

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 2022

Report No. O22HQ0006-23-02
November 3, 2022



HIGHLIGHTS

AUDIT OF EAC'S COMPLIANCE WITH FISMA FOR FISCAL YEAR 2022

Report No. O22HQ0006-23-02

November 3, 2022

What OIG Audited

The Office of Inspector General, through the independent public accounting firm of Brown & Company CPAs and Management Consultants, PLLC, audited the U.S. Election Assistance Commission's (EAC's) information security program for fiscal year 2022 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

The 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, and therefore the EAC information security program is effective.

However, the EAC Office of the Chief Information Officer did not: (1) consistently resolve known vulnerabilities; (2) fully configure Security Content Automation Protocol (SCAP) scanning procedures; (3) track software license usage; and (4) test its contingency plan and provide contingency training.

What OIG Recommended

The Office of Inspector General made five recommendations to address the noted deficiencies:

- 1 Remediate configuration-related vulnerabilities or document acceptance of the risk.
- 2 Implement a plan for vulnerabilities that cannot be remediated within timeframes established by policy.
- 3 Develop a process for tracking software license usage.
- 4 Perform annual contingency plan testing.
- 5 Provide contingency training to users according to their assigned roles and responsibilities.

Additionally, two recommendations from the prior year remain open:

- 1 SCAP scan network systems to identify vulnerabilities, as required by OMB.
- 2 Ensure Windows 10 devices comply with CIS security benchmarks as required by the system security plan.



OFFICE OF INSPECTOR GENERAL

U.S. Election Assistance Commission

DATE: November 3, 2022

TO: U.S. Election Assistance Commission, Interim Executive Director, Mark Robbins

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 2022 (Report No. O22HQ0006-23-02)

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 2022. 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 five recommendations, as well as the two recommendations that remain open from prior year, 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 Thomas Hicks, Chair
Commissioner Christy McCormick, Vice Chair
Commissioner Benjamin W. Hovland
Commissioner Donald L. Palmer

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



**Fiscal Year 2022
November 1, 2022**

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 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 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 Special Publication (SP) 800-53, Revision (Rev) 5.1, *Security and Privacy Controls for Information Systems and Organizations*.

For this audit, we reviewed selected controls from EAC's General Support System. The selected controls included 20 Core Inspector General (IG) FISMA Reporting Metrics 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 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 April 18, 2022 through September 30, 2022.

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 four findings and making five recommendations to assist EAC OCIO in strengthening its information security program. There are two 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.

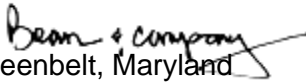

Greenbelt, Maryland
November 1, 2022

Table of Contents

Summary of Results.....	1
Audit Results.....	3
Audit Findings	3
1. EAC OCIO Needs to Consistently Resolve Known Vulnerabilities.....	3
2. EAC OCIO Needs to Improve Its Configuration Scanning Procedures.	4
3. EAC OCIO Needs to Track Software License Usage.	5
4. EAC OCIO Needs to Test Its Contingency Plan and Provide Contingency Training.	6
Appendix I – Scope, Methodology and Criteria.....	7
Appendix II – Status of Prior Years Audit Recommendations.....	10
Appendix III - Acronyms	11
Appendix IV – Management’s Comments	12



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 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 four findings and making five recommendations to assist EAC OCIO in strengthening its information security program. Specifically, EAC OCIO needs to:

1. Consistently Resolve Known Vulnerabilities
2. Improve Its Configuration Scanning Procedures
3. Track Software License Usage
4. Test Its Contingency Plan and Provide Contingency Training

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

Audit Results

We concluded 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). The Table below shows a summary of the overall assessed maturity levels for each function area and domain in the Fiscal Year (FY) 2022 Core IG FISMA Reporting Metrics.

Table Summary of Overall Assessed Maturity Levels

Function Areas	FY 22 Core 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	Managed and Measurable (Level 4)
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.

NIST SP 800-53 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 June 3, 2022, Brown & Company conducted an independent internal vulnerability scan on EAC’s network for 17 selected IP addresses and confirmed 2 “Urgent,” 18 “Critical,” 38 “Serious” and 92 “Medium” risk vulnerabilities related to patch and configuration management. The internal vulnerability scan identified urgent vulnerabilities relating to Transport Layer Security (TLS) Protocol and authentication; and critical vulnerabilities relating to TLS, Secure Sockets Layer (SSL)/TLS, and Open-source version of the Secure Shell (OpenSSH).

EAC OCIO runs vulnerability scans weekly; 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.

Recommendation 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.

Auditor's Evaluation of Management's Response:

EAC's management does not concur with this recommendation.

Recommendation 2: We recommend EAC OCIO develop and implement a flaw remediation plan for vulnerabilities that cannot be remediated within the policy recommended timeframes.

Auditor's Evaluation of Management's Response:

EAC's management concurred with this recommendation.

Management's full response is provided in Appendix IV.

2. EAC OCIO Needs to Improve Its Configuration Scanning 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 the Center for Internet Security (CIS) and Standard Technical Implementation Guides (STIGs). The policy also requires EAC OCIO to conduct SCAP scans to monitor and control configuration settings.

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 22.

EAC OCIO controls for configuration management are not operating effectively to ensure scanning practices are fully implemented. Starting 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 information systems face an increased risk of being comprised if the OCIO does not conduct SCAP scanning to identify, track, and control configuration settings in accordance with risk.

No new recommendation is being made because recommendation 3 from the FY 21 FISMA audit is substantially similar and open. See Appendix II.

3. EAC OCIO Needs to Track Software License Usage.

NIST SP 800-53 Rev. 5.1, CM-10 “Software Usage Restrictions”, requires the organization to track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

The EAC Configuration Management Policy requires the EAC OCIO to establish a procedure to ensure the agency’s use of software meets all copyright and licensing requirements. EAC OCIO has implemented an automated tool to track software applications installed on EAC’s endpoint devices. However, the tool does not track software license usage to monitor compliance with software copyrights and licensing agreements

The condition was due to EAC OCIO lacking a process and tool for tracking software license usage for its information systems.

The failure to track software license usage increases the risk of EAC violating software contract agreements and copyright laws; copying and distributing duplicate software licenses; purchasing unnecessary software licenses; enabling the use of peer-to-peer file sharing; and extending licenses that are no longer needed by EAC.

Recommendation 3: We recommend EAC OCIO develop a process for tracking software license usage.

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 Test Its Contingency Plan and Provide Contingency Training.

NIST SP 800-53 Rev. 5.1, Contingency Plan (CP)-3 “Contingency Training”, requires an organization to provide contingency training to system users consistent with assigned roles and responsibilities. CP-4 “Contingency Plan Testing” requires the organization to test the contingency plan for the system based on the organization’s defined frequency, using tests to determine the effectiveness of the plan and the readiness to execute the plan.

The EAC Contingency Planning Policy requires management to test and/or conduct exercises for its contingency/continuity plan annually, at a minimum. It also requires EAC OCIO to provide contingency training to information system users for the following conditions: prior to assuming a contingency role or responsibility, when required by information system changes, and annually thereafter.

EAC OCIO does not have processes or procedures in place to ensure the annual testing of the agency’s contingency plan and for providing contingency training to information system users consistent with assigned roles and responsibilities.

EAC OCIO's lack of control to test the contingency plan increases the risk that the agency has not determined the plan's effectiveness and readiness to execute the plan. The lack of control in conducting annual contingency plan training increase the risk that assigned roles and responsibilities will not be performed to support the specific continuity requirements in the contingency plan.

Recommendation 4: We recommend EAC OCIO perform annual contingency plan testing.

Auditor’s Evaluation of Management’s Response:

EAC’s management concurred with this recommendation.

Management’s full response is provided in Appendix IV.

Recommendation 5: We recommend EAC OCIO provide contingency training to information system users consistent with assigned roles and responsibilities.

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 Inspector General (IG) FISMA Reporting Metrics³ 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 on external systems. The audit also included a review of vulnerability assessments of EAC-managed internal system 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 U.S. Department of Homeland Security guidance⁴ 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

³ OMB Office of the Federal Chief Information Officer FY22 Core IG Metrics Implementation Analysis and Guidelines, Appendix A: Core IG Metrics

⁴ OMB M-25-05 Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements.

APPENDIX I

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' 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 FYs 2018, 2020 and 2021 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

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*;
- 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 ERM and Internal Control*;
- *OMB Circular A-130, Managing Information as a Strategic Resource, July 28, 2016*;
- *OMB Memorandum M-22-05, Guidance on Federal Information Security and Privacy*;
- *OMB Memorandum M-20-32 Improving Vulnerability Identification, Management, and Remediation*;
- *OMB Memorandum M-08-22, Guidance on the FDCC*;
- *OMB Memorandum M-08-05, Implementation of Trusted Internet Connections*;
- *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act), Federal Acquisition Supply Chain Security*; and
- *United States Computer Emergency Readiness Team (US-CERT) Incident Notification Guidelines*.

The audit was conducted at Brown & Company in Greenbelt, Maryland, and EAC's headquarters in Washington, DC, from April 18, 2022 through September 30, 2022.

Appendix II – Status of Prior Years Audit Recommendations

The following table provides the status of the Fiscal Years' (FY) 2018, 2020 and 2021 audit recommendations. Two recommendations from prior years were not fully implemented.

No.	FY 2018 ⁵ , 2020 ⁶ , and 2021 ⁷ Audit Recommendations	Status	Auditor's Position on Status
1	FY 2018 FISMA audit recommendation No. 3: EAC Office of Information Technology (OIT) to remediate configuration-related vulnerabilities in the network identified, and document the results or document acceptance of the risks of those vulnerabilities.	Closed	Agree
2	FY 2020 FISMA audit recommendation No. 2: We recommend EAC OIT ensure Data Owners sign user access recertifications.	Closed	Agree
3	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). (Repeated for FY 22)	Open	Agree
4	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.	Open	Agree

⁵ The EAC Compliance with the Federal Information Security Modernization Act Fiscal 2018 (EAC IG Report No. I-PA-EAC-02-18, November 28, 2018).

⁶ The Fiscal Year 2020 EAC Compliance with the Federal Information Security Modernization Act (EAC IG Report No. I-PA-EAC-02-20, December 14, 2020).

⁷ 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).

Appendix III - Acronyms

Acronyms	
CIS	Center for Internet Security
CM	Configuration Management
CP	Contingency Plan
DHS	U.S. Department of Homeland Security
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
IG	Inspector General
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OIT	Office of Information Technology
OCIO	Office of Chief Information Technology
OMB	U.S. Office of Management and Budget
RA	Risk Assessment
REV	Revision
SCAP	Security Content Automation Protocol
SECURE Technology Act	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act
SI	System and Information Integrity
SP	Special Publication
STIG	Standard Technical Implementation Guides
TLS	Transport Layer Security
SSL	Secure Sockets Layer
OpenSSH	Open-source version of the Secure Shell
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: Brianna Schletz, Inspector General
FROM: Jessica Bowers, CIO/CISO
DATE: October 31, 2022
SUBJECT: Response to Draft FISMA Audit Report FY2022

1. Remediate configuration-related vulnerabilities or document acceptance of the risk.

Manage Response:

The EAC continues to work through a backlog of vulnerability mitigations and anticipates resolving remaining vulnerabilities by the end of Q2, FY23. Critical vulnerabilities with known exploits are currently resolved within two weeks of notice, per binding operational directive 22- 01.

2. Implement a plan for vulnerabilities that cannot be remediated within timeframes established by policy.

Management Response:

For vulnerabilities that the EAC is not able to resolve within our established timeframes, we will document the acceptance of this risk in our POA&M and work to improve our capabilities to respond more quickly. With the completion of backlog remediations by the end of Q2, FY23, our ability to immediately remediate should be significantly improved.

3. Develop a process for tracking software license usage.

Management Response:

The EAC has acquired IT asset management software that will allow the agency to track software license usage. This software is being deployed with completion expected by the end of Q1, FY23.

4. Perform annual contingency plan testing.

Management Response:

The EAC will conduct a contingency plan exercise by the end of Q3, FY23.



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

5. Provide contingency training to users according to their assigned roles and responsibilities.

Management Response:

The EAC will develop a contingency plan training program relevant to specific assigned roles and responsibilities and ensure training is tracked and documented by the end of Q3, FY23.

Sincerely,

A handwritten signature in black ink that reads "Jessica Bowers".

Jessica Bowers
CIO/CISO

U.S. Election Assistance Commission



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](#)