OFFICE OF INSPECTOR GENERAL

U.S. Election Assistance Commission

AUDIT OF THE U.S. ELECTION ASSISTANCE COMMISSION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT FOR FISCAL YEAR 2024

Report No. P24HQ0052-24-15
September 24, 2024

HIGHLIGHTS

AUDIT OF EAC'S COMPLIANCE WITH FISMA FOR FISCAL YEAR 2024

Report No. P24HQ0052-24-15 September 24, 2024

What Was Audited

The independent public accounting firm of RMA Associates, LLC, under contract with the Office of Inspector General, audited the U.S. Election Assistance Commission's (EAC) information security program for fiscal year 2024 in support of the Federal Information Security Modernization Act of 2014 (FISMA).

In addition to following up on open recommendations made in prior FISMA audits, the audit included a review of the following areas within EAC's security program:

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

What Was Found

The audit found that EAC generally implemented an effective information security program. The overall maturity level of EAC's program was *Level 4-Managed and Measurable*.

However, weaknesses were identified in EAC's security posture in preserving the confidentiality, integrity, and availability of its information and information systems: (1) EAC did not monitor performance metrics associated with outsourced services; (2) required annual anti-counterfeit training was not provided to staff with supply chain risk management responsibilities; (3) EAC did not meet event logging requirements; (4) EAC did not consistently implement its data breach response plan and conduct annual exercises; (5) EAC did not develop an enterprise-wide information security continuous monitoring strategy and consistently capture lessons learned; and (6) EAC did not identify or utilize an automated mechanism to test its system-level contingency plans.

What Was Recommended

The audit made seven recommendations to improve EAC's security posture. Additionally, three recommendations from prior years remain open.

Based on actions already taken by EAC, recommendation 5 is closed upon report issuance.

U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL

DATE: September 24, 2024

TO: U.S. Election Assistance Commission, Executive Director, Brianna Schletz

FROM: U.S. Election Assistance Commission, Acting Inspector General, Sarah Dreyer

SUBJECT: Audit of the U.S. Election Assistance Commission's Compliance with the Federal Information Security Modernization Act for the Fiscal Year 2024 (Report No. P24HQ0052-24-15)

This memorandum transmits the final report on the U.S. Election Assistance Commission's Compliance with the Federal Information Security Modernization Act (FISMA) for Fiscal Year 2024. The Office of Inspector General contracted RMA Associates, LLC, an independent certified public accounting firm, to conduct the audit. The contract required that the audit be performed in accordance with U.S. generally accepted government auditing standards.

RMA is responsible for the attached auditor's report dated September 9, 2024, and the conclusions expressed therein. While the Office of Inspector General coordinated and monitored RMA's performance under the contract, we did not evaluate their adherence to standards and therefore do not express an opinion on EAC's compliance with FISMA.

The report contains seven recommendations. Recommendation 5 has been addressed and closed. Please keep us informed of the actions taken on the open recommendations, as we will track the status of their implementation.

We appreciate the assistance you and your staff provided to us during this audit.

cc: Commissioner Benjamin W. Hovland, Chair
Commissioner Donald L. Palmer, Vice Chair
Commissioner Thomas Hicks
Commissioner Christy McCormick

RMA Associates

Auditors. Consultants. Advisors.

Election Assistance Commission (EAC)

Federal Information Security Modernization Act of 2014 (FISMA)

Final Report

Fiscal Year 2024

RMA | Associates
Auditors. Consultants. Advisors.

September 09, 2024

Ms. Sarah Dreyer
Acting Inspector General
United States Election Assistance Commission
Office of the Inspector General
633 3rd Street NW, Suite 200
Washington, D.C. 20001

Dear Ms. Dreyer:

RMA Associates, LLC, is pleased to present our report on Election Assistance Commission (EAC) compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024.

Thank you for the opportunity to serve your organization and the assistance provided by your staff and EAC. We will be happy to answer any questions you may have concerning the report.

Respectfully,

Reza Mahbod

Reza Mahbod, CPA, CISA, CFE, CGFM, CICA, CGMA, CDFM, CDPSE
President
RMA Associates, LLC

RMA | Associates
Auditors. Consultants. Advisors.

Inspector General
United States Election Assistance Commission
Washington, D.C. September 09, 2024

RMA Associates, LLC, conducted a performance audit of the Election Assistance Commission (EAC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). The objective of this performance audit was to determine whether EAC implemented an effective information security program. The scope of this audit was to assess EAC's information security program, which is consistent with FISMA, and reporting instructions issued by the Office of Management and Budget and the Department of Homeland Security. The audit included tests of management, technical, and operational controls outlined in the National Institute of Standards and Technology Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, updated September 2020.

For this audit, we reviewed three judgmentally selected systems in EAC's inventory as of March 6, 2024. Audit fieldwork covered EAC's headquarters located in Washington, D.C., from October 1, 2023, to May 29, 2024.

Our audit was performed in accordance with *Generally Accepted Government Auditing Standards*, as specified in 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We concluded that EAC implemented an effective information security program. However, we found weaknesses in EAC's security posture in preserving the agency's information and information systems' confidentiality, integrity, and availability. Consequently, we noted weaknesses in five of the domains. Therefore, we made seven recommendations to assist EAC in strengthening its information security program.

Additional information on our findings and recommendations are included in the accompanying report.

Respectfully,

RMA Associates

RMA Associates LLC

Contents

Summary of Results

Background

The United States Agency for the Election Assistance Commission (EAC) Office of Inspector General engaged RMA Associates, LLC (RMA) to conduct an audit in support of the Federal Information Security Modernization Act of 2014[1] (FISMA) requirement for an evaluation of the Election Assistance Commission (EAC) information security program for fiscal year (FY) 2024. The audit objective of this performance audit was to determine whether EAC implemented an effective information security program.[2]

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other sources.

The statute also provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires agency heads to ensure (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes.

FISMA also requires the agency's Inspector General (IG) to assess the effectiveness of agency information security programs and practices and report the results of the assessments to the Office of Management and Budget (OMB).

Annually, OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) provide instructions to Federal agencies and IGs for assessing agency information security programs. The FY 2024 metrics are designed to assess the maturity[3] of an information security program and align with the five functional areas in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, Version 1.1: Identify, Protect, Detect, Respond, and Recover as highlighted in Table 1.

---

[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 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

[2] For this audit, an effective information security program is defined as having an overall mature program based on the current year Inspector General FISMA reporting metrics.

[3] The five maturity models include: Level 1 - Ad hoc; Level 2 - Defined; Level 3 - Consistently Implemented; Level 4 - Managed and Measurable; and Level 5 - Optimized.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2024 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2024 IG FISMA Metric Domains
Identify	Risk Management and Supply Chain Risk Management (SCRM)
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

This 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 objective. RMA believes the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Audit Results

The audit concluded that EAC generally implemented an effective information security program. For example, EAC:

- Maintained an effective process for assessing the risk associated with positions involving information system duties.
- Maintained an accurate inventory of hardware and software assets.
- Implemented an enterprise-wide single sign-on solution. All systems interfaced with the solution, resulting in an ability to centrally manage user (privileged) accounts and privileges and report on effectiveness on a near real-time basis.
- Provided its personnel with awareness and specialized training that produced a demonstratable improvement in phishing exercises.

As shown in Table 2, the overall maturity level of EAC' ‘s information security program was Managed and Measurable (Effective).

Table 2: FY 2024 EAC Maturity Levels

Cybersecurity Framework Security Functions	Core Metrics	Supplemental Metrics	Assessed Maturity Levels
Identify	Not Effective	Effective	Consistently Implemented
Protect	Effective	Effective	Managed and Measurable
Detect	Not Effective	Not Effective	Defined
Respond	Not Effective	Effective	Consistently Implemented
Recover	Effective	Effective	Managed and Measurable
Overall	Not Effective	Not Effective	**Managed and Measurable**

However, weaknesses were identified in EAC's security posture in preserving the confidentiality, integrity, and availability of its information and information systems. Six of the nine IG FISMA metric domains had weaknesses (Table 3).

Table 3: Cybersecurity Framework Security Functions Mapped to Deficiencies Noted in FY 2024 FISMA Assessment

Cybersecurity Framework Security Functions	FY 2024 IG FISMA Metric Domains	Weakness Noted in FY 2024
Identify	Risk Management	None
Identify	Supply Chain Risk Management (SCRM)	EAC Did Not Identify and Monitor the Performance Metrics Associated with Outsourced Services (Finding 1) EAC Needs to Provide Component Authenticity/Anti-counterfeit Training for Designated Personnel Annually (Finding 2)
Protect	Configuration Management	None
Protect	Identity and Access Management	EAC Needs to Implement Event Logging Requirements (Finding 3)

Cybersecurity Framework Security Functions	FY 2024 IG FISMA Metric Domains	Weakness Noted in FY 2024
Protect	Data Protection and Privacy	EAC Needs to Conduct an Annual Data Exfiltration and Table-top Exercise (Finding 4)
Protect	Security Training	None
Detect	Information Security Continuous Monitoring	EAC Needs to Develop an Organization-wide Continuous Monitoring Strategy and Consistently Capture Lessons Learned to make improvements to its ISCM policies and strategy (Finding 5)
Respond	Incident Response	EAC Needs to Implement Event Logging Requirements (Finding 3)
Recover	Contingency Planning	EAC Did Not Employ an Automated Mechanism to test System Contingency Plans more Thoroughly and Effectively (Finding 6)

We are making seven new recommendations in addition to the three prior FISMA audit recommendations that EAC has not yet taken final action on. (See the "Audit Findings" section.) Appendix II illustrates that EAC took final corrective actions on six of nine prior FISMA audit recommendations. EAC officials explained that competing priorities within their information security program were the main challenges faced by the agency toward addressing the remaining three recommendations.

Audit Findings

1. EAC Did Not Monitor the Performance Metrics Associated with Outsourced Services.

Cybersecurity Framework Security Function: *Identify*
FY24 IG FISMA Metric Domain: *Supply Chain Risk Management*

EAC did not monitor qualitative and quantitative performance metrics to measure the performance of third-party services. No formal reporting was completed on behalf of EAC to monitor the information security and SCRM performance of organizationally defined products, systems, and services that external providers provided. EAC also did not incorporate supplier risk evaluations based on criticality into continuous monitoring practices to maintain situational awareness of the supply chain risks.

NIST SP 800-53, Revision 5*, Security and Privacy Controls for Information Systems and Organizations* states:

SR-6 Supplier Assessments and Reviews

Control: The organization must: Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].

In addition, CIS Top 18 Security Controls: Control 15: *Service Provider Management* states:

15.6 Monitor Service Providers

> Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.

According to EAC, officials leveraged the documentation provided within the FedRAMP secure repository as a key element of the Authority to Operate (ATO) and based on the documentation within the repository. Although the documentation covers the FedRAMP systems, EAC has not implemented the requirements to assess and review SCRM risks for non-FedRAMP systems. As a result, we are making the following recommendation.

Recommendation 1: *We recommend that the Chief Information Security Officer identify qualitative and quantitative metrics on service level agreements held with third parties, then perform an analysis with monthly reporting received from those third parties to identify metrics that can be measured and documented, on either a monthly or quarterly basis, to ensure that EAC is receiving all contracted services.*

Recommendation 2*: We recommend that the Chief Information Security Officer develop and implement procedures to leverage the Repository for Software Attestation and Artifacts to obtain sufficient assurance that the security and supply chain controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements.*

2. EAC Needs to Provide an Annual Component Authenticity/Anti-counterfeit Training for IT Staff with SCRM Responsibilities.

Cybersecurity Framework Security Function: *Identify*
FY24 IG FISMA Metric Domain: *Supply Chain Risk Management*

EAC did not perform Annual Component Authenticity Anti-Counterfeit Training as required by NIST 800-53 Rev 5 controls SR-11(1).

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* states:

SR-11 (1) Component Authenticity – Anti-Counterfeit Training

> Control: Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).

In addition, EAC's Supply Chain Risk Management Policy (December 2023) states:

SR-11 (1) Component Authenticity – Anti-Counterfeit Training

> The EAC Provides annual training to OCIO and SCRM Team members on the detection of counterfeit systems and components.

Officials last completed Anti-Counterfeit Training that covered counterfeit prevention, the impact of counterfeit items, eliminating counterfeit, avoidance strategies, detecting warning flags for counterfeit components, mitigation actions, protecting the supply chain, and communication if a counterfeit product/system is detected in July 2022. Therefore, EAC may be susceptible to cybersecurity threats, data breaches, and non-compliance with regulations. As a result, we are making the following recommendation.

Recommendation 3: *We recommend that the Chief Information Security Officer provide annual Anti-Counterfeit Training for IT staff with SCRM responsibilities.*

3. EAC Needs to Implement Event Logging Requirements.

Cybersecurity Framework Security Function: *Respond*
FY24 IG FISMA Metric Domain: *Identity and Access Management & Incident Response*

The EAC did not meet the Event Logging (EL) requirements at the EL2 (intermediate) maturity level, as stipulated by M-21-31. The EAC was required to reach EL2 maturity within 18 months of the memorandum issued on August 27, 2021. However, as of May 25, 2024, 33 months after the issuance, the EAC remained at the EL1 (basic) maturity level. Furthermore, the memorandum set an August 2023 deadline for adherence to EL3 (advanced) requirements, which the EAC also did not meet.

OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021) states:

> Section I: Maturity Model for Event Log Management
>
> Tier EL2, Rating – Intermediate
>
> The agency and all of its components meet the following requirements, as detailed in Table 3 (EL2 Intermediate Requirements) within Appendix A (Implementation and Centralized Access Requirements):
>
> - Meeting EL1 maturity level
> - Intermediate Logging Categories
> - Publication of Standardized Log Structure
> - Inspection of Encrypted Data
> - Intermediate Centralized Access
>
> Section II: Agency Implementation Requirements
>
> Agencies must immediately begin efforts to increase performance in accordance with the requirements of this memorandum. Specifically, agencies must:
>
> […]
>
> Within 18 months of the date of this memorandum, achieve EL2 maturity.
>
> Within two years of the date of this memorandum, achieve EL3 maturity.
>
> Appendix B: EL2 Intermediate Requirements – Inspection of Encrypted Data

> Federal agencies shall retain and store in clear text form the data or Encrypted Data metadata from Appendix C that is collected in their environment. If agencies perform full traffic inspection through active proxies, they should log additional available fields as described in Appendix C and can work with CISA to implement these capabilities. If agencies do not perform full traffic inspection, they should log the metadata available to them. In general, agencies are expected to follow zero-trust principles concerning least privilege and reduced attack surface, and relevant guidance from OMB and CISA relating to zero-trust architecture.

According to EAC officials, system limitations prevented EAC from logging metadata, not allowing it to perform full traffic inspections to meet the Inspection of Encrypted Data requirement set forth by OMB M-21-31.

By not meeting the Inspection of Encrypted Data requirement for maturity EL2 (intermediate), EAC did not follow the zero-trust principle concerning least privilege or reduce the attack surface that could be exploited in a cyberattack scenario.

Recommendation 4: *We recommend that the Election Assistance Commission's Chief Information Officer implement EL3 logging requirements in accordance with Office of Management and Budget memorandum M-21-31.*

4. EAC Needs to Conduct Annual Data Exfiltration and Table Exercises

Cybersecurity Framework Security Function: *Protect*
FY24 IG FISMA Metric Domain: *Data Protection and Privacy*

EAC did not consistently implement its Data Breach Response plan. Additionally, the Breach Response team did not participate in a table-top exercise or use lessons learned to improve the plan as appropriate. Also, EAC did not conduct an annual exfiltration exercise to measure the effectiveness of its data exfiltration and enhanced network defenses.

OMB M-17-12: *Preparing for and Responding to a Breach of Personally Identifiable Information* states:

X. Table-top Exercises and Annual Plan Reviews

A. Table-top Exercises

The Senior Agency Official Privacy (SAOP) shall periodically, but not less than annually, convene the agency's breach response team to hold a table-top exercise. The purpose of the table-top exercise is to test the breach response plan and to help ensure that members of the team are familiar with the plan and understand their specific roles. Testing breach

response plans is an essential part of risk management and breach response preparation. Table-top exercises should be used to practice a coordinated response to a breach, to further refine and validate the breach response plan, and to identify potential weaknesses in an agency's response capabilities.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* states:

SC-7 (10) BOUNDARY PROTECTION | PREVENT EXFILTRATION

(a) Prevent the exfiltration of information; and

(b) Conduct exfiltration tests [Assignment: organization-defined frequency].

FY 2023-2024 IG FISMA Reporting Metrics (February 2023), Question 37, Managed and Measurable:

The organization also conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses.

FY 2023-2024 IG FISMA Reporting Metrics (February 2023), Question 38, Consistently Implemented:

The organization consistently implements its Data Breach Response plan. Additionally, the breach response team participates in table-top exercises and uses lessons learned to make improvements to the plan as appropriate.

EAC did not conduct a Table-top/Data Exfiltration for FY24. By not performing a table-top/data exfiltration exercise for the data breach, EAC may not be prepared to react to a data breach, and there is an increased risk to confidentiality, integrity, and availability of information may be comprised.

Recommendation 5: *We recommend that the Election Assistance Commission's Chief Information Officer perform the breach table-top exercises annually which includes a data-exfiltration exercise.*

5. EAC Needs to Develop an Organization-wide Continuous Monitoring Strategy and Consistently Capture Lessons Learned to Make Improvements to Its ISCM Policies and Strategy.

Cybersecurity Framework Security Function: *Detect*
FY24 IG FISMA Metric Domain: *Information Security Continuous Monitoring*

The EAC did not develop an enterprise-wide Information Security Continuous Monitoring (ISCM) Strategy. Instead, it used the Enterprise Risk Management Strategy and Cybersecurity Framework as an ISCM strategy, which lacked detailed metrics for monitoring. Additionally, there was no ongoing process for learning lessons to improve the ISCM strategy.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* states:

PM-31 CONTINUOUS MONITORING STRATEGY

Control: Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include:

a. Establishing the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics];
b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;
c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy;
d. Correlation and analysis of information generated by control assessments and monitoring;
e. Response actions to address results of the analysis of control assessment and monitoring information; and
f. Reporting the security and privacy status of organizational systems to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

NIST SP 800-37 Revision 2 *Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy* states:

> […] to incorporate lessons learned as continuous monitoring and ongoing authorization processes are implemented for moderate impact and high-impact systems. Incorporating lessons learned facilitates the consistent progression of the continuous monitoring and ongoing authorization implementation from the lowest to the highest impact levels for the systems within the organization.

EAC's Assessment. Authorization, and Monitoring Policy, Version 1.3, dated September 1, 2022, states that:

CA-7 Continuous Monitoring

The EAC develops a continuous monitoring strategy and implements a continuous monitoring strategy that includes:

a. Establishes metrics as defined in OMB memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems, November 18, 2013, and NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011 to be monitored.
b. Establishes continuous monitoring through CISA CDM and Qualys and annually assesses control effectiveness.
c. Ongoing control assessments in accordance with CISA CDM.
d. Ongoing monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.
e. Correlation and analysis of security-related information generated by assessments and monitoring.
f. Response actions to address results of the analysis of security-related information.

EAC did not have a specific continuous monitoring strategy. Without an ISCM strategy, it increases the risk that EAC is vulnerable to the escalating threats of vulnerabilities, and attack vectors may not be adequately accounted for in an outdated plan, leaving EAC vulnerable to cyberattacks and data breaches. In addition, without a formal, disciplined lesson-learned process, EAC may not capture information from previous practice, and actual risk events lose the opportunity to strengthen EAC's security posture.

Recommendation 6: *We recommend that the Election Assistance Commission's Chief Information Officer establish and implement a formal Information Security Continuous Monitoring Strategy and an effective monitoring mechanism to track the progress of ongoing lessons learned.*

6. EAC Did Not Employ an Automated Mechanism to Test System Contingency Plans More Thoroughly and Effectively.

Cybersecurity Framework Security Function: *Recover*
FY24 IG FISMA Metric Domain: *Contingency Planning*

EAC did not identify or utilize an automated mechanism to test its system-level contingency plans. Although EAC leveraged FedRAMP to employ automated mechanisms for two of its systems, it does not absolve its responsibility for its internal systems.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* states:

CP-4 (3) CONTINGENCY PLAN TESTING - AUTOMATED TESTING

Control: Test the contingency plan using [Assignment: organization-defined automated mechanisms].

Recommendation 7: *We recommend that the Election Assistance Commission's Chief Information Officer identify and employ an automated notification mechanism to test its system level contingency plans thoroughly and effectively.*

Evaluation of Management Comments

In response to the draft report, EAC outlined its plan to address recommendations 1 through 7. EAC's comments are included in their entirety in Appendix III. Based on the evaluation of management comments, we acknowledge management's decisions on recommendations 1 through 7. Subsequently, management provided evidence of an FY24 Data Exfiltration Table-Top exercise that occurred on August 22nd, 2024. As a result, recommendation 5 has been addressed and is deemed closed.

Appendix I – Scope and Methodology

Scope

RMA conducted this audit in accordance with Generally Accepted Government Auditing Standards, as specified in the Government Accountability Office *Government Auditing Standards*. These 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Our audit was conducted for FY 2024 and tested the core and supplemental metrics identified in the *FY 2023 - 2024 IG FISMA Reporting Metrics* issued by OMB and CIGIE.

The scope of this audit was to assess EAC's information security program, which is consistent with FISMA, and reporting instructions issued by OMB and the CIGIE. In addition, the audit included tests of management, technical, and operational controls outlined in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations.* We assessed EAC's performance and compliance with FISMA in the following control areas:

- Risk Management
- Supply Chain Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Awareness Training
- Information System Continuous Monitoring
- Incident Response
- Contingency Planning

We conducted a risk assessment to identify a representative number of systems (a minimum of one internal and two external) to be tested when needed for system-level testing. Only moderate systems were selected for FY 2024. Three systems were selected for FY 2024 in EAC's current system inventory as of March 6, 2024, to meet the requirement.

For this audit, we reviewed the following three judgmentally selected systems in EAC's inventory as of March 6, 2024:

- Azure
- Microsoft Office 365
- EAC HQ Boundary

The audit also included a follow-up on nine prior audit recommendations[4][5][6] to determine if EAC had made progress in implementing the recommended improvements concerning its information security program. See Appendix II for the status of recommendations for the prior year.

Audit fieldwork was conducted at EAC's headquarters located in Washington, DC, from October 1, 2023 to May 29, 2024.

Methodology

To determine if EAC implemented an effective information security program, RMA conducted interviews with EAC officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. Additionally, RMA reviewed documentation supporting the information security program. These documents included, but were not limited to, EAC's (1) risk management policy, (2) configuration management procedures, (3) identity and access control measures, (4) security awareness training, and (5) continuous monitoring controls. RMA compared documentation against requirements stipulated in NIST special publications. Also, RMA performed tests of information system controls, including a vulnerability assessment, to determine the effectiveness of those controls. Furthermore, RMA reviewed the status of FISMA audit recommendations for FYs 2021, 2022, and 2023.

In testing the effectiveness of the security controls, RMA exercised professional judgment in determining the number of items selected for testing and the method used to select them. RMA considered the relative risk and the significance of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity and not the proportion of deficient items found compared to the total population available for review when documenting the results of our testing. Lastly, in some instances, RMA tested judgmental samples rather than the entire audit population. In those cases, the results cannot be projected to the population as that may be misleading.

[4] Recommendation 1 in Fiscal Year 2021 EAC Compliance with the Federal Information Security Modernization Act (Audit Report, I-PA-EAC-04-21, October 29, 2021)

[5] Recommendations 1 and 2 in Audit of the U.S. Election Assistance Commission's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2022 (Audit Report, O22HQ0006-23-02, November 3, 2022)

[6] Recommendations 1-6 in Audit of the U.S. Election Assistance Commission's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2023 (Audit Report, O23HQ0029-23-07, August 9, 2023)

Appendix II - Status of Prior Year Recommendations

The following table provides the status of the FY 2021, 2022, and 2023 FISMA audit recommendations.[7][8][9]

Table 4: Prior Year FISMA Audit Recommendations

Audit Report & Recommendation No.	FY 2021 Audit Recommendations	EAC's Position	Auditor's Position
I-PA-EAC-04-21 (Rec. 1)	We recommend EAC OCIO 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).	Closed	Agree
O22HQ0006-23-02 (Rec. 1)	We recommend EAC OCIO remediate vulnerabilities in the network identified, according to the agency's policy, and document the results or document acceptance of the risks of those vulnerabilities.	Open	Agree
O22HQ0006-23-02 (Rec. 2)	We recommend EAC OCIO develop and implement a flaw remediation plan for vulnerabilities that cannot be remediated within the policy recommended timeframes.	Open	Agree

[7] Recommendation 1 in Fiscal Year 2021 EAC Compliance with the Federal Information Security Modernization Act (Audit Report, I-PA-EAC-04-21, October 29, 2021)

[8] Recommendation 1 and 2 in Audit of the U.S. Election Assistance Commission's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2022 (Audit Report, O22HQ0006-23-02, November 3, 2022)

[9] Recommendation 1-6 in Audit of the U.S. Election Assistance Commission's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2023 (Audit Report, O23HQ0029-23-07, August 9, 2023)

O23HQ0029-23-07 (Rec. 1)	We recommend EAC OCIO resolve conflicting baseline configuration settings for Windows 10 devices and ensure iPhones meet the agency's configuration setting requirements.	Closed	Agree
O23HQ0029-23-07 (Rec. 2)	We recommend EAC OCIO ensure information systems meet STIG's secure configuration settings as required by the agency's policy.	Closed	Agree
O23HQ0029-23-07 (Rec. 3)	We recommend EAC OCIO update its hardware inventory system to include the level of detail needed to manage devices according to Federal requirements and document management's oversight and review.	Closed	Agree
O23HQ0029-23-07 (Rec. 4)	We recommend EAC OCIO update its POA&M procedures and, in coordination with management, develop and maintain POA&M reports based on Federal requirements.	Open	Agree
O23HQ0029-23-07 (Rec. 5)	We recommend EAC OCIO update the agency's SSP document to align with NIST requirements and include the network environment's current state.	Closed	Agree
O23HQ0029-23-07 (Rec. 6)	We recommend EAC OCIO fully implement its GRC solution to manage and monitor cybersecurity risk activities required by NIST SP 800-39 and provide a centralized enterprise-wide view of all risks across the agency.	Closed	Agree

Appendix III – Management Comments

U.S. Election Assistance Commission

633 3rd St. NW, Suite 200

Washington, DC 20001

TO: U.S. Election Assistance Commission, Acting Inspector General, Sarah Dreyer

FROM: U.S. Election Assistance Commission, CIO/CISO, Jessica Bowers

DATE: August 29, 2024

SUBJECT: Response to Draft FISMA Audit Report FY2024

The Office of the Chief Information Officer (OCIO) provides the following responses to the Inspector General's FY2023 FISMA audit findings and recommendations.

1. **EAC did not monitor the performance metrics associated with outsourced services.**

   Management Response: Agree
   The EAC regularly reviews documentation provided by third-party services as part of its Authority to Operate (ATO) program. This commonly involves security review reports, plans of action and milestone documentation, and other artifacts necessary to evaluate the security of these providers. The EAC will add additional monitoring for supply chain risk management and will integrate with the newly created national repository for software attestation and artifacts into its authorization and monitoring processes.

   Estimated completion date: December 13, 2024

2. **EAC needs to provide an annual component authenticity/anti-counterfeit training for IT staff with SCRM responsibilities.**

   Management Response: Agree
   The EAC has developed authenticity/anti-counterfeit training for IT staff with SCRM responsibilities but had not ensured that it recurred on an annual basis. The automated system used for EAC cybersecurity training has been updated to ensure this training occurs on an annual basis and EAC IT personnel have been assigned training for FY24 and completion is in-progress.

   Estimated completion date: September 13, 2024

3. **EAC needs to implement event logging requirements.**

Management Response: Agree
The EAC has experienced logging limitations with its cloud services provider that have not allowed it to achieve EL3 prior to the audit period. The EAC's cloud provider has recently made enhanced logging available to the agency and the EAC is working to integrate the applicable logging to meet the EL3 requirements.

Estimated completion date: May 30, 2025

4. **EAC needs to conduct annual data exfiltration and table exercises.**

Management Response: Agree; completed, recommend closing
The EAC recently completed an agency-wide data exfiltration table-top exercise. Findings from the exercise have been documented and plans are being developed to make improvements to the agency's ability to respond.

Completion date: August 26, 2024

5. **EAC needs to develop an organization-wide continuous monitoring strategy and consistently capture lessons learned to make improvements to its ISCM policies and strategy.**

Management Response: Agree
The EAC will remove outdated references from its plans and add defined organizational metrics and timelines for monitoring control effectiveness to its ISCM policies and strategy documentation and operations.

Estimated completion date: March 14, 2025

6. **EAC did not employ an automated mechanism to test system contingency plans more thoroughly and effectively.**

Management Response: Agree
The EAC is researching system contingency plan testing automation tools to meet this recommendation. Due to limited resources, this may involve defining an automated process within existing EAC automation solutions.

Estimated completion date: July 1, 2025

Appendix IV – Areas of Improvement

1. Consider the Utilization of Additional Cybersecurity Infrastructure Security Agency (CISA) Continuous Diagnostics and Mitigation (CDM) Program Services

   RMA recommends that EAC make considerations for additional services provided free of charge through CISA CDM enrollment. There are benefits to the robust services offered by third-party vendors; however, government-shared services like CISA CDM cater to agencies of the EAC's size and security profile for free of charge.

2. Performance of a Workforce Assessment to Identify Specialized Training Needs

   RMA recommends that EAC perform a workforce assessment that more closely mirrors the required skills needed to utilize IT tools in specialized roles. During the assessment, it was noted that soft skill training took precedence over the more technical training tied to specific IT Tools and the readily identifiable skill gaps for IT staff.

Visit our website at **oig.eac.gov**.

U.S. Election Assistance Commission
Office of Inspector General
633 3rd Street, NW, Second Floor
Washington, DC 20001

Report Waste, Fraud, and Abuse

eacoig@eac.gov | Online Complaint Form