

**UNITED STATES
ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL**



***Fiscal Year 2021 EAC Compliance
with the Federal Information
Security Modernization Act***




OFFICE OF THE INSPECTOR GENERAL
US ELECTION ASSISTANCE COMMISSION
633 3RD STREET, NW, SUITE 200
WASHINGTON, DC 20001

Memorandum

Date: November 2, 2021

To: Donald L. Palmer, Chairman
U.S. Election Assistance Commission

From: 
Mia M. Forgy
Deputy Inspector General

Subject: Final Report – Fiscal Year 2021 U.S. Election Assistance Commission Compliance with the Requirements of the Federal Information Security Modernization Act (Assignment No. I-PA-EAC-04-21)

The Office of Inspector General (OIG) engaged Brown & Company, PLLC (Brown & Co.), an independent certified public accounting firm, to conduct an audit of the U.S. Election Assistance Commission's (EAC's) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) and related information security policies, procedures, standards, and guidelines. The audit included assessing the EAC's effort to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the EAC.

Results of Audit

Based on Brown & Co.'s testing of selected controls on the EAC systems, the audit concluded that EAC generally complied with FISMA requirements by implementing security controls. Those tests were designed to obtain sufficient, appropriate evidence to provide a reasonable basis for Brown & Co.'s findings and conclusions, based on their audit objectives.

Although EAC generally had policies for its information security program, its implementation of those policies for selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or

destruction. Consequently, the audit identified areas in EAC's information security program that need to be improved.

Brown & Co. made seven recommendations to assist EAC in strengthening its information security program:

- Perform Security Content Automation Protocol scanning.
- Ensure Windows 10 devices comply with EAC's system security plan.
- Timely implement and process software patches.
- Develop and implement a supply risk chain management strategy.
- Develop and implement an anti-counterfeit policy and procedures.
- Provide proper training to IT staff to detect counterfeit system components.
- Update EAC's Plan of Action & Milestone (POA&M) workbook to align with all requirements from the U.S. Office of Management and Budget.

EAC management generally agreed with the findings and recommendations. EAC management has provided responses to the recommendations, and they are included in the final report.

In accordance with *Government Auditing Standards*, Brown & Co. also followed up on the status of the recommendations contained in prior FISMA audit reports. They found that EAC had completed corrective actions for eight of the 10 outstanding recommendations (see Appendix II, page 10). The recommendations that remain uncorrected are:

- Remediate configuration related vulnerabilities in the network identified and document the results or document acceptance of the risks of those vulnerabilities. (2018)
- We recommend EAC OIT ensure Data Owners sign user access recertifications. (2020)

[Evaluation of Brown & Co.'s Audit Performance](#)

To fulfill our responsibilities under *Government Auditing Standards* and other related requirements, the OIG:

- Reviewed Brown & Co.'s approach and planning of the audit;
- Evaluated the qualifications and independence of the auditors;
- Monitored the progress of the audit at key points;
- Coordinated or participated in periodic meetings with Brown & Co. and EAC management to discuss progress, findings, and recommendations;
- Reviewed Brown's draft audit report;
- Performed other procedures we deemed necessary, and
- Coordinated issuance of the audit report.

Brown & Co. is responsible for the attached auditor's report and the findings and conclusions expressed in the report. The work the EAC OIG performed in evaluating Brown & Co.'s conduct of the audit was not sufficient to support an opinion on the effectiveness of internal control or

compliance with laws and regulations, thus EAC OIG does not express any opinion on EAC's internal controls or compliance.

Report Distribution

The Inspector General Act of 1978, as amended, requires semiannual reporting to Congress on all reports issued, actions taken to implement recommendations, and recommendations that have not been implemented. Therefore, we will report the issuance of this audit report in our next semiannual report to Congress. The distribution of this report is not restricted and copies are available for public inspection. Pursuant to the IG Empowerment Act of 2016, the EAC OIG will post this audit report on the OIG website within 3 days of its issuance to EAC management. The OIG will also post the report to Oversight.gov.

Please contact the EAC OIG if you have any questions regarding this report.

cc: Commissioner Thomas Hicks, Vice-Chair
Commissioner Christy McCormick
Commissioner Benjamin W. Hovland
Mona Harrington, Executive Director
Jessica Bowers, Chief Information Officer/Chief Information Security Officer

Attachment

**Independent Audit of the
U.S. Election Assistance Commission's Compliance with the
Federal Information Security Modernization Act of 2014**



**Fiscal Year 2021
October 29, 2021**

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

Ms. Mia Forgy
Deputy Inspector General
U.S. Election Assistance Commission
Office of the Inspector General
Washington, DC

Dear Ms. Forgy:

Enclosed is the audit report on the United States Election Assistance Commission's (EAC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). The EAC Office of the Inspector General (OIG) contracted with the independent certified public accounting firm of Brown & Company CPAs and Management Consultants, PLLC (Brown & Company), to conduct the audit in support of the FISMA requirement for an annual evaluation of EAC Office of Information Technology (OIT) information security program.

The objective of this performance audit was to determine whether EAC OIT implemented selected security controls for certain information systems in support of FISMA. The audit included the testing of selected management, technical, and operational controls outlined in the National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

For this audit, we reviewed selected controls from EAC's General Support System. The audit also included a review of vulnerability assessments on internal systems and an evaluation of the EAC OIT process to identify and mitigate information systems vulnerabilities. Audit fieldwork was performed at EAC's headquarters in Washington, DC from April 1, 2021 through September 30, 2021.

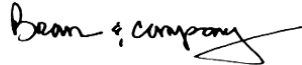
Our performance audit was performed in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions 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 audit concluded that EAC OIT generally complied with FISMA requirements by implementing selected security controls for tested systems. Although EAC OIT generally had policies for its information security program, its implementation of those policies for selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction.

Consequently, the audit identified areas in EAC OIT information security program that needed to be improved. We are making seven recommendations to assist EAC OIT in strengthening its information security program. In addition, findings related to recommendations from prior years were not yet fully implemented.

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 assistance we received from the staff of EAC and the opportunity to serve you. We will be pleased to discuss any questions you may have.



Greenbelt, Maryland
October 29, 2021

Table of Contents

Summary of Results.....	1
Audit Findings	3
1. EAC OIT needs to improve its configuration management practices.	3
2. EAC needs to develop and implement a supply chain risk management (SCRM) strategy, policies, and procedures.....	4
3. EAC OIT needs to update its Plan of Action and Milestones (POA&M) to meet OMB requirements.	5
Appendix I – Scope, Methodology and Criteria.....	7
Appendix II – Status of Prior Years Findings	10
Appendix III - Acronyms	12
Appendix IV – Management’s Comments	13



Summary of Results

The Federal Information Security Modernization Act of 2014¹ (FISMA), requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems², including those provided or managed by another agency, contractor, or other sources. Because the United States Election Assistance Commission (EAC) is a federal agency, it is required to comply with federal information security requirements.

FISMA also requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capabilities are established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the U.S. Office of Management and Budget (OMB) and to congressional committees on their information security program's effectiveness. FISMA has also established that the standards and guidelines issued by the National Institute of Standards and Technology (NIST) are mandatory for federal agencies.

The EAC's Office of Inspector General (OIG) engaged Brown & Company CPAs and Management Consultants, PLLC (Brown & Company) to conduct an audit in support of the FISMA requirement for an annual evaluation of EAC OIT information security program. This performance audit's objective was to determine whether EAC OIT implemented certain security controls for selected information systems in support of FISMA.

Our audit was performed in accordance with generally accepted government auditing standards. 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.

For this audit, we reviewed selected controls from EAC's General Support System.

¹ The Federal Information Security Modernization Act of 2014 (Public Law 113–283— December 18, 2014) amends the Federal Information Security Management Act of 2002.

² According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Results

Although, EAC OIT generally has policies for its information security program, its implementation of those policies for security controls reviewed was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, the audit identified areas in the EAC OIT information security program that needed to be improved. Specifically, EAC OIT needs to:

1. Improve its configuration management practices
2. Develop and implement a supply chain risk management (SCRM) strategy, policies, and procedures
3. Update its Plan of Action and Milestones (POA&M) to meet OMB requirements

This report makes seven recommendations to assist EAC OIT in strengthening its information security program. In addition, as illustrated in Appendix II, findings related to two prior years' recommendations had not yet been fully implemented, and therefore, new recommendations were not made. Detailed findings appear in the following section.

Audit Findings

1. EAC OIT needs to improve its configuration management practices.

Office of Management and Budget (OMB) *Guidance on the Federal Desktop Core Configuration (FDCC)*, M-08-22 memorandum, dated August 11, 2008, states:

Both industry and government information technology providers must use Security Content Automation Protocol (SCAP) validated tools with FDCC Scanner capability to certify their products operate correctly with FDCC configurations and do not alter FDCC settings.

NIST SP 800-53 Rev. 4, CM-2 “Baseline Configuration”, requires organization to develop, document, and maintain under configuration control, a current baseline configuration of the system.

NIST SP 800-53 Rev. 4, SI-2 “Flaw Remediation”, requires organizations to install security-relevant software and firmware updates within the organization-defined time period of the release of the updates. Also, NIST SP 800-53 Rev. 4, CM-3 “Configuration Change Control”, requires organization to retains records of configuration-controlled changes to the information system for the organization-defined time period.

EAC OIT does not conduct SCAP scanning to assess both code-based and configuration-based vulnerabilities for systems on its network. EAC OIT has SCAP-enabled tools; however, EAC OIT has not deployed this feature.

EAC *System Security Plan* requires Center for Internet Security (CIS) configuration settings for Windows 10 workstations. However, EAC OIT has not ensured Window 10 workstations comply with its CIS security benchmarks. The EAC OIT CIS latest compliance report (dated May 31, 2021) shows a total of 20,880 controls tested, 72% passed, and 28% failed.

EAC *System Security Plan* requires flaw remediation to be performed through patch deployment and software update no more than 17 days of the release of updates. EAC has not implemented software patches for its information systems in a timely manner. Specifically, during the auditors’ observation of EAC OIT’s patch management tools, we noted thirty-nine missing patches, of which ten were critical. In addition, EAC’s OIT patch remediation does not go through change control process prior to implementation and EAC OIT has not provided samples of change control tickets.

The cause of these conditions is the EAC OIT internal controls around configuration management are not operating effectively to ensure all configuration practices implemented are fully implemented.

The effect of not having effective controls is EAC OIT information systems face an increased risk of being comprised if OIT does not conduct SCAP scans, implement CIS security baselines and remediate patches.

Recommendation 1:

We recommend EAC OIT perform Security Content Automation Protocol (SCAP) scanning to identify vulnerabilities in all systems on the network to assess both code-based and

configuration-based vulnerabilities as required by Office of Management and Budget (OMB).

Auditor's Evaluation of Management's Response:

EAC's management concurred with the recommendation.

Management's full response is provided in Appendix IV.

Recommendation 2:

We recommend EAC OIT ensure its Windows 10 devices comply with its Center for Internet Security (CIS) security benchmarks as required by its system security plan.

Auditor's Evaluation of Management's Response:

EAC's management concurred with the recommendation.

Management's full response is provided in Appendix IV.

Recommendation 3:

We recommend EAC OIT implement software patches in its information systems in a timely manner and process patches through its change control process as required by its system security plan.

Auditor's Evaluation of Management's Response:

EAC's management concurred with the recommendation.

Management's full response is provided in Appendix IV.

2. EAC needs to develop and implement a supply chain risk management (SCRM) strategy, policies, and procedures.

OMB Circular A-130, Managing Information as a Strategic Resource, requires agencies to implement supply chain risk management (SCRM) principles to protect against supply chain risks, such as the insertion of counterfeits, unauthorized production, tampering, the insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle.

NIST SP 800-53 Rev. 4, PM-30 "*Supply Chain Risk Management Strategy*", requires organizations to develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services.

NIST SP 800-53 Rev. 4, SR-11 "*Component Authenticity*", requires organizations to develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; train organization-defined personnel or roles to detect counterfeit system components (including hardware, software, and firmware); and maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service.

EAC developed an Enterprise Risk Management Strategy (ERM) requiring the implementation integration of EAC's risk management process throughout the Agency. However, EAC did not

develop and implement an SCRM strategy to manage supply chain risks associated with the development, acquisition, maintenance, disposal of systems, components, and system services.

In addition, EAC developed a System and Service Acquisition Policy to address EAC's hardware, software acquisition process. However, EAC has not developed and implemented policies and procedures to ensure counterfeit components are detected and prevented from entering the organization's systems. Also, EAC did not provide OIT staff training to detect counterfeit system components (including hardware, software, and firmware).

This condition occurred because EAC OIT lacks controls for implementing SCRM Strategy, policies and procedures.

Not developing and implementing a SCRM strategy, policies and procedures increases the risk of bad actors exploring unknown vulnerabilities in EAC's supply chain and, thus, compromise the confidentiality, integrity, or availability of the agency's systems and the information contained in the systems.

Recommendation 4:

We recommend EAC develop and implement a supply risk chain management strategy that aligns with NIST and as required by OMB.

Auditor's Evaluation of Management's Response:

EAC's management concurred with the recommendation.

Management's full response is provided in Appendix IV.

Recommendation 5:

We recommend EAC develop and implement an anti-counterfeit policy and procedures that include detecting and preventing counterfeit components from entering the system.

Auditor's Evaluation of Management's Response:

EAC's management does not concur with the recommendation.

Management's full response is provided in Appendix IV.

Recommendation 6:

We recommend EAC provide training for the OIT staff to detect counterfeit system components (including hardware, software, and firmware).

Auditor's Evaluation of Management's Response:

EAC's management concurred with the recommendation.

Management's full response is provided in Appendix IV.

3. EAC OIT needs to update its Plan of Action and Milestones (POA&M) to meet OMB requirements.

OMB Memorandum 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, states an agency POA&M must include all security weaknesses found, and in need of remediation, during any other assessment done by, for, or on behalf of the agency, including Government Accountability Office (GAO) audits, financial system audits, and critical

infrastructure vulnerability assessments. It also states the appropriate level of detail include severity and brief description of the weakness; agency head responsible for resolving the weakness; estimated funding resources required to resolve the weakness; scheduled completion date for resolving the weakness; key milestones with completion dates; changes to milestones; source (e.g., program review, Inspector General (IG) audit, GAO audit, etc.) of the weakness; and status of corrective actions.

The *Election Assistance Commission Plan of Action and Milestones Procedure*, states POA&M is the corrective action plan (document or tool) for tracking and planning the resolution of the weaknesses. It details the resources (e.g., personnel, technology, funding) required to accomplish the elements of the plan, milestones for correcting the weaknesses, and scheduled completion dates for the milestones.

The auditors examined EAC's fiscal year (FY) 21 POA&M and noted that the document did not contain all security weaknesses and did not align with OMB's attribute requirements for reporting. Specifically, EAC's POA&M did not contain unresolved weaknesses identified in its vulnerability reports, Department of Homeland Security (DHS) assessment reports, and Federal Information Security Management Act (FISMA) reports. The POA&M list do not include sufficient information (e.g., criticality of the deficiencies, resources required, scheduled completion date, and estimated funding).

Without sufficient documentation of the agency's POA&M, EAC cannot ensure all security risks have been fully addressed and mitigated.

This condition occurred because EAC OIT lacks controls for updating and maintaining the agency's POA&M for unresolved weaknesses identified in its vulnerability reports, DHS assessment reports, and FISMA reports.

Recommendation 7:

We recommend EAC OIT update its PO&AM workbook to include all known weakness and add the appropriate level of detail required as instructed by OMB.

Auditor's Evaluation of Management's Response:

EAC's management does not concur with the recommendation.

Management's full response is provided in Appendix IV.

Appendix I – Scope, Methodology and Criteria

Scope

We conducted this audit in accordance with generally accepted government auditing standards, as specified in the Government Accountability Office's *Government Auditing Standards*. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was designed to determine whether EAC OIT implemented selected security controls for certain information systems in support of the FISMA Act of 2014.

Our overall objective was to evaluate EAC OIT security program and practices, as required by FISMA. Specifically, we reviewed the status of the following areas of EAC OIT security program in accordance with DHS FISMA Inspector General reporting requirements:

- Risk Management;
- Supply Chain Risk Management
- Configuration Management;
- Identity, Credential, and Access Management;
- Data Protection and Privacy;
- Security Training;
- Information Security Continuous Monitoring;
- Incident Response; and
- Contingency Planning.

In addition, we evaluated the status of EAC's IT security governance structure and the Agency's system security assessment and authorization (SA&A) methodology. We also followed up on outstanding recommendations from prior FISMA audits (see Appendix II) and performed audit procedures on EAC's internal and on external systems. The audit also included a review of vulnerability assessments of EAC-managed internal system and an evaluation of EAC OIT process for identifying and mitigating technical vulnerabilities.

Methodology

We reviewed EAC's general FISMA compliance efforts in the specific areas defined in DHS's guidance³ and the corresponding reporting instructions. We also audited an internal system and EAC's SA&A process. We considered the internal control structure for EAC's systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain 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 EAC's internal system and contractor-owned and managed systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. Our understanding of these systems'

³ OMB M-21-02 Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements.

APPENDIX I

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.

We assess internal controls, deemed significant to our audit, which include the following:

- Risk Assessment:
 - Define Objectives and Risk Tolerances
 - Identify, Analyze, and Respond to Risks
 - Identify, Analyze, and Respond to Change
- Control Activities:
 - Design Control Activities
 - Implement Control Activities
- Information and Communication:
 - Communicate Internally
 - Communicate Externally
- Monitoring:
 - Perform Monitoring Activities
 - Evaluate Issues and Remediate Deficiencies.

To accomplish our audit objective, we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA;
- Reviewed documentation related to EAC OIT information security program, such as security policies and procedures, system security plans, and risk assessments;
- Tested system processes to determine the adequacy and effectiveness of selected controls;
- Reviewed the status of recommendations in the fiscal years 2018, 2019 and 2020 FISMA audit reports; and
- Reviewed the network vulnerability assessment of the EAC OIT internal system.

Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the set of internal controls for EAC's systems taken as a whole.

Criteria

The criteria used in conducting this audit included:

- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*;
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*;
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*;
- NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*;
- NIST SP 800-61, Rev. 1, *Computer Security Incident Handling Guide*;
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*;
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*;
- NIST SP 800-137, *Information Security for Continuous Monitoring for Federal Information Systems and Organizations*;
- *NIST Framework for Improving Critical Infrastructure Cybersecurity, V 1.1*;
- *Chief Financial Officers Council and the Performance Improvement Council release the Playbook: Enterprise Risk Management (ERM)*;
- *Federal Acquisition Regulation (FAR); FAR Case 2007-004, Common Security Configurations*;
- *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*;
- *OMB Circular A-130, Managing Information as a Strategic Resource, July 28, 2016*
- *OMB Memorandum M-08-05, Implementation of Trusted Internet Connections*;
- *OMB Memorandum M-08-22, Guidance on the Federal Desktop Core Configuration (FDCC)*;
- *OMB Memorandum M-18-02, Guidance on Federal Information Security and Privacy Management Requirements*; and
- *SECURE Technology Act, Federal Acquisition Supply Chain Security*;
- *US-CERT Incident Notification Guidelines*; and
- *OMB M-20-32 Improving Vulnerability Identification, Management, and Remediation*;

The audit was conducted at EAC's headquarters in Washington, DC, from April 1, 2021 through September 30, 2021.

Appendix II – Status of Prior Years Findings

The following table provides the status of the Fiscal Year (FY) 2018, 2019 and 2020 audit recommendations.

No.	FY 2018 ⁴ , 2019 ⁵ , 2020 ⁶ Audit Recommendations	Status	Auditor's Position on Status
1.	FY 2018 FISMA audit recommendation No. 3: EAC OIT to remediate configuration-related vulnerabilities in the network identified, and document the results or document acceptance of the risks of those vulnerabilities.	Open	Agree
2.	FY 2018 FISMA audit recommendation No. 6: EAC to review and approve Agency's information security policies and procedures on an annual basis.	Closed	Agree
3.	FY 2018 FISMA audit recommendation No. 7: EAC to implement a remediation plan to commit resources to update all EAC-wide information security policies and procedures on the frequency required by NIST SP 800-53, Rev. 4.	Closed	Agree
4.	FY 2019 FISMA audit recommendation No. 4: We recommend EAC OIT develop an annual specialized training schedule that identifies individuals who need training. The training program should include training objectives, specific appropriate training to ensure IT staff gains specific knowledge, skills, and abilities required to perform tasks in their work role.	Closed	Agree
5.	FY 2019 FISMA audit recommendation No. 5: We recommend EAC OIT track the training schedule to ensure individuals receive assigned training according to the agency's policy.	Closed	Agree
6.	FY 2020 FISMA audit recommendation No. 1: We recommend EAC OIT prepare an authorization package for its Microsoft Azure system that includes a security and privacy plan, security and privacy assessment report, plans of action and milestones, and an executive summary.	Closed	Agree
7.	FY 2020 FISMA audit recommendation No. 2: We recommend EAC OIT ensure Data Owners sign user access recertifications.	Open	Agree

⁴ The *Election Assistance Commission's Compliance with the Federal Information Security Modernization Act of 2014* (EAC IG Report No. I-PA-EAC-02-18, November, 2018).

⁵ The *Election Assistance Commission's Compliance with the Federal Information Security Modernization Act of 2014* (EAC IG Report No. I-PA-EAC-02-19, December 9, 2019).

⁶ The *Election Assistance Commission's Compliance with the Federal Information Security Modernization Act of 2014* (EAC IG Report No. I-PA-EAC-02-20, December 14, 2020).

APPENDIX II

No.	FY 2018 ⁴ , 2019 ⁵ , 2020 ⁶ Audit Recommendations	Status	Auditor's Position on Status
8.	FY 2020 FISMA audit recommendation No. 3: We recommend EAC OIT implement DMARC policy and HSTS security controls required by DHS Binding Operational Directive 18-01.	Closed	Agree
9.	FY 2020 FISMA audit recommendation No. 4: We recommend EAC OIT reconcile its physical inventory to its inventory system report and update inventory records for separated employees to reflect the EAC operating environment accurately.	Closed	Agree
10.	FY 2020 FISMA audit recommendation No. 5: We recommend EAC OIT prepare performance metrics that measure the effectiveness or efficiency of its information security program and security controls the EAC employs in support of its programs.	Closed	Agree

Appendix III - Acronyms

Acronyms	
CIS	Center for Internet Security
CM	Configuration Management
DHS	U.S. Department of Homeland Security
DMARC	Domain-based Message Authentication, Reporting and Conformance
EAC	Election Assistance Commission
ERM	Enterprise Risk Management
FAR	Federal Acquisition Regulation
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAO	Government Accountability Office
HTTP	Hypertext Transfer Protocol
HSTS	Strict Transport Security
IG	Inspector General
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OIT	Office of Information Technology
OMB	U.S. Office of Management and Budget
POA&M	Plan of Actions and Milestones
REV	Revision
SA&A	Security Assessment and Authorization
SCAP	Security Content Automation Protocol
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team

Appendix IV – Management’s Comments



U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

TO: Deputy Inspector General (EAC) Mia Forgy
FROM: Jessica Bowers, CIO/CISO
DATE: October 29, 2021
SUBJECT: Response to Draft FISMA Audit Report FY2021

1. Finding: EAC OIT needs to improve its configuration management practices

Recommendation 1:

We recommend EAC OIT perform Security Content Automation Protocol (SCAP) scanning to identify vulnerabilities in all systems on the network to assess both code-based and configuration-based vulnerabilities as required by Office of Management and Budget (OMB).

Management Response: Agree

The EAC will adjust its current automated vulnerability scanning to utilize SCAP to identify vulnerabilities in all systems on the network. While we believe our current scanning is comprehensive, we agree that there is value in utilizing a standards-based approach.

Recommendation 2:

We recommend EAC OIT ensure its Windows 10 devices comply with its Center for Internet Security (CIS) security benchmarks as required by its system security plan.

Management Response: Agree

The EAC will ensure that its baseline Windows 10 configurations fully comply with the CIS security benchmarks. While full compliance has been our goal, we understand that have not yet achieved full compliance as we have a number of older laptops running Windows 10 that are being replaced with newer equipment implementing the benchmark. This roll out has been delayed due to staffing resources and ongoing COVID-19 restrictions.



U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

Recommendation 3:

We recommend EAC OIT implement software patches in its information systems in a timely manner and process patches through its change control process as required by its system security plan.

Management Response: Agree

While the EAC has been working through a backlog of vulnerability mitigations, we understand that we need to resolve critical vulnerabilities in a much timelier manner. Management has instructed IT personnel to resolve all critical vulnerabilities within 14 days of their appearance and to prioritize older vulnerabilities that may currently exist.

2. Finding: EAC needs to develop and implement a supply chain risk management (SCRM) strategy, policies, and procedures

Recommendation 4:

We recommend EAC develop and implement a supply chain risk management strategy that aligns with NIST and as required by OMB.

Management Response: Agree

The EAC cybersecurity framework policy defines our supply chain risk management strategy; however, there are documents referenced in this policy that have not yet been updated with the necessary SCRM controls.

Recommendation 5:

We recommend EAC develop and implement an anti-counterfeit policy and procedures that include detecting and preventing counterfeit components from entering the system.

Management Response: Partially disagree

The EAC's systems run in a FedRAMP approved cloud environment and inherit that platform's robust anti-counterfeit policies and procedures. The EAC has reviewed the controls in place for this platform as part of its ATO process. Additionally, the EAC makes use of 3rd party SaaS offerings that are also FedRAMP approved or otherwise reviewed for counterfeit protection during the EAC's ATO process. ATOs for non-FedRAMP systems are detailed in PBC015 – EAC-OCIO-014 Assessment, Authorization, and Monitoring policy.



U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

Hardware is purchased mostly through GSA-approved vendors with anti-counterfeit language contained in the contracts.

Recommendation 6:

We recommend EAC provide training for the OIT staff to detect counterfeit system components (including hardware, software, and firmware).

Management Response: Agree

As mentioned in the response to recommendation 5 above, the EAC inherits anti-counterfeit controls from its providers. Staff is trained in procuring hardware from trusted sources and we will add additional training in identifying counterfeit hardware, software, and firmware, where applicable.

3. Finding: EAC OIT needs to update its Plan of Action and Milestones (POA&M) to meet OMB requirements.

Recommendation 7:

We recommend EAC OIT update its POA&M workbook to include all known weaknesses and add the appropriate level of detail required as instructed by OMB.

Management Response: Partially agree

The EAC POA&M workbook includes all known weaknesses and records additional details for each. The workbook falls short in not listing vulnerability sources, assigned resources, or other detail required by OMB and will be tracking this additional information.

Sincerely,

A handwritten signature in black ink that reads "Jessica Bowers". The signature is written in a cursive style.

Jessica Bowers
CIO/CISO
U.S. Election Assistance Commission

