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 2023

Report No. O23HQ0029-23-07
August 9, 2023

HIGHLIGHTS

AUDIT OF EAC'S COMPLIANCE WITH FISMA FOR FISCAL YEAR 2023

Report No. O23HQ0029-23-07 August 9, 2023

What OIG Audited

The Office of Inspector General (OIG), through the independent public accounting firm of Brown & Company Certified Public Accountants and Management Consultants, PLLC, audited the U.S. Election Assistance Commission's (EAC's) information security program for fiscal year 2023 in support of the Federal Information Security Modernization Act of 2014 (FISMA). The objective was to determine whether EAC implemented selected security controls for certain information systems in support of 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 Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Training
- Information Security Continuous Monitoring
- Incident Response
- Contingency Planning

What OIG Found

OIG found that EAC generally complied with FISMA requirements by implementing selected security controls for tested systems. EAC received an overall *Level 4-Managed and Measurable* maturity level, which reflects an effective information security program.

However, the EAC Office of the Chief Information Officer did not: (1) consistently resolve known vulnerabilities; (2) meet configuration requirements; (3) have a hardware inventory with the level of detail needed; (4) have a comprehensive plan of action and milestone report; (5) update its system security and privacy plan; and (6) fully implement its governance, risk and compliance solution.

What OIG Recommended

OIG made six recommendations:

1. Resolve conflicting settings for Windows 10 devices and ensure iPhones meet EAC configuration requirements.
2. Ensure information systems meet standard secure configuration settings per EAC policy.
3. Update the hardware inventory system to meet federal requirements and document management's oversight and review.
4. Develop and maintain, in coordination with management, a Plan of Action and Milestones report based on federal requirements.
5. Update its system security and privacy plan to align with NIST requirements and include the network environment's current state.
6. Implement its governance, risk and compliance solution to monitor cybersecurity risk activities and provide a centralized enterprise-wide view of risk across EAC.

Additionally, three recommendations from prior years remain open.

OFFICE OF INSPECTOR GENERAL

U.S. Election Assistance Commission

DATE: August 9, 2023

TO: U.S. Election Assistance Commission, Executive Director, Steven Frid

FROM: U.S. Election Assistance Commission, Inspector General, Brianna Schletz

SUBJECT: Audit of the U.S. Election Assistance Commission's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2023 (Report No. O23HQ0029-23-07)

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 2023. The Office of Inspector General contracted Brown & Company, PLLC, 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. We monitored the firm's work to ensure that it adhered to those standards.

Please keep us informed of the actions taken on the report's six recommendations, as well as the three recommendations that remain open from prior years, 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 Christy McCormick, Chair
Commissioner Benjamin W. Hovland, Vice Chair
Commissioner Donald L. Palmer
Commissioner Thomas Hicks

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

Fiscal Year 2023
July 27, 2023

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. Brianna Schletz
Inspector General
U.S. Election Assistance Commission
Office of the Inspector General
Washington, DC

Dear Ms. Schletz:

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, Brown & Company CPAs and Management Consultants, PLLC (Brown & Company), to conduct the audit in support of the FISMA requirement for an annual evaluation of the EAC Office of Chief Information Officer (OCIO) information security program.

The objective of this performance audit was to determine whether EAC OCIO 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 (NIST) Special Publication (SP) 800-53, Revision (Rev) 5.1, *Security and Privacy Controls for Information Systems and Organizations.*

We reviewed selected controls from EAC's general support system for this audit. The selected controls included 20 Core and 20 Supplemental Inspector General FISMA Reporting Metrics in five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of the agency's information security program and the maturity level of each function area. The audit also included a review of vulnerability assessments on internal and external systems and an evaluation of the EAC OCIO process to identify and mitigate information systems vulnerabilities. Audit fieldwork was performed at Brown & Company in Greenbelt, Maryland, and EAC's headquarters in Washington, DC, from March 30, 2023, through July 6, 2023.

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 OCIO generally complied with FISMA requirements by implementing selected security controls for tested systems. EAC OCIO generally had policies for its information security program Its implementation of those policies for selected controls was effective.

We found EAC's selected controls effective. However, we are reporting six findings and making six recommendations to assist EAC OCIO in strengthening its information security program. There are three recommendations from prior years that were not 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
July 27, 2023

Table of Contents

Summary of Results....1

Audit Results....3

Audit Findings....4

1. EAC OCIO Needs to Consistently Resolve Known Vulnerabilities....4
2. EAC OCIO Needs to Improve Its Configuration Procedures....5
3. EAC OCIO Needs to Maintain Hardware Inventory Records According to Federal Requirements....6
4. EAC OCIO Needs to Develop Plan of Action and Milestone (POA&M) Reports According to Federal Requirements....7
5. EAC OCIO Needs to Update the System Security and Privacy Plan (SSP) in Accordance with NIST....8
6. EAC OCIO Needs to Implement its Governance, Risk and Compliance (GRC) Solution to Manage Risk....8

Appendix I – Scope, Methodology and Criteria....10

Appendix II – Status of Prior Years Audit Recommendations....13

Appendix III - Acronyms....14

Appendix IV – Management's Comments....15

Summary of Results

The Federal Information Security Modernization Act of 2014[1] (FISMA), requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems[2], 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 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 the Election Assistance Commission (EAC) Office of Chief Information Officer (OCIO) information security program. This performance audit's objective was to determine whether EAC OCIO 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

The audit concluded that EAC OCIO generally complied with FISMA requirements by implementing selected security controls for tested systems. EAC OCIO generally had policies for its information security program, and its implementation of those policies for selected controls was effective.

We found EAC's selected controls effective and operating as intended. However, we are reporting six findings and making six recommendations to assist EAC OCIO in strengthening its information security program. Specifically, EAC OCIO needs to:

1. Consistently Resolve Known Vulnerabilities
2. Improve Configuration Procedures
3. Maintain Hardware Inventory Records According to Federal Requirements
4. Develop a Plan of Action and Milestone (POA&M) Reports According for Federal Requirements
5. Update the System Security and Privacy Plan (SSP) in Accordance with NIST
6. Implement Its Governance, Risk and Compliance (GRC) Solution to Manage Risk

As illustrated in Appendix II, there are three recommendations from prior years that were not fully implemented. Detailed findings appear in the following section.

Audit Results

We concluded that EAC implemented effective information security policies, procedures and practices, receiving an overall Level 4 – Managed and Measurable maturity level, and therefore the EAC information security program is effective. To be considered effective, EAC's information security program must be rated Managed and Measurable (Level 4).

Table-1 below details the five maturity model levels: ad hoc, defined, consistently implemented, managed and measurable, and optimized.

Table-1 Assessment Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable *	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.
	* Within the context of the maturity model, OMB believes that achieving a Level 4 (managed and measurable) or above represents an effective level of security.

Table-2 below summarizes the overall assessed maturity levels for each function area and domain in the Fiscal Year (FY) 2023 Inspector General FISMA Reporting Metrics. Three out of five functions met the managed and measurable level, with two consistently implemented.

Table-2 Summary of Overall Calculated Average Maturity Levels

Function and Domain Areas	FY 23 Core and Supplemental FISMA Maturity Levels
Identify: Risk Management and Supply Chain Risk Management	Consistently Implemented (Level 3)
Protect: Configuration Management, Identity and Access Management, Data Protection & Privacy, and Security Training	Managed and Measurable (Level 4)
Detect: Information Security Continuous Monitoring	Consistently Implemented (Level 3)
Respond: Incident Response	Managed and Measurable (Level 4)
Recover: Contingency Planning	Managed and Measurable (Level 4)
Overall Effectiveness Rating - Effective	**Managed and Measurable (Level 4)**

Audit Findings

1. EAC OCIO Needs to Consistently Resolve Known Vulnerabilities.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev) 5.1, RA-5 “Vulnerability Monitoring and Scanning”, requires organizations to remediate legitimate vulnerabilities based on the organization-defined response times and in accordance with an organizational assessment of risk.

Also, NIST SP 800-53 Rev. 5.1, System and Information Integrity (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.

The vulnerability assessment is an automated assessment of Internet or intranet connected assets, including firewalls, routers, web and mail servers and other hosts residing within the provided IP address range. On April 10, 2023, Brown & Company conducted an independent internal vulnerability scan on EAC’s network for 17 selected IP addresses and confirmed 18 unique vulnerabilities: 1 “Urgent,” 2 “Critical,” 5 “Serious,” and 10 “Medium” risk vulnerabilities related to patch and configuration management. The 18 vulnerabilities were not resolved within the agency’s policies and procedure timeframes.

EAC OCIO runs vulnerability scans continuously (e.g., every 72 hours); however, flaw remediation controls were not consistently implemented to remediate known vulnerabilities due to a lack of a remediation plan.

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

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

No new recommendations are being made to remediate vulnerabilities in the network identified and develop and implement a flaw remediation plan for vulnerabilities because recommendations 1 and 2 from the FY 22 FISMA audit are substantially similar and open. See Appendix II.

2. EAC OCIO Needs to Improve Its Configuration Procedures.

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. 5.1, Configuration Management (CM)-6 “Configuration Setting”, requires organizations to monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

The EAC OCIO Configuration Management Policy requires EAC OCIO to establish mandatory configuration settings using standards such as Standard Technical Implementation Guides (STIGs). The Configuration Management Policy also requires EAC OCIO to conduct SCAP scans to monitor and control configuration settings.

The Microsoft Intune EAC Endpoint Security report, dated May 11, 2023, showed 176 conflicting configuration settings for BitLocker for Windows 10 devices. "Conflict" means there's an existing setting on the device(s) that Intune can't override, or two policies were deployed with the same setting using different values. The Microsoft Mobile Device authorization report showed 59 out of 122 iPhones did not meet configuration requirements.

We also noted that the U.S. Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA) dashboard report for EAC showed STIGs security settings were not consistently applied. The EAC STIGs report, dated May 11, 2023, showed 29 out of 405 misconfigurations, which consists of 15 out of 210 misconfigurations for the EAC Azure environment and 14 out of 195 misconfigurations for the EAC Headquarters' environment.

Starting in March 2020, a remote working environment was imposed on the agency, limiting the EAC OCIO's ability to conduct SCAP scanning for all devices, specifically remote devices. EAC OCIO has a SCAP-enabled tool; however, the tool can only scan devices directly connected to the EAC network and cannot scan EAC's remote devices (e.g., laptops and workstations located outside of the EAC office). Therefore, EAC OCIO did not perform a SCAP scan for FY 23.

EAC OCIO does not have adequate policies and procedures to ensure configuration management settings are fully implemented.

EAC OCIO information systems face an increased risk of being compromised if baseline configuration settings are not deployed and maintained in accordance with the agency’s configuration management policy.

Recommendation 1:
We recommend EAC OCIO resolve conflicting baseline configuration settings for Windows 10 devices and ensure iPhones meet the agency’s configuration setting requirements.

Auditor’s Evaluation of Management’s Response:
EAC’s management concurred with this recommendation. Management’s full response is provided in Appendix IV.

Recommendation 2:
We recommend EAC OCIO ensure information systems meet STIGs secure configuration settings as required by the agency's policy.

Auditor's Evaluation of Management's Response:
EAC's management concurred with this recommendation. Management's full response is provided in Appendix IV.

No new recommendation is being made for SCAP scanning because recommendation 1 from the FY 21 FISMA audit is substantially similar and open. See Appendix II.

3. EAC OCIO Needs to Maintain Hardware Inventory Records According to Federal Requirements.

The NIST SP 800-53, Rev. 5.1, CM-8 "System Component Inventory", requires organizations to ensure that inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and networked components or devices, machine names, and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.

EAC OCIO needs to update its hardware inventory records to include the detail level needed to manage its devices. EAC OCIO utilizes a hardware application tool to track and maintain hardware inventory. The inventory report shows EAC OCIO is not capturing the level of detail needed to manage devices according to Federal requirements. Specifically, the report of 557 devices did not include the date of receipt, cost, manufacturer, supplier information, and physical location.

In addition, some fields were incomplete. Several fields within the hardware inventory report are blank such as "assigned owner", "price", "bar code", "serial numbers", "tag", and International Mobile Equipment Identity (IMEI). Specifically:

- 332 out of 557 devices exclude the assigned owner
- 490 out of 557 devices exclude the barcode
- 408 out of 557 devices exclude the serial number
- 420 out of 557 devices exclude tag (component type)
- 7 out of 557 iPhone devices are missing IMIE numbers

EAC OCIO inventory processes lack oversight to ensure hardware inventory records are maintained at the level of detail needed to meet Federal requirements.

The effect of not having an accurate inventory could cause duplicate accounting of system components. Also, there is a lack of accountability when component ownership and system association are unknown.

Recommendation 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.

Auditor's Evaluation of Management's Response:
EAC's management concurred with this recommendation. Management's full response is provided in Appendix IV.

4. EAC OCIO Needs to Develop Plan of Action and Milestone (POA&M) Reports According to Federal Requirements.

NIST Special Publication 800-37 requires POA&M reports to be developed based on assessment results obtained from control assessments, audits, and continuous monitoring and to follow applicable laws, executive orders, directives, policies, regulations, standards, or guidance.

The NIST SP 800-53 Rev. 5.1, Program Management (PM)-4 "Plan of Action and Milestones Process", requires agencies to implement a process to ensure that POA&Ms for the information security, privacy, and supply chain risk management programs and associated organizational systems are developed, maintained. The POA&Ms should include documentation showing remedial actions taken to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation. The POA&M reports should not be the sole responsibility of the EAC OCIO. Instead, agency leadership should be involved to ensure the necessary resources are allocated and to hold accountable the entities responsible for executing the corrective actions. The POA&M reports should be developed from an organization-wide perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization.

Also, POA&M reports are a key organizational document and are subject to reporting requirements established by the OMB. OMB Memorandum 02-09 requires, at a minimum, the agency's POA&M report contains (1) the type of weakness, (2) the agency head responsible for resolving the weakness, (3) estimated funding resources required to resolve the weakness, (4) scheduled completion date for resolving the weakness, (5) key milestones with completion dates, (6) milestone changes, (7) sources of the weakness, and (8) status.

The latest EAC OCIO POA&M report included vulnerability and configuration management weaknesses obtained from network scans. However, the POA&M report did not include weaknesses identified in audit reports and continuous monitoring activities. For example, the POA&M report did not include weaknesses originating from the prior EAC FISMA audit reports and other remedial actions (e.g., planned implementation of the agency's automated risk management system).

EAC OCIO does not have adequate procedures to ensure the agency's POA&M reports are developed and maintained according to Federal requirements.

If EAC does not properly document and maintain an adequate POA&M report, management cannot ensure the agency's risk posture is maintained. Also, EAC cannot prioritize weaknesses to ensure high-priority weaknesses receive the funding and resources necessary to remediate the most significant risks, since funding and assignment of resources to remediate weakness changes over time.

Recommendation 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.

Auditor's Evaluation of Management's Response:
EAC's management concurred with this recommendation and said that corrective action had already been implemented. However, support for the corrective action was not provided prior to the issuance of the report so it could not be evaluated. Management's full response is provided in Appendix IV.

5. EAC OCIO Needs to Update the System Security and Privacy Plan (SSP) in Accordance with NIST.

NIST SP 800-53 Rev. 5.1 establishes controls for systems and organizations. The use of these controls is mandatory for Federal information systems in accordance with Office of Management and Budget (OMB) Circular A-130 and the provisions of the Federal Information Security Modernization Act, which requires the implementation of minimum controls to protect federal information and information systems. NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in the agency' SSP for each system, and provides guidance.

We reviewed the EAC OCIO's SSP, last updated in January 2022, and determined the document does not align with the NIST SP 800-53 Rev. 5.1 security control recommendations for moderate-level systems. NIST SP 800-53 Rev 5.1 was published in September 2020; includes updates as of December 10, 2020, that contain two new control families (Program Management and Supply Chain Risk Management) and one privacy family (Personally Identifiable Information Processing and Transparency). The EAC SSP document does not include security controls for these families. In addition, the EAC SSP document does not reflect the current network environment. For example, the SSP does not include the latest network diagram, all information systems, system components, and software that comprises the general support system.

During our interview, EAC OCIO management explained they did not have sufficient resources needed to update the agency's SSP to align with NIST requirements.

The lack of an updated SSP in accordance with NIST guidelines increases the risk of not implementing safeguarding measures and privacy controls to protect the agency's operations, agency's assets, and the privacy of individuals.

Recommendation 5:
We recommend EAC OCIO update the agency's SSP document to align with NIST requirements and include the network environment's current state.

Auditor's Evaluation of Management's Response:
EAC's management concurred with this recommendation. Management's full response is provided in Appendix IV.

6. EAC OCIO Needs to Implement its Governance, Risk and Compliance (GRC) Solution to Manage Risk.

NIST Special Publication 800-39, Managing Information Security Risk, Organization, Mission, and Information System View, states that effective risk management requires an agency's mission/business process to explicitly account for information security risk when making operational decisions and that cybersecurity risk information should be shared with key stakeholders throughout the organization. Also, NIST SP 800-39 recommends automating risk management requirements for efficiency, consistency, and effectiveness of a unified platform for

managing governance, risk assessment, control implementation, incident response, continuous monitoring, and reporting.

We examined EAC OCIO's implementation of NIST SP 800-39 and the agency's ability to provide and share cybersecurity risk information across the agency with key stakeholders. EAC OCIO has developed an enterprise risk management strategy and supply chain risk management strategy (SCRM). Risk management responsibilities are performed by the EAC OCIO, which has developed risk management plans and monitors information system security risk.

EAC OCIO leverages several tools to monitor and manage information system risks, such as a cloud-based security management system, network security system, DHS/CISA Continuous Diagnostics and Mitigation Program dashboard, and vulnerability assessment application. EAC OCIO has developed SCRM strategy.

EAC OCIO has procured and implemented a GRC solution that can provide a centralized enterprise-wide view of all risks across the agency. Also, the GRC solution has the capability to manage and monitor cybersecurity risk activities required by NIST SP 800-39. However, EAC OCIO has not fully implemented its GRC solution including the SCRM strategy across the organization.

During our interview, EAC OCIO management explained they did not have sufficient resources to fully implement its GRC solution.

EAC's processes for managing risk do not provide an integrated risk management view into an agency's processes, policies, and decision-making for communicating and sharing risk- related information across the agency.

Recommendation 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 risk across the agency.

Auditor's Evaluation of Management's Response:
EAC's management concurred with this 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 OCIO implemented selected security controls for certain information systems in support of the FISMA Act of 2014.

Our overall objective was to evaluate EAC OCIO security program and practices, as required by FISMA. Specifically, we reviewed 20 Core and 20 Supplemental IG FISMA Reporting Metrics[3] in five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of the agencies' information security program and the maturity level of each function area. The maturity levels range from lowest to highest — Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized:

Function (Domains)

- Identify (Risk Management)
- Identify (Supply Chain Management)
- Protect (Configuration Management)
- Protect (Identity and Access Management)
- Protect (Data Protection and Privacy)
- Protect (Security Training)
- Detect (Information Security Continuous Monitoring)
- Respond (Incident Response)
- Recover (Contingency Planning)

We also followed up on outstanding recommendations from prior FISMA audits (see Appendix II) and performed audit procedures on EAC's internal and external systems. The audit also included a review of vulnerability assessments of EAC-managed internal systems and an evaluation of the EAC OCIO process for identifying and mitigating technical vulnerabilities.

Methodology

We reviewed EAC's general FISMA compliance efforts in the specific areas defined in DHS guidance[4] and the corresponding reporting instructions. 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

[3] *OMB Memorandum M 23-03, Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, December 2, 2022.
[4] OMB *M-25-05 Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*.

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' 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 assessed internal controls deemed significant to our audit, which includes 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 the EAC OCIO 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 2021 and 2022 FISMA audit reports; and
- Reviewed the network vulnerability assessment of the EAC OCIO 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. There were no internal control weaknesses identified that affected the audit objective.

Appendix I - Continue

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. 5.1, *Security and Privacy Controls for Information Systems and Organizations, September* 2020; updated as of December 10, 2020;
- 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;*
- *Federal Acquisition Regulation (FAR); FAR Case 2007-004, Common Security Configurations;*
- *OMB Memorandum M-22-18 Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, September 14, 2022;*
- *OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022;*
- *OMB Memorandum M-22-05, Guidance on Federal Information Security and Privacy;*
- *OMB Memorandum M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response, October 8, 2021;*
- *OMB Memorandum M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident, August 27, 2021.*

The audit was conducted at Brown & Company in Greenbelt, Maryland, and EAC's headquarters in Washington, DC, from March 30, 2023 through July 6, 2023.

Appendix II – Status of Prior Years Audit Recommendations

The following table provides the status of the fiscal years' (FY) 2021 and 2022 audit recommendations. Three recommendations from prior years were not fully implemented.

No.	FY 2021[5] and 2022[6] Audit Recommendations	Status
1	**FY 2021 FISMA audit recommendation No. 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).	Open
2	**FY 2021 FISMA audit recommendation No. 2:** We recommend EAC OCIO ensure its Windows 10 devices comply with its Center for Internet Security (CIS) security benchmarks as required by its system security plan.	Closed
3	**FY 2022 FISMA audit recommendation No. 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
4	**FY 2022 FISMA audit recommendation No. 2:** We recommend EAC OCIO develop and implement a flaw remediation plan for vulnerabilities that cannot be remediated within the policy recommended timeframes.	Open
5	**FY 2022 FISMA audit recommendation No. 3:** We recommend EAC OCIO develop a process for tracking software license usage.	Closed
6	**FY 2022 FISMA audit recommendation No. 4:** We recommend EAC OCIO perform annual contingency plan testing.	Closed
7	**FY 2022 FISMA audit recommendation No. 5:** We recommend EAC OCIO provide contingency training to information system users consistent with assigned roles and responsibilities.	Closed

[5] The *Fiscal Year 2021 EAC Compliance with the Federal Information Security Modernization Act (*EAC IG Report No. I-PA-EAC-04-21, November 2, 2021).

[6] *Audit of the U.S. Election Assistance Commission's Compliance with The Federal Information Security Modernization Act for Fiscal Year 2022* (EAC IG Report No. O22HQ0006-23-02, November 3, 2022).

Appendix III - Acronyms

Acronyms	
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CM	Configuration Management
DHS	U.S. Department of Homeland Security
EAC	Election Assistance Commission
FAR	Federal Acquisition Regulation
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GRC	Governance, Risk and Compliance
IMEI	International Mobile Equipment Identity
NIST	National Institute of Standards and Technology
OCIO	Office of Chief Information Officer
OMB	U.S. Office of Management and Budget
POA&M	Plan of Action and Milestone
REV	Revision
SCAP	Security Content Automation Protocol
SECURE Technology Act	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act
SCRM	Supply Chain Risk Management
SI	System and Information Integrity
SP	Special Publication
SSP	System Security and Privacy
STIGs	Standard Technical Implementation Guides

Appendix IV – Management's Comments

U.S. Election Assistance Commission
633 3rd St. NW, Suite 200
Washington, DC 20001

TO: U.S. Election Assistance Commission, Inspector General, Brianna Schletz
FROM: U.S. Election Assistance Commission, OCIO, Jessica Bowers
DATE: July 24, 2023
SUBJECT: Response to Draft FISMA Audit Report FY2023

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 OCIO needs to consistently resolve known vulnerabilities.**

   Management Response: Agree
   The EAC continues to work to reduce its backlog of identified low and medium severity vulnerabilities. Critical vulnerabilities with known exploits are now resolved within two weeks of notice, per binding operational directive 22-01.

   Estimated completion date: March 29, 2024

2. **EAC OCIO needs to improve its configuration procedures.**

   Management Response: Agree

   The audit report included two recommendations. Recommendation 1 recommends that the EAC resolve conflicting baseline configuration settings for Windows 10 devices and ensure iPhones meet the agency's configuration setting requirements. Work is ongoing to resolve the reported configuration conflicts with Windows 10 and mobile devices.

   Recommendation 2 recommends that the EAC ensure information systems meet STIG secure configuration settings and verified using SCAP scanning. The EAC has recently implemented STIG configuration settings and we believe we are compliant with the SCAP scanning requirement using our existing tools. Although the tools are not branded as a SCAP scanner, they are performing the required configuration checks and the reports reviewed by the auditors during this period were generated by these tools. The EAC would benefit from clarification on whether its current scanning meets the recommendation or whether a specifically branded SCAP scanning tool is required.

   Estimated completion date: September 30, 2023

3. **EAC OCIO needs to maintain hardware inventory records according to federal requirements.**

   Management Response: Agree

The EAC is working to improve the quality of its hardware inventory records to include the level of detail needed to effectively manage devices.

Estimated completion date: December 31, 2023

4. **EAC OCIO needs to develop plan of action and milestone (POA&M) reports according to federal requirements.**

   Management Response: Agree

   The EAC has updated its POA&M to include information identified by the auditors as missing or incomplete.

   Estimated completion date: July 12, 2023

5. **EAC OCIO needs to update the system security and privacy plan (SSP) in accordance to NIST.**

   Management Response: Agree

   The EAC is updating its SSP in accordance with NIST recommendations and the revision 5 update to NIST SP 800-53.

   Estimated completion date: September 30, 2023

6. **EAC OCIO needs to implement its governance, risk, and compliance (GRC) solution to manage risk.**

   Management Response: Agree

   The EAC is transitioning to a new automated GRC tool due to vendor deprecation of our existing tool. Part of this migration will be to more fully utilize the risk management portions of the tool to automate our risk register in accordance with NIST recommendations.

   Estimated completion date: March 29, 2024

This response acknowledges the work of the Inspector General and provides an update to the EAC's ongoing efforts to improve agency information practices. The Office of the Chief Information Officer thanks the Inspector General for their attention to these matters.

Sincerely,

Jessica Bowers

Jessica Bowers
EAC Chief Information Officer

Visit our website at **eac.gov/inspector-general**

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