PERFORMANCE AUDIT REPORT

FEDERAL ELECTION COMMISSION'S SECURITY PATCHES AND VULNERABILITIES MANAGEMENT PROGRAMS FOR THE FISCAL YEAR ENDING SEPTEMBER 30, 2024

June 30, 2025

Prepared by:
Brown & Company Certified Public Accountants and Management Consultants, PLLC
6401 Golden Triangle Drive, Suite 310
Greenbelt, Maryland 20770

BROWN & COMPANY
CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS, PLLC

June 30, 2025

[redacted], CPA, CFE
Senior Auditor
Federal Election Commission
Office of the Inspector General
1050 First Street, NE
Washington, DC 20463

Dear [redacted]:

Subject: Performance Audit of the Federal Election Commission's (FEC) Security Patches and Vulnerabilities Management Programs for Fiscal Year 2024

Brown & Company CPAs and Management Consultants, PLLC is pleased to submit the attached audit report detailing the results of our performance audit of the Federal Election Commission's Security Patches and Vulnerabilities Management Programs for Fiscal Year 2024.

We performed our work from September 30, 2024, through May 9, 2025, covering the fiscal year 2024 from October 1, 2023, through September 30, 2024. We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), issued by the Comptroller General of the United States. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our conclusion based on our audit objectives. Our objectives, scope, and methodology are described further in the report sections titled "Objectives, Scope, and Methodology."

We appreciate the assistance provided by the FEC Office of Inspector General, FEC's management and staff.

Brown & Company
Greenbelt, Maryland
June 30, 2025

6401 GOLDEN TRIANGLE DRIVE, SUITE 310 • GREENBELT, MD 20770
PHONE: (240) 770-4900 • FAX: (301) 773-2090 • mail@browncо-cpas.com • www.browncо-cpas.com

PERFORMANCE AUDIT REPORT

Federal Election Commission's Security Patches And Vulnerabilities Management Programs For The Fiscal Year Ending September 30, 2024

TABLE OF CONTENTS

INDEPENDENT AUDITORS' PERFORMANCE AUDIT REPORT

Federal Election Commission's Security Patches And Vulnerabilities Management Programs For The Fiscal Year Ending September 30, 2024

Susan Ruge-Hudson
Inspector General
Federal Election Commission

This report presents the results of our Independent Auditors' Performance Audit Report on the Federal Election Commission's (FEC) Security Patches and Vulnerabilities Management Programs for the Fiscal Year Ending September 30, 2024. The FEC Office of the Inspector General (OIG) contracted with Brown & Company CPAs and Management Consultants, PLLC (Brown & Company) to conduct a performance audit of FEC's Security Patches and Vulnerabilities Management Programs for the Fiscal Year Ending September 30, 2024.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objective of this performance audit was to assess the operating effectiveness of the FEC's Security Patches and Vulnerabilities Management Programs for the Fiscal Year Ending September 30, 2024. Overall, we found that the FEC Office of Chief Information Officer (OCIO) has established, maintained, and implemented policies and procedures for its information systems security programs that are generally effective and comply with the applicable Office of Management and Budget (OMB) requirements and National Institute of Standards and Technology (NIST) standards and guidelines.

However, we determined that while system security controls in place are working as intended, they are not sufficient to reduce the risk of potential security breaches to an acceptable level. This is partially due to the FEC's reliance on legacy systems that prevents the agency from patching known vulnerabilities in a timely manner[1]. Moreover, we also noted, through inquiry, that the FEC has had significant budget and resource constraints for several years that have contributed to its inability to remediate vulnerabilities and patches related to legacy systems and outdated equipment. Based on the agency's risk-based approach to system security, there are instances that justify the decisions not to implement all the standard government-wide system controls outlined in related OMB information system policy and guidance.

[1] This is a repeat finding from prior Annual Financial Statement Audits.

6401 GOLDEN TRIANGLE DRIVE, SUITE 310 • GREENBELT, MD 20770
PHONE: (240) 770-4900 • FAX: (301) 773-2090 • mail@brownco-cpas.com • www.brownco-cpas.com

This report identifies eight significant findings and ten recommendations to improve the FEC Security Patches and Vulnerabilities Management Programs. Our recommendations are as follows:

1. Update the System Security and Privacy Plans (SSPP) and establish a privacy program plan.
2. Develop and implement Supply Chain Risk Management (SCRM) strategy, policies, and procedures.
3. Secure and monitor Security Technical Implementation Guide (STIG) security configuration settings for [redacted] application.
4. Review and monitor STIG security configuration settings for its network server.
5. Implement STIG security configuration settings for its [redacted] server (Server 1).
6. Scan Server 1 regularly to verify compliance with STIG security configuration settings.
7. Reassess and reprioritize resources to identify opportunities to accelerate the remediation of urgent, critical, and high vulnerabilities.
8. Regularly conduct risk assessments in accordance with OMB Circular A-130, *Managing Information as a Strategic Resource,* to help identify other corrective actions to improve the timeliness of vulnerability remediation.
9. Develop and implement Service Level Agreements (SLA) policy and procedures and define Key Performance Measurements (KPM) for third-party service contracts.
10. Forward [redacted] logs to the agency's centralized Security Information and Event Management (SIEM) system.

Addressing our significant findings and implementing our recommendations will strengthen the FEC's Security Patches and Vulnerabilities Management Programs and contribute to ongoing efforts to maintain reasonable assurance of adequate security over information systems.

In accordance with GAGAS, we have also issued a separate Management Letter that communicates less significant matters and opportunities for improvement that do not rise to the level of a significant deficiency but are nonetheless important for management's consideration.

This report is for the purpose of concluding on the audit objective described above. Accordingly, this report is not suitable for any other purpose. We appreciate the cooperation and courtesies that FEC personnel extended to us during the execution of this performance audit.

Agency Comments

We provided the FEC with a Draft of our report on May 27, 2025, and received the FEC's response on June 9, 2025. The FEC's response to our report was not subjected to the auditing procedures that we applied to our audit and, therefore, we express no opinion on the response.

Brown & Company

Greenbelt, Maryland
June 30 2025

BACKGROUND

The Federal Election Commission (FEC or Commission) is the independent regulatory agency charged with administering, enforcing, defending and interpreting the *Federal Election Campaign Act of 1971* ("FECA" or the "Act"), as amended. The FEC's mission is to protect the integrity of the federal campaign finance process by ensuring the public has access to information about the sources of financial support for federal candidates, political party committees, and other political committees.

The FEC Office of the Chief Information Officer (OCIO) is responsible for providing the FEC with the information technology (IT) support necessary to administer and enforce the campaign finance laws. Its mission is to ensure that agency personnel, end users, and the public are supported by a stable and strong technological infrastructure that enables the effective performance of daily responsibilities.

The agency's overall IT infrastructure is comprised of two main parts: (1) the agency's headquarters data center, the FEC Local Area Network (FECLAN), and (2) the FEC Cloud Infrastructure (FECCI). The agency has procured additional cloud infrastructure for specific services, such as the [redacted] server (Server 2), which is discussed later in the report.[2] Most of the FEC's legacy systems (as discussed in more detail below) are in the FECCI, but some are still located in FECLAN.

Both FECLAN and FECCI provide critical IT infrastructure services, including network management, authentication, data storage, and system and application hosting in accordance with Office of Management and Budget (OMB) guidelines. These services support the security and operation of mission-critical applications.

In April 2024, the agency experienced a security incident that impacted several information systems and ultimately forced the decommissioning of the agency's [redacted].[3] In response to both this event and the results from the Office of the Inspector General (OIG)'s annual risk assessment, the FEC OIG contracted with Brown & Company to conduct an audit of the agency's Security Patches and Vulnerabilities Management Programs.

The primary objective of this audit is to assess the operating effectiveness of FEC's Security Patches and Vulnerabilities Management Programs. Our audit engagement focused on the FEC'S OCIO policies and procedures that support FEC's Security Patches and Vulnerabilities Management Programs.

[2] We note that the FEC also contracts with outside vendors that use a cloud-based infrastructure, and which can interact with FECCI. Each of those vendors is solely responsible for security of that particular infrastructure, which means such infrastructure is outside the scope of this audit.

[3] [redacted].

Legacy Systems

The agency relies on legacy systems that contain over 20 applications to support its core mission-critical work and daily operations. These applications were developed over several decades and are hosted on an aging infrastructure. According to the FEC OCIO, many of the security vulnerabilities identified in recent assessments are associated with outdated equipment and the legacy systems. The FEC OCIO has noted that applying the latest patches or upgrading operating systems presents a risk of disrupting application functionality, as these systems were not designed to operate in modern IT environments. To address these challenges, the FEC OCIO has developed a "replacement feasibility plan" as of September 2024, to replace the applications that are components of the legacy systems. However, budgetary constraints have prevented the OCIO from fully implementing their action plan, which further complicates its ability to maintain or secure the legacy systems effectively.

OMB Guidance

OMB Circular A-130, *Managing Information as a Strategic Resource* (dated July 28, 2016), requires federal agencies to establish and employ a formal, risk-based process for selecting and implementing security controls for information systems and their operating environments. This process must meet the minimum information security requirements outlined in FIPS Publication 200[4] and align with the security control baselines in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53,[5] appropriately tailored to the agency's mission, operational contexts, and risk levels.

The FEC has categorized both its FECLAN and FECCI as moderate-impact systems based on NIST guidelines and has applied the FIPS Publication 200 information security controls, as applicable. OMB Circular A-130 also requires federal agencies, including the FEC, to establish and maintain a comprehensive privacy program that ensures compliance with applicable privacy requirements, develops and evaluates privacy policy, and manages privacy risks.[6]

[4] Federal Information Processing Standards (FIPS) Publication 200 *Minimum Security Requirements for Federal information and Information Systems*.
[5] NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations.*
[6] OMB Circular A-130 states that its requirements apply to the information resources management activities of all agencies of the Executive Branch of the federal government. Footnote 2 of the document states, "'Agency' means any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency".

AUDIT RESULTS

As part of this audit, we reviewed selected information system security controls[7] for the FECLAN and reviewed the System Security and Privacy Plans (SSPP) for the FECCI. Overall, the FEC OCIO has established policies and procedures for its security patches and vulnerabilities management programs, and most of the selected security controls were implemented effectively. However, our examination identified areas where significant improvements are needed to enhance the agency's overall security posture. These findings and our related recommendations are presented in the Audit Findings and Recommendations section of this report.

Also, during the engagement, we assessed the efficiency and effectiveness of the IT patching process by examining the following questions:

1. Are vulnerabilities patched per the FEC patch management policy?

   Auditor's Conclusion: The FEC OCIO has not consistently patched vulnerabilities in accordance with the timelines and procedures outline in the agency's System Security Plan (SSP), indicating noncompliance with established patch management policy requirements. See Recommendations 7 and 8 in the Audit Findings and Recommendations section below.

2. Are key performance indicators (KPIs)[8] for patch management kept for all FEC IT systems, both internal and external, and are those measurements accurate and adequate?

   Auditor's Conclusion: The FEC OCIO utilizes patch management and vulnerability tools that automatically discover devices connected to the FEC's network and track KPIs, including the number of patches applied and pending, vulnerabilities resolved and un-remediated, and vulnerabilities categorized by severity and risk level. However, we were unable to determine whether these measurements are accurate and adequate because the agency has not established requirements to document or implement information security performance measures in accordance with NIST SP 800-53, nor has it included comprehensive service level agreements (SLAs) with provisions to track key KPIs in its third-party contracts. See Recommendations 1 and 9 below.

3. What is the average cost of addressing patch vulnerabilities?

   Auditor's Conclusion: We were not able to calculate the average cost for patching individual vulnerabilities. We were, however, able to calculate the FEC OCIO's estimated direct cost for managing its Security Patches and

[7] Selected information system security controls are from the NIST SP 800-40, Rev.4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, Appendix A, April 2022. Selected controls include CM-2, Baseline Configuration, CM-3, Configuration Change Control, CM-8, System Component Inventory, RA-7, Risk Response, SI-2, Flaw Remediation, SR-2, Supply Chain Risk Management Plan, SR-3, Supply Chain Controls and Processes, SR-5, Acquisition Strategies, Tools, and Methods. Also, included are related security controls from the NIST Cybersecurity Framework.

[8] KPIs are quantifiable measures used to evaluate the effectiveness, efficiency, and success of an organization's processes or activities. In the context of patch management, KPIs may include metrics such as patch deployment timelines, compliance rates, and vulnerability remediation performance.

Vulnerabilities Management Programs for the Fiscal Year ending 2024, which was $817,439. For more details see Table 1, Estimated Direct Cost of Addressing Patches and Vulnerabilities.

Also, we calculated the estimated direct cost for the modernization project aimed at upgrading the legacy platform, which supports over 20 applications, for the Fiscal Year ending 2024, to be $3,980,073.

Table 1. Estimated Direct Cost of Addressing Patches and Vulnerabilities

Categories	Vulnerability Management	Patch Deployment	Total
Personnel Labor: The cost is based on the estimated labor hours required to implement system changes as documented in FEC OCIO's change request tickets submitted during fiscal year 2024.	$ 0	$ 44,011	$ 44,011
Technologies: The cost is based on the tools utilized by FEC OCIO for patches and vulnerabilities management, security monitoring, and patch testing and deployment activities.	$ 295,920	$ 66,158	$ 362,078
External Service Providers: The cost is based on third-party service support contracts that provide vulnerability management services.	$ 411,350	$ -	$ 411,350
Total Estimated Direct Cost	**$ 707,270**	**$ 110,169**	**$ 817,439**

4. Are patching efficiencies addressed in the agency's most significant IT contracts and SLA, and is the agency receiving the contract deliverables, or are the contractors patching the systems as required?

   Auditor's Conclusion: We reviewed the statement of work for the FEC's third-party Vulnerability Management (Patch Management) support services. The contract requires the contractor to monitor, prioritize, test, deploy, and verify vulnerability remediation, as well as provide administrator training. However, the contract does not include a comprehensive SLA and KPM to assess and monitor contractor performance. As a result, we were unable to determine whether patching efficiencies are being achieved, whether contractor deliverables are being met, or whether contractors are fulfilling patching requirements as intended. See Recommendation 9 in the Audit Findings and Recommendations section below.

5. Are FEC personnel and contractors performing secure baseline consistently, and what is the frequency?

   Auditor's Conclusion: Secure baseline performance refers to the establishment, documentation, and consistent application of standardized security configuration settings across IT assets, such as servers [redacted].

Our review found that the FEC OCIO is not consistently maintaining these security configuration baselines for its network servers [redacted], as required by the agency's SSP. The SSP requires annual reviews and updates, as well as updates following significant changes, including the installation or upgrade of information system components. Inconsistent application of secure baselines increases the risk of misconfigurations and security vulnerabilities See Recommendations 3, 4, 5 and 6 in the Audit Findings and Recommendations section below.

6. Does the FEC have sufficient personnel to accomplish critical system management and security?

   Auditor's Conclusion: Based on inquiries with the FEC OCIO personnel, we found that the agency does not currently have sufficient staffing levels to effectively manage its critical systems and associated security controls. This staffing shortfall would likely impact the agency's ability to consistently implement and monitor essential cybersecurity functions and operational requirements. See Recommendations 1, 2, 3, and 4 in the Audit Findings and Recommendations section below.

7. Are platforms and processes exhibiting fully compliant/effective vulnerability patching? If so, are there distinguishing characteristics contributing to this success?

   Auditor's Conclusion: The FEC's Security Patches and Vulnerabilities Management Programs processes align with applicable OMB Circular A-130 policy and NIST SP 800-53 standards and guidelines. While some legacy systems within the FEC environment remain noncompliant due to platform limitations or lack of vendor support, the OCIO has implemented a comprehensive suite of tools and processes that support vulnerability and patch management for compliant systems. The agency utilizes a range of technologies—including patch deployment tools, ticketing and incident tracking systems, vulnerability and endpoint management solutions, antivirus and forensic tools, firewalls, data-loss prevention technologies, database security controls, network monitoring tools, and configuration management solutions—to monitor, prioritize, and address security vulnerabilities.

   These tools and processes contribute significantly to the effectiveness of the agency's Security Patches and Vulnerabilities Management Programs across supported platforms. However, the presence of unsupported or legacy systems introduces ongoing risk and requires targeted mitigation strategies until full remediation or system replacement can occur. See Recommendations 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10 in the Audit Findings and Recommendations section.

While we found the selected information system security controls to be generally effective and operating as intended, we identified eight findings and made ten recommendations to help the FEC strengthen its Security Patches and Vulnerabilities Management Programs. Specifically, we recommend that the FEC OCIO:

1. Update the FEC's System Security and Privacy Plans (SSPPs) and establish a privacy program plan.
2. Develop and implement a Supply Chain Risk Management (SCRM) strategy, policies, and procedures.
3. Secure [redacted] by monitoring configuration settings to ensure compliance with Security Technical Implementation Guide (STIG) security configuration settings.
4. Review and monitor STIG security configuration settings for its network server.
5. Implement STIG security configuration settings for its Server 1.
6. Scan its Server 1 regularly to verify compliance with STIG security configuration settings.
7. Reassess and reprioritize resources to identify opportunities to accelerate the remediation of urgent, critical, and high vulnerabilities.
8. Regularly conduct risk assessments in accordance with OMB Circular A-130, *Managing Information as a Strategic Resource,* to help identify other corrective actions to improve the timeliness of vulnerability remediation.
9. Develop and implement Service Level Agreements (SLA) policy and procedures and define Key Performance Measurements (KPM) for managing the performance of third-party service contracts.
10. Ensure [redacted] logs are forwarded to and actively monitored by the agency's centralized Security Information and Event Management (SIEM) system. (We note that this recommendation was immediately implemented when it was brought to management's attention.)

Detailed audit findings and recommendations are presented in the following section.

AUDIT FINDINGS AND RECOMMENDATIONS

Finding 1: The FEC OCIO Did Not Update System Security and Privacy Plans (SSPPs).

Condition

The OCIO categorized the FEC FECLAN and FECCI systems as moderate-impact systems[9] in their respective system security documentation. We reviewed the FECLAN SSP, dated April 6, 2022, and the FECCI SSPP, dated May 3, 2024, and found that neither document was fully updated to reflect the required security controls for systems categorized at the moderate-impact level. Specifically, three controls were still based on the previous version of NIST SP 800- 53 Revision (Rev.) 4, rather than the current Rev. 5.1.1, and two required controls were not documented at all. We identified the following issues:

List of Moderate-Impact Controls Not Updated or Documented

Controls based on NIST SP 800-53 Rev.4 (not updated to Rev 5.1.1):

1. CA-02 Security Assessments (FECLAN)
2. PL-02 System Security and Privacy Plans (FECLAN)
3. SA-04: Acquisition Process (FECLAN)

Controls from NIST SP 800-53 Rev. 5.1.1 not documented:

1. RA-7: Risk Response (FECLAN and FECCI)
2. RA-09: Criticality Analysis (FECLAN and FECCI)

Updating these controls is essential to align with evolving federal cybersecurity standards and to incorporate lessons learned from emerging threats, technologies, and risk management practices. Failure to update and properly document these controls can result in incomplete or outdated security postures, leaving critical systems vulnerable to exploitation. For example:

- CA-02 (Security Assessments): This control ensures periodic evaluations of security controls are conducted and updated based on current risks. Without timely updates, management cannot reliably assess whether the system's security controls remain effective.
- PL-02 (System Security and Privacy Plans): This control provides the foundation for defining the system's overall security strategy. Outdated plans limit visibility into implemented safeguards and hinder informed, risk-based decision-making.
- RA-07 (Risk Response) and RA-09 (Criticality Analysis): These controls are part of the updated risk management controls that help agencies prioritize and respond to threats based on mission and business impact. Not documenting these controls limits the agency's ability to proactively manage risk and protect high-value assets.

[9] A moderate-impact system refers to an information system that, if compromised in terms of confidentiality, integrity, or availability, would have a serious adverse effect on an agency's operations, assets, or individuals. This designation is based on the FIPS Publication 199, which categorizes systems according to the potential impact of a security breach. Moderate-impact systems require appropriate security controls as outlined in NIST SP 800-53 to mitigate associated risks

- SA-04 (Acquisition Process): The control addresses requirements for standardized contract language such as descriptions, and criteria, explicitly or by reference, in the acquisition contract for the system, system component, or system service.

Also, the FEC OCIO has not established an organizational-wide Privacy Program Plan to address the privacy-related controls within the Program Management (PM) control family. These controls, which became effective with the release of Rev. 5 in September 2020 and were further updated in Rev. 5.1.1, are designed to ensure that privacy risks are proactively managed at the organizational level and integrated into agency-wide governance structures. The absence of documentation for these controls indicates that the FEC has not yet fully aligned its privacy program with current federal guidance.

List of Privacy Management Controls Not Documented

Controls Privacy Controls from NIST SP 800-53 Rev. 5.1.1 are not documented:

1. PM-06: Information Security Measures of Performance
2. PM-08 Critical Infrastructure Plan
3. PM-09 Risk Management Strategy
4. PM-11 Mission/Business Process Definition
5. PM-18 Privacy Program Plan
6. PM-19: Privacy Program Plan
7. PM-28: Risk Framing
8. PM-31: Continuous Monitoring Strategy

Criteria

The FEC OCIO's SSP documentation states that SSPs be reviewed "at least annually or when a major change occurs." This internal requirement aligns with federal guidance from OMB Circular A-130. The OMB Circular A-130 requires agencies to establish and maintain a comprehensive privacy program that ensures compliance with applicable privacy requirements, supports privacy policy development, and effectively manages privacy risks. The Circular further mandates that agencies select and implement security controls consistent with FIPS Publication 200 and the NIST SP 800-53 security control baselines, tailored as appropriate.

NIST SP 800-53, Rev. 5.1.1, outlines detailed requirements for System Security and Privacy Plans, including documenting the system's components, operational context, security categorization, applicable threats, and privacy risks. Plans must also describe the security and privacy controls implemented, identify key personnel roles, include risk determinations, and be reviewed and approved by an authorizing official.

Cause

In response to the auditor's inquiry, FEC OCIO management explained that they did not have sufficient resources or staffing capacity to update the agency's SSPPs and establish a privacy program plan that aligned with NIST SP 800-53, Rev. 5.1.1 requirements.

Effect

The lack of controls to update the SSPPs and privacy program plan increases the risk that the FEC may not be implementing safeguarding measures and privacy controls to protect the agency's operations, assets, and individuals' privacy.

The lack of documentation and implementation of the privacy control limits the FEC's ability to effectively govern privacy risk, demonstrate compliance with federal privacy requirements, and integrate privacy consideration into enterprise risk management and strategic planning.

Recommendation 1:

We recommend that the FEC OCIO update the agency's SSPP documents and establish a privacy program plan that aligns with NIST SP 800-53, Rev.5.1.1 requirements as required by OMB.

Management's Response:

The FEC OCIO management concurs with the recommendation to update the SSPP. They stated that updates are currently underway following the recent migration to the FECCI, with corresponding updates to the FECLAN forthcoming. However, progress is hindered by limited cybersecurity staffing due to an ongoing hiring freeze. Regarding the agency's privacy program, management noted that while FEC is not subject to FISMA requirements due to statutory exemptions, it maintains a formal privacy policy and a dedicated Privacy Office responsible for oversight and compliance. Furthermore, management emphasized that FEC has voluntarily adopted the NIST Risk Management Framework for key systems and remains committed to enhancing its privacy program within existing resource constraints. Management's full response is provided in Appendix I.

Auditor's Evaluation of Management's Response:

The management's response is generally responsive to the recommendation. The ongoing efforts to update SSPP documentation and the commitment to a formal privacy program are noted. The auditors acknowledge the agency's voluntary alignment with NIST best practices as a constructive measure. Nonetheless, staffing limitations may delay the completion and full implementation of these updates, and the auditors encourage management to explore interim solutions to mitigate the impact of resource constraints.

Finding 2: The FEC OCIO Has Not Developed and Implemented Supply Chain Risk Management (SCRM) Strategy, Policies, and Procedures.

Condition

Our examination of the FEC OCIO's information security policies and procedures revealed that the FEC OCIO has not developed and implemented a SCRM strategy, policies, and procedures to manage supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, components, and system services as required by OMB and NIST requirements. Managing supply chain risks is important because it helps organizations manage the complexities of modern supply chains, ensuring stability and continuity and reducing the

likelihood of costly disruptions. Additionally, the agency has not conducted a supplier chain risk assessment. Conducting such an assessment is critical to identifying potential threats posed by suppliers, assessing the trustworthiness of third parties, and enabling informed procurement and risk mitigation decisions.

Criteria

OMB Circular A-130 requires all agencies to "[i]mplement supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development lifecycle". It also requires agencies to develop supply chain risk management plans as described in NIST SP 800-161, in addition to meeting the security control requirements of FIPS Publication 200 and the security baselines in NIST SP 800-53 (tailored as appropriate), as discussed in Finding 1 above.

NIST SP 800-161 provides guidance on identifying, assessing, and responding to cybersecurity risks throughout the supply chain at all levels of an organization. Additionally, NIST SP 800-53, Rev. 5.1.1 requires that agencies develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of an agency's systems. It also requires agencies to assess and review the supply-chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide.

Cause

In response to the auditor's inquiry, FEC OCIO management acknowledged the importance of this issue, but stated that they did not have sufficient resources or staffing capacity to develop an SCRM strategy, policies, and procedures.

Effect

In absence of an SCRM strategy, policies, and procedures, there is an increased risk of bad actors exploiting unknown vulnerabilities in the FEC OCIO's supply chain. This can lead to compromised confidentiality, integrity, or availability of the agency's systems and the information contained within those systems. Supply chain risks include:

- Insertion of counterfeit products.
- Unauthorized production of components.
- Tampering with production parts and processes.
- Theft of components.
- Insertion of malicious hardware and software.
- Poor manufacturing and development practices compromise quality.

Recommendation 2:

We recommend that the FEC OCIO develop and implement a SCRM strategy, policies, and procedures that align with NIST and as OMB requires.

Management's Response:

The FEC OCIO management concurs with the recommendation. Management acknowledged the absence of a SCRM policy and procedures and agreed that implementation is necessary. As an initial step, they plan to review the GSA's C-SCRM Program guidance and convene a planning session to determine the path forward. However, due to agency-wide budgetary and staffing constraints, management is unable to commit to a specific timeline for completion. Management's full response is included in Appendix I.

Auditor's Evaluation of Management's Response:

Management's concurrence with the recommendation and acknowledgment of the need for an SCRM policy are noted. While the proposed initial actions are reasonable, the absence of a defined timeline raises concerns about the timely implementation of this critical control. Budget and staffing limitations may further delay progress, and the auditors encourage management to prioritize this effort within available resources.

Finding 3: The FEC OCIO Did Not Monitor Compliance of Security Technical Implementation Guide (STIG) Security Configuration Settings for [redacted].

Condition

We interviewed key personnel responsible for managing [redacted] and observed the functionality of [redacted] application. We noted the FEC OCIO did not monitor [redacted] application to ensure compliance with STIG security configuration settings as required by the agency's FECLAN SSP. STIG is a checklist used to make sure computers and software are set up in a safe and secure way. The FEC utilizes the STIG security configuration settings developed by the U.S. Department of Defense's Defense Information Systems Agency (DISA) to help protect systems used by the military and other federal agencies.

Criteria

The FECLAN SSP, dated April 6, 2022, states that the FEC OCIO will use the DISA STIG security configuration settings as the baseline for configuring security settings for information systems that include operating systems, databases, applications, and networking components (e.g., [redacted]). The FECLAN SSP further states that the FEC OCIO will review and update the baseline configuration settings for information systems on an annual basis.

As discussed in Finding 1, OMB Circular A-130 requires agencies to implement security controls that satisfy the requirements of FIPS Publication 200 and the security baselines in NIST SP 800-53 (tailored as appropriate). NIST SP 800-53, Rev., 5.1.1 requires agencies to develop a current baseline configuration of the system and institute a process describing how and when it will be reviewed and updated.

Cause

In response to the auditors' inquiry, FEC OCIO management acknowledged this was an important issue, but stated that they did not have sufficient resources or staffing capacity to monitor [redacted] STIG security configuration settings to ensure ongoing compliance.

Effect

Not having an adequately secure [redacted] increases the network's exposure to threats such as unauthorized access, data breaches, and system compromise.

Recommendation 3:

We recommend the FEC OCIO secure [redacted] by monitoring configuration settings to ensure compliance with STIG security configuration settings as required by the agency's SSP.

Management's Response:

The FEC OCIO management concurs with the recommendation. Management acknowledged that STIG settings have not been fully implemented across certain systems. They are currently evaluating the impact of STIG configurations and expressed concern that full implementation may result in operational disruptions. As an interim measure, management plans to review failed configurations on a case-by-case basis using available tools and to implement validated STIG settings in a phased and controlled manner. Management's full response is provided in Appendix I.

Auditor's Evaluation of Management's Response:

The management response is generally appropriate. The acknowledgment of partial STIG implementation and the proposed phased approach demonstrate awareness of the risks associated with immediate configuration changes. However, this gradual process may extend the timeline for achieving full compliance, and the auditors encourage management to expedite implementation where feasible while ensuring system stability.

Finding 4: The FEC OCIO Did Not Fully Enforce Security Technical Implementation Guide (STIG) Security Configuration Settings for Network Server 2.

Condition

One of the FEC OCIO's network servers, Server 2, is not fully secured in accordance with established STIG security configuration settings baseline intended to reduce network vulnerabilities. Our review of the FEC OCIO's STIG compliance report for Server 2, dated March 5, 2025, revealed that 32 out of 272 security configurations failed to meet STIG compliance requirements, and 37 out of 272 configurations were not assessed for compliance.

Criteria

The FECLAN SSP states that the system owner is responsible for reviewing and updating the baseline configuration of the information system annually, when a significant change occurs, and as part of the installation or upgrade of system components. As discussed under Finding 3, the FEC uses STIG as a baseline of security settings for operating systems, databases, applications, and networking components (e.g., server equipment). The FECLAN SSP further states that the FEC OCIO will review and update the baseline configuration settings for information systems on an annual basis.

As discussed in Finding 1, OMB Circular A-130 requires agencies to implement security controls that satisfy the requirements of FIPS Publication 200 and the security baselines in NIST SP 800-53 (tailored as appropriate). As discussed in Finding 3, NIST SP 800-53, Rev. 1.1.1 requires agencies to develop a current baseline configuration of the system and institute a process describing how and when it will be reviewed and updated.

Cause

In response to the auditor's inquiry, FEC OCIO management acknowledged the importance of this issue but stated that they did not allocate sufficient resources or staffing to ensure the annual review and update of STIG security configuration settings for Server 2.

Effect

If the FEC OCIO does not review and monitor the enforcement of baseline security configuration settings in the network server, management cannot fully assess the potential risks that could compromise the agency.

Recommendation 4:

We recommend the FEC OCIO review and monitor STIG security configuration settings for its Server 2 as required by the FECLAN SSP.

Management's Response:

The FEC OCIO management concurs with the recommendation and plans to address STIG compliance issues within the next year. Management intends to leverage a scanning tool to assess and adjust the STIG baseline, document configuration exceptions with appropriate justifications, and promote uniform implementation across applicable systems. To support this effort, weekly compliance reports and review sessions will be established to monitor progress and ensure accountability. Management's full response is provided in Appendix I.

Auditor's Evaluation of Management's Response:

The management's response is satisfactory. The outlined actions and target timeline reflect a commitment to remediating STIG compliance issues. The use of automated tools and recurring oversight mechanisms is a positive step toward achieving and maintaining compliance.

Finding 5: The FEC OCIO Did Not Enforce Security Technical Implementation Guide (STIG) Security Configuration Settings for Server 1.

Condition

The FEC OCIO was not able to provide evidence that the STIG security configuration settings were implemented for Server 1, located in the FECLAN. [redacted]. The FEC OCIO's general practice is to enforce STIG security configuration settings for servers through directory Group Policy Objects (GPOs). However, the agency stated that Server 1 is a [redacted] located [redacted], which prevents it from receiving security policies applied via directory GPOs. As a result, STIG security configuration settings are not automatically enforced on Server 1, and no reports are generated to validate its compliance.

Criteria

The FECLAN SSP requires the FEC OCIO to develop, document, and maintain under configuration control a current baseline configuration of the information system. As discussed under Finding 3, the FEC OCIO uses STIG as a baseline of security settings for operating systems, databases, applications, and networking components (e.g., Server 1).

As discussed in Finding 1, OMB Circular A-130 requires agencies to implement security controls that satisfy the requirements of FIPS Publication 200 and the security baselines in NIST SP 800-53 (tailored as appropriate). As discussed in Finding 3, NIST SP 800-53, Rev. 5.1.1 requires agencies to develop a current baseline configuration of the system and institute a process describing how and when it will be reviewed and updated.

Cause

The FEC OCIO's directory GPOs containing STIG security configuration settings cannot be automatically applied to Server 1 because [redacted]. Additionally, the agency has not implemented an alternative method to enforce STIG security configuration settings or validate compliance, as required by its FECLAN SSP.

Effect

The absence of STIG security configuration settings for Server 1 could expose the agency's network to security vulnerabilities.

Recommendation 5:

We recommend that the FEC OCIO implement STIG security configuration settings for Server 1 in accordance with the agency's FECLAN SSP. If the agency cannot utilize its directory GPOs, we recommend that the agency use alternative methods.

Recommendation 6:

We recommend that the FEC OCIO conduct regular security scans of Server 1 to verify compliance with STIG security configuration settings in accordance with the agency's FECLAN SSP.

Management's Response:

The FEC OCIO management concurs with both recommendations and clarified that the affected server [redacted], which limits the ability to implement automated configuration management. As a corrective action, management is manually developing a local GPO server to manage configurations and plans to include the system in future vulnerability scans and STIG compliance reviews. In the interim, individual security settings have been applied as compensating controls to mitigate associated risks. Management's full response is provided in Appendix I.

Auditor's Evaluation of Management's Response:

The management's response is acceptable. The planned development of a local GPO server and the use of compensating controls are reasonable given the technical limitations [redacted]. Continued monitoring and inclusion in future compliance activities will be important to ensure risk is appropriately managed.

Finding 6: The FEC OCIO Did Not Remediate Vulnerabilities in a Timely Manner.

Condition

We reviewed the FEC OCIO vulnerability report dated October 17, 2024, and found that vulnerabilities were not remediated in a timely manner as required in the agency's FECLAN SSP. The vulnerability report identified a total of 717 detected vulnerabilities, of which 523 were not remediated within the required timeframe. See Table 2, Vulnerability Report Results, for more details.

Table 2: Vulnerability Report Results (as of 10/17/2024)

Severity Levels	FECLAN SSP Remediation Timeframe	Range of Days - Vulnerabilities Were Not Remediated Timely					
		<100	101-200	201-300	301-400	401-500	Total
Level 5 -Urgent	30-Days	11	14	10	4	18	**57**
Level 4 - Critical	30-Days	45	72	83	16	71	**287**
Level 3 - High	45-Days	28	22	10	9	67	**136**
Level 2 - Moderate	90-Days	2	3	2	4	32	**43**
Total		**86**	**111**	**105**	**33**	**188**	**523**

Table 3, Vulnerability Severity Levels, defines the severity levels used to classify vulnerabilities, explains the associated risks, and provides examples for each level.

Table 3: Vulnerability Severity Levels

Severity Levels	Description
Level 5 - Urgent	These vulnerabilities could allow intruders to easily gain control of the host, which can lead to the compromise of the entire network's security. For example, vulnerabilities at this level may permit an intruder to obtain full read and write access to files, remotely execute commands, and create backdoors.
Level 4 - Critical	Critical vulnerabilities could allow intruders to gain control of the host or allow potential leakage of highly sensitive information. For example, an intruder may take advantage of vulnerabilities at this level to obtain full read access to files, create potential backdoors, or access a listing of all the users on the host.
Level 3 - High	These vulnerabilities could permit intruders to gain access to specific information stored on the host, including its security settings. This could result in the potential misuse of the host by intruders. For example, vulnerabilities at this level could allow an intruder partial access to file contents, access to certain files on the host, the ability to browse the directory, access to the filtering rules and security mechanisms, the ability to institute denial of service attacks, and the unauthorized use of services, such as mail-relaying.
Level 2 - Moderate	Moderate vulnerabilities could permit intruders to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.

The FEC OCIO utilizes security monitoring tools as compensating controls to reduce the risk of vulnerability exposure. These tools are effective at detection, response, and vulnerability management. Also, the FEC OCIO is in the process of implementing new equipment and developing new applications, which indicate progress toward addressing outstanding vulnerabilities.

Criteria

The FECLAN SSP states that the FEC OCIO is responsible for remediating legitimate vulnerabilities according to the timelines listed in Table 4, FECLAN SSP Vulnerability Remediation Timelines.

Table 4: FECLAN SSP Vulnerability Remediation Timelines

Vulnerability Severity Level	Timeline for Remediation from Date of Detection
Level 5 – Urgent	30 days or less
Level 4 – Critical	30 days
Level 3 – High	45 days
Level 2 – Moderate	90 days

OMB Circular A-130 requires agencies to "[i]mplement and maintain current updates and patches for all software and firmware components of information systems." NIST SP 800-53, Rev. 5.1.1 requires agencies to monitor and scan for vulnerabilities in their systems and applications, including by utilizing a variety of vulnerability monitoring tools and techniques. It also sets forth requirements for a flaw remediation program that will identify, report, and correct system flaws; test software and firmware updates before installation; establish timelines for security-relevant

software and firmware updates; and incorporate flaw remediation into the organizational configuration management process.

Cause

During the IT evaluation for the FY 2024 Financial Statement Audit (ending September 30, 2024), FEC OCIO management acknowledged that several un-remediated vulnerabilities were associated with outdated equipment and the legacy platform that remain in operation. Management stated that applying patches to these systems risked disrupting functionality, potentially leading to system failures due to compatibility issues. Consequently, the FEC OCIO deferred patching efforts in favor of a longer-term plan to implement new equipment and migrate legacy applications to modern platforms. As a result, critical vulnerabilities remain unaddressed, increasing the agency's exposure to security risks related to unsupported systems and less effective patch management.

Effect

Not remediating vulnerabilities, especially those deemed urgent, critical, or high risk, represent an ongoing threat to the agency's mission goals, data security, and public confidence in the organization.

This audit finding is concerning because sustained vulnerabilities increase the risk of unauthorized access to sensitive systems or data, compromised operational integrity, disrupted essential services, and noncompliance with OMB Circular A-130.

Recommendation 7:

We recommend that the FEC OCIO reassess and reprioritize resources to identify opportunities to accelerate the remediation of urgent, critical, and high vulnerabilities.

Management's Response:

The FEC OCIO management concurs with the recommendation. Management acknowledged delays in vulnerability remediation and attributed them to resource limitations, the presence of legacy systems, and the lack of automated tools. They described the adoption of a risk-based approach to vulnerability management and outlined ongoing efforts such as system upgrades, the implementation of compensating controls, and a phased transition to cloud-native platforms. Management emphasized that sustained progress is contingent upon the availability of funding and staffing resources. Management's full response is provided in Appendix I.

Auditor's Evaluation of Management's Response:

Management's response presents a reasonable risk-based approach and identifies multiple initiatives to improve vulnerability remediation. The recognition of systemic constraints is appropriate; however, the continued reliance on limited resources raises concerns about the timeliness and effectiveness of mitigation efforts. The auditors encourage prioritization of high-risk vulnerabilities and recommend exploring interim measures to accelerate remediation where feasible.

Recommendation 8:

We recommend that the FEC OCIO regularly conduct risks assessments in accordance with OMB Circular A-130, *Managing Information as a Strategic Resource,* to help identify other corrective actions to improve the timeliness of vulnerability remediation.

Management's Response:

The FEC OCIO management concurs with the recommendation and reported that risk assessments are integrated into current IT modernization initiatives and the agency's annual risk profile, in accordance with OMB Circular A-130. Management noted that risks are analyzed, prioritized, and documented annually as part of the agency's enterprise risk management activities. However, they acknowledged that resource constraints continue to limit the agency's capacity to fully remediate identified risks. Management's full response is provided in Appendix I.

Auditor's Evaluation of Management's Response:

The management's response is appropriate. The integration of risk assessments into modernization efforts and the annual risk profile demonstrates alignment with OMB policy. Nonetheless, the effectiveness of these efforts may be diminished by ongoing resource constraints, and the auditors encourage continued efforts to address and mitigate high-priority risks within existing capabilities.

Finding 7: The FEC OCIO Did Not Define Comprehensive Service Level Agreements (SLA) or Key Performance Measurements (KPM) for Third-Party Services Contracts.

Condition

We reviewed two FEC OCIO third-party service contracts and noted the contracts do not include SLAs and KPMs to monitor contract performance.

Summary of the contracts reviewed:
The first contract we reviewed was between FEC and a third-party vendor for vulnerability management support. The contract total was $1,269,060 and was issued for one base year and three option years. See Table 5, Third-party Vulnerability Management Support, for more details. The contract outlines general tasks such as monitoring vulnerabilities, deploying patches, and managing plans of action and milestones. The contract does not define performance metrics such as required response times for addressing identified vulnerabilities (e.g., how quickly an organization begins to act after a vulnerability is discovered or reported), timeframes for remediation (e.g., allowed or expected time to fully resolve or fix the vulnerability) , patch deployment success rates, or clearly defined roles and responsibilities between the FEC OCIO staff and the vendor's staff.

Table 5: Third-party Vulnerability Management Support

Period of Performance	Dates	Status	Amount
Base Period	March 30, 2021 - March 29, 2022	Executed	$ 288,268
Option Year I	March 30, 2022 - March 29, 2023	Executed	$ 365,520

Period of Performance	Dates	Status	Amount
Option Year II	March 30, 2023 - March 29, 2024	Executed	$ 304,039
Option Year II	March 30, 2024 - March 29, 2025	Executed	$ 311,233
Total			**$ 1,269,060**

The other contract we reviewed was between FEC and a third-party vendor to support the legacy platform consisting of over 20 applications. Similar to the contract discussed above, this one also outlines general tasks such as help desk support, patch management, documentation, knowledge transfer, and agile development. The total value of the contract is $7,599,016, and it was issued for one base year and four option years. See Table 6, Third-party Support for Legacy Platform, for more details. The contract does not define performance metrics such as uptime guarantees,[10] response and resolution times, patch deployment success rates, service availability expectations, and clearly defined roles and responsibilities between the FEC OCIO staff and the vendor's staff.

Table 6: Third-party Support for Legacy Platform

Period of Performance	Dates	Status	Amount
Base Period	May 01, 2021 – April 30, 2022	Executed	$ 1,489,300
Option Year I	May 01, 2022 – April 30, 2023	Executed	$ 1,494,661
Option Year II	May 01, 2023 – April 30, 2024	Executed	$ 1,522,462
Option Year II	May 01, 2024 – April 30, 2025	Executed	$ 1,540,876
Option Year IV	May 01, 2025 – April 30, 2026	Pending	$ 1,551,717
Total			**$ 7,599,016**

Criteria

The FECLAN SSP describes the security requirements that any provider of external information system services to the FEC must comply with. It also requires that the FEC define and document "government oversight and user roles and responsibilities with regard to external information system services" and employ contractual tools, including service level agreements, to monitor the external service provider's compliance.

NIST SP 800-53 contains requirements similar to the FECLAN SSP. In addition, NIST SP 800-53, Rev. 5.1.1 supplemental guidance notes: "Service-level agreements define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance."

[10] Uptime guarantees can be thought of as a promise that a system or service will be working and available for use a certain percentage of the time. For example, if a company promises 99.9% uptime, they are saying their system (such as mapping software, data portals, or online lease databases) will be available almost all the time, with very little downtime for maintenance or unexpected issues.

Additionally, we note that the Federal Integrated Business Framework (FIBF)[11], includes service measures—standard performance indicators that agencies can adopt or tailor in SLAs. While the FEC is not required to comply with the FIBF, the FIBF represents the best practice for federal agencies across the government.

Cause

The FEC OCIO does not have a formal, written policy and procedures for developing and implementing SLAs and defining KPMs to measure third-party contract performance.

Effect

In the absence of formal SLA policy and procedures and defined KPMs service-level expectations within the contract, there is an increased risk of inconsistent service delivery, unclear accountability, delayed remediation of critical issues, and difficulty evaluating contractor performance.

Recommendation 9:

We recommend that the FEC develop and implement SLA policy and procedures and define KPMs for managing the performance of third-party service contracts.

Management's Response:

The FEC OCIO management partially concurs with the recommendation. Management acknowledged that while SLA policies are not currently in place, SLA principles and performance metrics are incorporated into technical approach documents and Quality Assurance Surveillance Plans. These documents serve as tools to monitor contractor performance through routine reporting and regular oversight meetings. Management noted that the development and implementation of formal SLA policies and KPMs would require coordination across the agency and approval from senior leadership, which may be delayed due to resource and staffing constraints. Management's full response is provided in Appendix I.

Auditor's Evaluation of Management's Response:

Management's response demonstrates awareness of the issue and highlights existing informal mechanisms for overseeing contractor performance. Specifically, management mentioned using technical approach documents and quality assurance plans to guide performance expectations. These are seen as informal mechanisms that serve a monitoring function, even though they are not part of a formalized SLA framework. The absence of formal SLA policies and defined implementation timelines limits the response's effectiveness. For the two contracts reviewed during the audit, the technical approach documents did not include specific SLA or KPM provisions. Accordingly, the auditors continue to recommend that FEC formalize its SLA and KPM practices to strengthen vendor accountability and performance monitoring.

[11]The FIBF is a government-wide standard developed by the OMB and the General Services Administration to help federal agencies align and modernize their business operations

Finding 8: The FEC OCIO Does Not Send [redacted] Logs to the Security Information and Event Management (SIEM) System for Monitoring.

Condition

We interviewed key personnel responsible for managing [redacted] and observed the logging functionality of [redacted] application. Based on our observation and assessment, we noted that the FEC OCIO is not ensuring that [redacted] logs are forwarded to and monitored by the agency's centralized SIEM system, even though this is a requirement in the agency's SSP. The FEC OCIO's SIEM system collects, correlates, and analyzes security logs from various sources, [redacted], to detect anomalies, threats, and compliance violations. Without this integration, the agency lacks centralized visibility into [redacted] activity, which hinders its ability to detect and respond to network-based threats effectively.

Criteria

The FECLAN SSP requires that the SIEM system collect, correlate, and analyze various logs from all network components, and applications, as well as reports alerts to the FEC Security Operations Team and the FEC Systems Operations Teams. The FECLAN SSP goes on to state that "[t]his automatic correlation and analysis and reporting support the security personnel" in the FEC OCIO, "enabling immediate investigation and response to suspicious activities."

As discussed in Finding 1, OMB Circular A-130 requires agencies to implement security controls that satisfy the requirements of FIPS Publication 200 and the security baselines in NIST SP 800-53 (tailored as appropriate). NIST SP 800-53, Rev. 5.1.1 requires agencies to integrate audit record review, analysis, and reporting processes using automated mechanisms, as selected by the agency, to log security events.

Cause

The FEC OCIO does not have adequate standard operating procedures to ensure [redacted] logs are sent to the centralized SIEM system for monitoring, as required by the agency's SSP.

Effect

Not sending [redacted] logging data to the SIEM system hinders the agency's ability to analyze cybersecurity incidents before, during, and after an occurrence.

Recommendation 10:

We recommend that the FEC OCIO ensure [redacted] logs are forwarded to and actively monitored by the agency's centralized SIEM system, in accordance with the agency's system security plan.

Management's Response:

The FEC OCIO management concurs with the recommendation and confirmed that corrective action has been implemented. [redacted] logs are now actively forwarded to and monitored by the agency's Security Information and SIEM system. Management provided documentation to verify the log receipt and noted that the agency's Logging and Monitoring Policy is being updated to reflect this change and ensure continued compliance. Management's full response is provided in Appendix I.

Auditor's Evaluation of Management's Response:

The management's response is satisfactory. The completed corrective actions and accompanying documentation adequately address the recommendation. The planned policy update further supports ongoing compliance and effective log management.

OBJECTIVES, SCOPE, AND METHODOLOGY

Audit Objective

The objective of this performance audit was to assess the operating effectiveness of the FEC's Security Patches and Vulnerabilities Management Programs. As part of our audit, we determined if vulnerabilities were patched in a timely manner and/or if alternate mitigating controls were implemented and sufficient.

Scope of Audit

This engagement focused on the FEC's Security Patches and Vulnerabilities Management Programs processes in effect as of September 30, 2024.

Methodology

We conducted this audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To accomplish our audit objective, we:

- Interviewed key personnel and reviewed applicable FEC information system security policies and procedures, as well as requirements stipulated by OMB;
- Reviewed documentation related to the FEC's Security Patches and Vulnerabilities Management Programs, such as security policies and procedures, system security plans, and risk assessments;
- Tested system processes to determine the adequacy and effectiveness of selected information system security controls;
- Reviewed the status of recommendations made in prior audit reports; and
- Reviewed the network vulnerability assessment of the FEC OCIO internal system.

To meet the audit objectives, we determined the efficiency and effectiveness of the IT patching process and responded to the following lines of inquiry:

1. Determine to what extent vulnerabilities are patched in accordance with the FEC patch management policy.
2. Determine to what extent KPIs for patch management are developed for all FEC IT systems, both internal and external; and whether those measurements are accurate and adequate.
3. Determine the average cost of addressing patch vulnerabilities.
4. Determine to what extent patching efficiencies are addressed in the agency's most significant IT contracts and service level agreements, to what extent the agency is receiving the contract deliverables, and to what extent contractors are patching the systems as required.
5. Determine to what extent FEC personnel and contractors are performing secure

baselining consistently, and the level of frequency.
6. Determine whether the FEC has sufficient personnel to accomplish critical system management and security.
7. Determine to what extent platforms and processes exhibit fully compliant/effective vulnerability patching.

Criteria

We have referenced the following criteria within this report:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004)
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006)
- NIST Special Publication (SP) 800-40 Rev. 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology* (July 2022)
- NIST SP 800-800-161, Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (November 2024)
- NIST SP 800-53 Rev. 5.1.1, *Security and Privacy Controls for Information Systems and Organizations* (November 2023)
- OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016)
- FEC information system policies and procedures.

Internal Control

We considered the internal control structure for the FEC's Security Patches and Vulnerabilities Management Programs in planning our audit procedures. We gained an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls over the FEC OCIO's internal system and contractor-owned and -managed systems through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. Our understanding of these systems' internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented. When appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

Since our audit would not necessarily disclose all significant matters in internal control, we do not express an opinion on the set of internal controls for the FEC OCIO's systems taken as a whole. There were no internal control weaknesses beyond those identified in this report that affected the audit objective.

AUDITOR'S COMMENT TO MANAGEMENT'S RESPONSE

Brown & Company thanks FEC OCIO's management for its comprehensive response to the performance audit report. We value the collaborative approach taken throughout the engagement and recognize management's ongoing commitment to enhancing the agency's Security Patches and Vulnerabilities Management Programs. We particularly appreciate FEC's acknowledgment of the audit's identification of opportunities to strengthen the agency's overall information system security posture.

Management has stated that no evidence of system compromise was identified. However, the scope of this audit did not include procedures to determine whether a compromise occurred during the review period. Accordingly, the audit does not provide assurance regarding the presence or absence of a system compromise.

Overall, management's responses to the audit recommendations are generally appropriate and demonstrate an understanding of the issues raised. In several areas, management agreed with the findings and outlined planned or ongoing corrective actions. Notably, management has taken immediate steps to address certain issues, such as forwarding [redacted] logs to the SIEM system and initiating updates to SSPP documents.

However, the effectiveness and timeliness of several planned actions are hindered by significant resource and staffing constraints. While management has expressed commitment to implementing best practices, including elements of the NIST Risk Management Framework, the lack of specific timelines and formalized policies—particularly for supply chain risk management, STIG compliance, and SLA/KPM development—presents challenges to full resolution.

In summary, while the responses are generally responsive and reflect a willingness to improve, sustained progress will depend heavily on the agency's ability to secure additional resources and leadership approval for broader agency-wide initiatives.

APPENDIX I - MANAGEMENT'S RESPONSE

FEDERAL ELECTION COMMISSION
WASHINGTON, D.C.

Management's Response to Findings in the Security Patches and Vulnerabilities Management Programs Audit for the Fiscal Year Ending September 30, 2024

The FEC Office of the Chief Information Officer (OCIO) appreciates the chance to respond to the recommendations made by Brown and Company. OCIO management is pleased to have this opportunity to confirm that the agency's systems have shown no evidence of compromise. However, this success has been achieved within the constraints of an increasingly austere budget environment, and OCIO management has made significant trade-offs in order to secure the FEC's systems within its limited staffing levels and project funding. As the findings of this audit show, OCIO has not had sufficient resources in terms of staff, tools and project funding to follow the government-wide best practices of planning, monitoring and documentation established to protect IT systems. Moreover, given the agency's current funding outlook, OCIO management does not anticipate that we will be able to remediate many of the findings included in this audit in the near future. Thus, as the results of this audit show, the FEC will be challenged to continue to safeguard its IT systems absent additional staffing, tools and funding. The Commission has made clear in its most recent Congressional Budget Justification that without sufficient funding for IT systems and projects the agency's mission is at risk. The findings of this audit serve to provide further evidence that the FEC needs additional funding to modernize the rest of its legacy systems as well as to hire additional staff to perform the job of securing the FEC's Local Area Network (FECLAN) and Cloud Infrastructure (FECCI).

Providing sufficient resources for the FEC's OCIO is essential to ensuring the FEC can perform its mission functions. OCIO ensures agency employees have a technology infrastructure that allows them to perform their day-to-day responsibilities administering and enforcing campaign finance law. OCIO also develops and supports analytic reporting tools that help staff perform their disclosure and compliance duties. In addition, OCIO develops and maintains the systems that serve as the public's primary source of information about campaign finance data and law. In this way, OCIO serves a pivotal role in ensuring the FEC protects the integrity of the federal campaign finance process by ensuring that the public has access to reliable data describing how candidates raise and spend funds to support their campaigns.

This year, OCIO updated its IT Strategic Plan to outline activities conducted by OCIO to continue to handle the agency's responsibilities with insufficient staffing and budget levels. The plan outlines OCIO's strategic activities that focus on IT modernization, security, privacy and a results-driven workforce. OCIO has demonstrated that the agency's focus on IT modernization has been successful, but its work is not complete. It is essential to continue working on these activities to ensure the 21st century FEC delivers results and effectively serves its 21st century constituents. Unfortunately, the FEC has experienced several years of essentially flat funding, representing a decline in real terms, for FEC operations. During that same period, campaign finance filing activity

has increased nearly fivefold. The requested FY 2026 funding level for the agency will result in a projected 21 percent decrease in employees on board by the end of the fiscal year. The FEC has continued to meet its statutory obligations to the public–despite reduced staffing and increasing campaign finance activity–by improving technology and processes, among other efficiencies. It must be noted that any reductions in funding in future fiscal years will negatively impact the ability of OCIO to adequately meet the recommendations made in this audit and, indeed, will place the continuation of current IT services, including those used by the public on FEC.gov and current IT modernization projects and cybersecurity contracts, in serious jeopardy.

OCIO's responses to each finding and recommendation follow.

Finding 1: The FEC OCIO Did Not Update System Security and Privacy Plans (SSPPs).

Recommendation 1:

We recommend that the FEC OCIO update the agency's SSPP documents and establish a privacy program plan that aligns with NIST SP 800-53, Rev.5.1.1 requirements as required by OMB.

Management's Response:

OCIO agrees with the recommendation to update the SSPP documents. The agency recently shut down a data center, migrated resources to the FEC Cloud Infrastructure (FECCI), and is in the process of updating the SSPP for FECCI. The FECLAN update will follow once the FECCI SSPP is completed. However, progress will be slowed due to a lack of additional cybersecurity staff. The FEC is experiencing budget and staffing limitations in FY 2025 and expects the same in FY 2026. OCIO had requested and received approval to post an additional cybersecurity analyst position; however, this hiring effort was halted due to a freeze on new hires by the agency in January 2025.

Regarding a privacy program, the FEC has prepared a privacy policy that applies to its website and third-party sites and applications that the FEC uses. This was provided to the auditors and identifies the agency's Privacy Officers. FEC has an established organization-wide privacy program, led by the Privacy Office, which oversees privacy compliance, policy implementation, and governance across the agency. The Privacy Office, in coordination with the Senior Agency Official for Privacy (SAOP), ensures that FEC's privacy policies, practices, and procedures align with applicable legal and regulatory requirements.

It is important to note that the FEC is generally exempt from the E-Government Act and the Federal Information Security Management Act of 2002 (FISMA) due to its exemption from the Paperwork Reduction Act (PRA), which provides the statutory definition of "agency" for both FISMA and the E-Government Act. Because FISMA applies only to entities defined as federal agencies by the PRA, and because the PRA specifically excludes the FEC in its definition of "agency," FISMA does not apply to the FEC. Accordingly, although NIST 800-53 refers to OMB Circular A-130, which generally applies to the FEC, because NIST 800-53 relies solely on FISMA for its legal authority, which does not apply to the FEC, NIST 800-53 does not apply to the FEC. As a result,

the FEC is not subject to these mandates, and its privacy program is structured to address applicable legal and operational requirements specific to the agency's mission and authorities.

That said, the FEC decided to adopt the National Institute of Science and Technology's (NIST) Risk Management Framework (RMF) as best practice for FEC's major and critical systems. The Commission's adoption of the RMF, specifically NIST 800-37, applies across the agency's key information systems. As part of the adoption of the RMF, OCIO conducts continuous monitoring to safeguard the agency's information and infrastructure.

The FEC remains committed to protecting personally identifiable information (PII) and will continue to refine its privacy program in alignment with agency priorities and available resources. Any future privacy initiatives will be coordinated through the Privacy Office with appropriate stakeholder engagement. Note, however, that any such future initiatives would be impacted by budget and staffing limitations that are affecting the entire agency and would need Commission approval.

Finding 2: The FEC OCIO Has Not Developed and Implemented Supply Chain Risk Management (SCRM) Strategy, Policies, and Procedures.

Recommendation 2:

We recommend that the FEC OCIO develop and implement a SCRM strategy, policies, and procedures that align with NIST and as OMB requires.

Management's Response:

OCIO acknowledges upfront that it does not currently have Supply Chain Risk Management Policy and Procedures. The FECCI ATO assessor recommended that the FEC implement the General Services Administration Cyber Supply Chain Risk Management (C-SCRM) Program (https://www.gsa.gov/system/files/OCISO-Cyber-Supply-Chain-Risk-Management-%28C-SCRM%29-Program-%5BCIO-IT-Security-21-117-Revsion-2%5D-03-07-24.pdf). This program provides guidance on strategies for managing supply chain risk, including conducting thorough assessments of suppliers and vendors to evaluate their security practices and potential risks. It also involves establishing contractual agreements that define security requirements and responsibilities, as well as continuously monitoring supply chain activities and integrating supplier risk assessments into procurement decisions. OCIO notes that our contracts do include standard language that relates to supply chain risk.

Implementing policy and procedures for Supply Chain Risk Management will be a large, agency-wide (not just OCIO) project that will require approval by FEC senior leaders as well as ultimately by the FEC's six Commissioners. The FEC is experiencing budget and staffing limitations in FY 2025. Nevertheless, OCIO acknowledges that it must be undertaken. To get started, OCIO's cloud operations team will begin with an initial planning session to determine the steps needed to develop the policy and procedures. This policy will need to be implemented as an agency-wide project during a time when many other government mandates are being

implemented and there are staffing and resource constraints, so OCIO is unable to provide an estimated date for this project at this time as it would be impacted by budget and staffing limitations that are affecting the entire agency.

Auditor's Evaluation of Management's Response:

Finding 3: The FEC OCIO Did Not Monitor Compliance of Security Technical Implementation Guide (STIG) Security Configuration Settings for [redacted] application.

Recommendation 3:

We recommend the FEC OCIO secure [redacted] by monitoring configuration settings to ensure compliance with STIG security configuration settings as required by the agency's SSP.

Management's Response:

OCIO acknowledges that there are no STIGS implemented for certain systems at this time. OCIO is looking into implementing the STIG security settings but due to their complexity and risk of breaking other systems, we want to proceed with caution and intention. OCIO has implemented various security settings on the application to make it as secure as possible. Using other available tools, OCIO will continuously review all settings that did not pass and address those settings one-by-one until STIGS are implemented. OCIO has devised a plan to use evaluated STIG settings which will be monitored and applied methodically.

Finding 4: The FEC OCIO Did Not Fully Enforce Security Technical Implementation Guide (STIG) Security Configuration Settings for its Network Server.

Recommendation 4:

We recommend the FEC OCIO review and monitor STIG security configuration settings for its Server 2 as required by the FECLAN SSP.

Management's Response:

OCIO Management agrees with this recommendation and plans to remediate this within the next year. OCIO intends to use our scanning tool to review and modify our STIG baseline, include proper justifications, and ensure settings are consistently applied across all devices.

To do this, we plan to:

1. Add compliance reporting to our weekly team meetings based on what we see in scans.

2. Schedule short weekly working sessions to review failed or Not Reviewed STIG items, then present this weekly. During these sessions, we'll capture justifications, confirm previous test, and update our scanning tool accordingly.

OCIO will approach this work gradually as we have competing vulnerability remediation projects. Nevertheless, we look forward to creating a reliable source of truth within our scanning tool to ensure we capture policy compliance across our environment, including the aforementioned server.

Finding 5: The FEC OCIO Did Not Enforce Security Technical Implementation Guide (STIG) Security Configuration Settings for [redacted] Server (Server 1).

Recommendation 5:

We recommend that the FEC OCIO implement STIG security configuration settings for Server 1 in accordance with the agency's FECLAN SSP. If the agency cannot utilize its directory GPOs, we recommend that the agency use alternative methods.

Recommendation 6:

We recommend that the FEC OCIO conduct regular security scans of Server 1 to verify compliance with STIG security configuration settings in accordance with the agency's FECLAN SSP.

Management's Response:

This server [redacted] which precludes OCIO from automating the implementation of STIGs. OCIO agrees that it will use an alternative method as recommended. OCIO's Infrastructure Team is currently manually developing a local GPO server for this. That server will be included in the scans and STIG review discussed in our response to Finding 4. Also, as a compensating control for not being able to control STIGS, OCIO has enforced individual security settings.

Finding 6: The FEC OCIO Did Not Remediate Vulnerabilities in a Timely Manner.

Management's Response:

The FEC Office of the Chief Information Officer (OCIO) acknowledges the outstanding vulnerabilities identified in the audit report and is committed to improving the timeliness and consistency of remediation efforts. OCIO currently follows a risk-based vulnerability management program that prioritizes remediation based on several factors: the severity and scope of vulnerabilities across FEC assets, the associated threat categories (e.g., lateral movement, ransomware vectors), exploitability, level of effort to remediate, and the presence of existing compensating controls.

Despite this prioritization framework, remediation of certain critical and high vulnerabilities remains delayed due to ongoing resource constraints, reliance on legacy systems, and limited automation. Many of these vulnerabilities are associated with outdated platforms and aging hardware, where standard patching tools offer limited effectiveness.

OCIO has developed a feasibility plan to address the majority of these vulnerabilities; however, full implementation has been hindered by budgetary limitations. This plan includes three core

components: (1) addressing legacy application systems and outdated equipment, (2) mitigating vulnerabilities in the current [redacted] platform until it can be fully replaced, and (3) modernizing and migrating [redacted]-hosted applications to cloud-native solutions.

Regarding legacy application systems and equipment, OCIO upgraded the [redacted] server application in 2024. Additionally, OCIO leveraged reallocated FY 2023 and FY 2024 end-of-year funding to purchase new laptops to replace outdated systems. These new laptops, which began arriving in late 2023, are being issued with the required security patches and upgraded software, including [redacted]. OCIO will be configuring and distributing an additional batch of laptops that also includes the upgraded [redacted] version.

To address vulnerabilities in the existing [redacted] environment, OCIO has adopted compensating controls to maintain security while ensuring mission-critical functionality is preserved. Applying certain remediations directly could disable key legacy applications that support core agency functions. Instead, OCIO's Security Operations (SecOps) team has implemented additional protections through specific tools which help defend the agency from cybersecurity intrusions.

In addition, OCIO is exploring whether a cloud-based zero trust access application can be used to enforce endpoint compliance by checking if devices are properly patched before allowing user logins. This approach would support timely updates and would also allow the remediation team to identify and address issues on specific machines more efficiently.

On the modernization front, OCIO has initiated a phased migration of [redacted]-hosted applications to cloud-native platforms. In 2023, OCIO conducted extensive market research on replacing three key [redacted] applications that are integral to Commission voting, workflow, and document certification processes. In 2024, the Commission approved funding for this modernization initiative, and development work began in July 2024 with a projected completion date of July 2026.

OCIO has also identified alternative modernization paths for two additional [redacted] applications used by the Office of General Counsel and is moving forward on these projects as staff time and resources allow. In particular, OCIO staff have begun working on a design and proof of concept for an in-house solution to one of these applications. OCIO plans to recommend decommissioning the other application as analytics show it is no longer used by OGC. Lastly, the Office of the Chief Financial Officer (OCFO) is planning to replace an invoice tracking application still on the [redacted] platform, and OCIO will support that migration effort.

As the first page of the final audit report notes, "The FEC has had significant budget and resource constraints for several years that have contributed to its inability to remediate vulnerabilities and patches related to legacy systems and outdated equipment." The successful migration of all [redacted] applications will ultimately enhance the FEC's overall security posture while reducing long-term maintenance and support expenses. Ultimately, however, staffing and funding constraints will limit the FEC's ability to pursue other much-needed IT modernization projects to find modern solutions for aging legacy applications.

Recommendation 8:

We recommend that the FEC OCIO regularly conduct risks assessments in accordance with OMB Circular A-130, *Managing Information as a Strategic Resource,* to help identify other corrective actions to improve the timeliness of vulnerability remediation.

Management's Response:

OCIO agrees with the recommendation and notes that all of the current modernization projects include risk assessments and the maintenance of a risk register. OCIO also actively participates each year in the development of the FEC's risk profile required by OMB Circular A-130, and as part of that process, annually fills out and submits a detailed roll-out spreadsheet to OCFO that analyzes the risks to the FEC's systems and data. In developing its responses, OCIO senior management analyzes many potential risks to the agency's systems and addresses impact, level of risk and mitigation plans.

Ultimately, however, as the first page of the final audit report notes, "The FEC has had significant budget and resource constraints for several years that have contributed to its inability to remediate vulnerabilities and patches related to legacy systems and outdated equipment."

Finding 7: The FEC OCIO Did Not Define Comprehensive Service Level Agreements (SLA) or Key Performance Measurements (KPM) for Third-Party Services Contracts.

Recommendation 9:

We recommend that the FEC develop and implement SLA policy and procedures and define KPMs for managing the performance of third-party service contracts.

Management's Response:

OCIO agrees that the FEC should implement SLAs and KPMs for managing the performance of third-party service contracts. While there is no formal policy, the FEC does implement these concepts and ensures that those contracts are closely managed to ensure that the vendors deliver what the FEC has requested.

Traditionally these items are included in Statements of Work during the solicitation process. The wording of solicitations can differ, however, depending on what the agency seeks to purchase. For example, the vulnerability management contract mentioned in the final audit report provides vulnerability and patch management consulting services while the IT Services contract that was mentioned provides development and technical support for FEC internal and public facing applications. In both cases, the patching is actually performed by FEC staff after coordinating what is needed with the vendors.

In certain cases, the FEC will include additional, more specific requirements in a separate document or Quality Assurance Surveillance Plan (QASP) provided to the vendors. In the cases of these two vendors, the companies each provided a technical approach document that included

their deliverables and key performance measures. The FEC agreed with the approaches presented so the awards were issued. Both contracts were issued in 2021 and during that time, the Procurement Office did not process the final contract to include the technical approach document. Thus, it was not included in the documentation of the contracts provided to the auditors. However, the technical approach documentation was considered part of the total contract award package and it was maintained separately by the Procurement Office. Those documents were provided to the auditors on April 10, 2025. It should be noted that in the present time, the technical approach documentation is included in the final contract and the template used for current Statements Of Work/Performance Work Statements includes additional requirements for quality control and assurance.

To ensure that work in the contracts is delivered as expected and outlined in the technical approach, both vendors hold regular meetings with the FEC and are in close contact with their Contracting Officer Representatives (CORs).

The vendor holding the vulnerability management contract holds a weekly SecOps briefing with the FEC's OCIO. Documentation of those weekly meetings was provided to the auditors. During those meetings, discussions of necessary remediations occur and work is assigned out as needed to FEC staff. (Again, it should be noted that it is FEC staff that patch operating systems and upgrade servers; this work is neither performed by the vendor nor it is required by their contract.)

The vendor holding the IT Services contract holds standup meetings three times a week with its COR and business owners where the IT Services team provides updates on the progress on their work and discusses concerns raised by the COR and business owners. In addition, the FEC notes that the COR for this contract changed twice in 2024 due to the longtime COR's retirement in June 2024. The new permanent COR instituted monthly sprints, monthly planning sessions and a monthly report in January 2025.

In summary, the FEC believes that it is meeting the requirements of establishing SLAs and monitoring performance of its third-party service IT contracts. Moreover, implementing SLA policies and defined KPIs for third party contracts will be an agency-wide (not just OCIO) project that will require approval by FEC senior leaders as well as ultimately by the FEC's six Commissioners. These policies and procedures would need to be implemented as an agency-wide project during a time when many other government mandates are being implemented and there are staffing and resource constraints, so OCIO is unable to provide an estimated date for this project at this time as it would be impacted by budget and staffing limitations that are affecting the entire agency.

Finding 8: The FEC OCIO Does Not Send [redacted] Logs to the Security Information and Event Management (SIEM) System for Monitoring.

Recommendation 10:

We recommend that the FEC OCIO ensure [redacted] logs are forwarded to and actively monitored by the agency's centralized SIEM system, in accordance with the agency's system security plan.

Management's Response:

OCIO agrees that [redacted] logs should be forwarded to and monitored by the agency's SIEM system. OCIO would like to clarify that OCIO has taken corrective action and [redacted] logs have now been forwarded to the SIEM system. Our security team has confirmed that they are now receiving the logs into the SIEM system and we have separately submitted relevant documentation of their receipt. Additionally, the security team is updating the agency's Logging and Monitoring policy to ensure that the policy adequately covers what needs to go into the SIEM. Given these corrective actions, OCIO believes that this recommendation should be closed as the situation has been rectified.

APPENDIX II - ACRONYMS

Acronyms	
CA	Assessment, Authorization, and Monitoring
CIO	Chief Information Officer
CM	Configuration Management
FEC	Federal Election Commission
FECCI	FEC Cloud Infrastructure
FECLAN	FEC General Support System Local Area Network
FIBF	Federal Integrated Business Framework
FIPS	Federal Information Processing Standards
GAGAS	Generally Accepted Government Auditing Standards
GPO	Group Policy Object
IT	Information Technology
KPI	Key Performance Indicator
KPM	Key Performance Measurements
NIST	National Institute of Standards and Technology
OCIO	Office of Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PM	Program Management
RA	Risk Assessment
REV	Revision
SA	System and Services Acquisition
SCRM\SR	Supply Chain Risk Management
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SP	Special Publication
SSPP	System Security and Privacy Plan
STIG	Security Technical Implementation Guide