring the new laptops to include the needed patches and upgrades that will remediate those vulnerabilities.

In the case of several Apache Tomcat servers with vulnerabilities, these servers relate to mission-critical legacy applications. Should OCIO put remediations in place, it may render those applications unusable and cause agency staff to be unable to accomplish their duties and mission. Instead, OCIO's SecOps team has put into place compensating controls using the CrowdStrike Endpoint Detection and Response and McAfee applications. Those applications help protect the agency from cybersecurity intrusions.

IT Finding 2022-02: FEC Needs to Improve Control over User Account Management

Recommendation #2:

We recommend the FEC OCIO establish controls to ensure user accounts are deactivated timely when employees separate from the agency.

Management Response:

- Management concurs with this finding.
 Management does not concur with this finding.

Management’s Response:

OCIO agrees that it is essential to disable user accounts of separating employees on the final day of their employment with the FEC. Thus, it has established controls and a workflow via the FEC’s Federal Systems Access (FSA) process to ensure user accounts are deactivated timely when employees separate. OCIO strives to ensure that accounts are de-activated as soon as the employee separation request is input by OHR and received by OCIO in FSA, but no later than 8 p.m. of the day of the employee’s separation.

In the case of the two employees who separated in 2020, a revised version of the FSA system was in the development stage and an anomaly in the FSA system failed to trigger the notification to OCIO that the two accounts needed de-activation. That bug has since been fixed and no longer occurs. When these two employees’ accounts were brought to OCIO’s attention, OCIO worked with OHR to determine if their separation requests had been submitted. OHR provided documentation that FSA separation requests had been timely submitted. OCIO quickly took action to disable their accounts and doublechecked the list of FEC Active Directory users to ensure no other separated employees were similarly impacted.

Going forward, OCIO believes the combination of the annual recertification by business owners of the users for financial systems coupled with regular review of the active system users along with the current controls and workflow will help ensure that user accounts are timely de-activated when an employee separates from the agency.

IT Finding # 2022-03 FEC Needs to Approve Its Configuration Management Procedures

Recommendation #3:

We recommend the FEC OCIO document and maintain evidence that the controls for identifying and obtaining management's approval for deviations from its established configuration settings for Windows 10 devices is performed on a consistent basis.

Management Response:

- Management concurs with this finding.
- Management does not concur with this finding.

If you disagree, please provide comment:

Management response:

OCIO currently identifies, documents and obtains management’s approval of deviations from established settings in a risk acceptance spreadsheet. The documentation includes descriptions of the deviation, the justification for risk acceptance and the applicable compensating controls. OCIO agrees with the auditors that the documentation is improved by adding columns for “Approved By” and “Approval Date” to the spreadsheet to indicate the approving manager and the date the approval was given. In response to the NFR, OCIO updated its spreadsheet to add those columns and provided that documentation to the auditors.