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 2026



Report No. P26HQ0003-27-04
November 13, 2026

HIGHLIGHTS

AUDIT OF THE EAC'S COMPLIANCE WITH FISMA FOR FISCAL YEAR 2026

Report No. P26HQ0003-27-04 November 13, 2026

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 2026 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 the EAC's security program:

- Cybersecurity Governance
- Cybersecurity Supply Chain Risk Management
- Risk and Asset 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 fiscal year 2026 audit found that the EAC's information security program and practices were effective overall. The audit also found that the EAC had addressed four prior-year recommendations, while some previously identified areas for improvement remained and one new area was identified. The audit found that the EAC could further strengthen its information security program by:

- Developing an IT staffing contingency plan.
- Better integrating cybersecurity risk management with enterprise risk management.
- Strengthening processes for maintaining complete and accurate inventories of data, software, hardware, mobile applications, and licenses.
- Establishing policies and risk-based procedures for the use of untrusted removable media.
- Documenting lessons learned from continuous monitoring activities.
- Improving contingency plan testing through automated notification capabilities.

What Was Recommended

The audit made one recommendation to improve the EAC's security posture, and six from prior years remain open.

U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL

DATE: November 13, 2026

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

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

SUBJECT: Audit of the U.S. Election Assistance Commission's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2026 (Report No. P26HQ0003-27-04)

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 2026. 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 November 13, 2026, 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 one recommendation. Please keep us informed of the actions taken to resolve it, as we will track the status of their implementation.

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

RMA Associates
Auditors. Consultants. Advisors.

United States Election Assistance Commission

Federal Information Security Modernization Act of 2014

Performance Audit Report for Fiscal Year 2026

RMA | Associates
Auditors. Consultants. Advisors.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

November 13, 2026

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

Re: United States Election Assistance Commission Federal Information Security Modernization Act of 2014 Performance Audit Report for Fiscal Year 2026

Dear Ms. Dreyer:

RMA Associates, LLC is pleased to submit our performance audit report on the effectiveness of the United States Election Assistance Commission's (EAC) information security program and Practices Report for Fiscal Year (FY) 2026. In accordance with the *Federal Information Security Modernization Act of 2014* (FISMA), the objective of this performance audit was to evaluate the effectiveness of the EAC's information security program and practices and determine the maturity level the EAC achieved for each core supplemental metric outlined in the *FY 2025 Inspector General (IG) FISMA Reporting Metrics v2.0*. For the FY 2026 audit cycle, Inspectors General and independent external auditors used the FY 2025 IG FISMA reporting metrics and associated implementation guidance. The performance audit fieldwork was conducted in Washington, DC, from April 15, 2026 to July 31, 2026.

Based on our performance audit results and our risk-based assessment of the totality of the evidence, we determined that the EAC's information security program and practices were effective for FY 2026. We assessed the EAC's overall information security program at the Consistently Implemented (Level 3) maturity level, closed four of 10 prior FISMA performance audit recommendations, and identified one new finding associated with the Identify function.

Our report includes **Appendices I**: Status of Prior Year Recommendations, **II**: Management Response, **III**: Evaluation of Management Response, and **IV**: Glossary of Acronyms.

We conducted this performance audit 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The performance audit included assessing the EAC's information security program and practices consistent with FISMA and reporting instructions issued by the Office of Management and Budget (OMB). We considered guidelines established by OMB, the Department of Homeland Security,

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

and the National Institute of Standards and Technology (NIST). We selected and assessed three FISMA reportable systems from the EAC's FISMA inventory of information systems.

For FY 2026, OMB required Inspectors General to assess 25 metrics from the *FY 2025 IG FISMA Reporting Metrics v2.0*,[1] dated April 3, 2025, including both core and supplemental metrics. The Council of the Inspectors General on Integrity and Efficiency, the Chief Information Security Officer, OMB, and the Cybersecurity and Infrastructure Security Agency coordinated and agreed on these metrics. This approach is aligned with NIST *Cybersecurity Framework 2.0*, which underscores the essential role of governance in managing cybersecurity risks and integrating cybersecurity into an organization's overall enterprise risk management strategy. The metrics were aligned with the following Cybersecurity Framework function areas: Govern, Identify, Protect, Detect, Respond, and Recover to determine the effectiveness of agencies' information security programs. They also classify information security programs and practices into five maturity levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

We also prepared responses to OMB's M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, encouraging agencies to shift toward a continuous assessment process for their annual independent assessment using *FY 2025 IG FISMA Reporting Metrics v2.0* and submitting evaluations via CyberScope. These metrics provide reporting requirements across function areas to be addressed in the independent assessment of agencies' information security programs.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. We caution that projecting the results of our performance audit to future periods is subject to the risk that conditions may change significantly from their current status. The information included in this report was generally obtained from the EAC on or before July 31, 2026. We are not obligated to update our report or revise the information contained therein to reflect events occurring after July 31, 2026.

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

Sincerely,

RMA Associates

RMA Associates, LLC
Arlington, VA

[1] Based on a joint message from OMB and Council of the Inspectors General on Integrity and Efficiency (CIGIE) received on March 17, 2026, on FY 2026 IG FISMA Metrics and Implementation Guidance, IGs and independent external auditors, as appropriate, are directed to use the *FY 2025 IG FISMA Reporting Metrics v2.0.*

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Table of Contents

Introduction 1
Background 1
United States Election Assistance Commission 1
Federal Information Security Modernization Act of 2014 2
Summary Performance Audit Results 4
Objective, Scope, and Methodology 12
Appendix I: Status of Prior Year Recommendations 18
Appendix II: Management Response 20
Appendix III: Evaluation of Management Response 23
Appendix IV: Glossary of Acronyms 24

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Introduction

This report presents the results of RMA Associates, LLC (RMA)'s independent performance audit of the United States Election Assistance Commission (EAC)'s information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to conduct an annual independent performance audit to assess their information security programs and practices, determine their effectiveness, and report the performance audit results to the Office of Management and Budget (OMB). OMB delegated its responsibility to the Department of Homeland Security (DHS) to collect annual FISMA responses.

The EAC's Office of Inspector General (OIG) engaged RMA to conduct an annual performance audit of the EAC's information security program and practices, in support of FISMA requirements. The objective of this performance audit was to evaluate the effectiveness of the EAC's information security program and practices, and to determine the maturity level achieved by the EAC for each core and supplemental metric outlined in the fiscal year (*FY) 2025 Inspector General (IG) FISMA Reporting Metrics v2.0*, dated April 3, 2025.[2] For the FY 2026 audit cycle, Inspectors General and independent external auditors used the FY 2025 IG FISMA reporting metrics and associated implementation guidance.

As part of our performance audit, we audited the EAC according to 20 core and five supplemental metrics specified in OMB's *FY 2025 IG FISMA Reporting Metrics v2.0*. These metrics align with the function areas in *the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0:* Govern, Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise. It provides IGs with guidance for assessing the maturity of controls to address those risks. We also considered applicable EAC and OMB policies and guidelines, as well as NIST standards.

Background

United States Election Assistance Commission

The Help America Vote Act of 2002 (HAVA) established the EAC. The EAC is an independent, bipartisan Commission charged with developing guidance to meet HAVA requirements, adopting voluntary voting system guidelines, and serving as a national clearinghouse for election administration information. The EAC also accredits testing laboratories, certifies voting systems, and monitors the use of HAVA grant funds. Other responsibilities include maintaining the national mail voter registration form developed in accordance with the National Voter Registration Act of 1993. HAVA also established the Standards Board and the Board of Advisors to advise the EAC.

[2] Based on a joint message from OMB and Council of the Inspectors General on Integrity and Efficiency (CIGIE) received on March 17, 2026, on FY 2026 IG FISMA Metrics and Implementation Guidance, IGs and independent external auditors, as appropriate, are directed to use the *FY 2025 IG FISMA Reporting Metrics v2.0.*

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

The law also established the Technical Guidelines Development Committee to help the EAC develop voluntary voting system guidelines.

The EAC Commissioners are appointed by the President and confirmed by the United States Senate. Two other statutory positions exist within the EAC: the Executive Director and the General Counsel. The Commissioners provide overall guidance and policy. The Executive Director reports to the Commissioners and directs the day-to-day operations of the EAC units which carry out the agency's principal duties.

Federal Information Security Modernization Act of 2014

On December 18, 2014, the President signed FISMA, which amended the Federal Information Security Management Act of 2002 and modernized federal security practices to address evolving security concerns. These changes strengthened continuous monitoring in systems, increased focus on agency compliance, and produced reports highlighting issues caused by security incidents.

FISMA requires federal agencies to undergo an annual, independent assessment of their information security programs and practices to determine their effectiveness and report the results to OMB. In addition to the annual review and reporting requirements, FISMA includes provisions to strengthen further the federal government's data and information systems security (e.g., requiring the development of minimum control standards for agencies' systems).

FISMA reestablished the OMB Director's oversight authority over agency information security policies and practices and set forth the Secretary of DHS's authority to administer the implementation of such policies and practices for information systems.[3]

FISMA requires the Secretary of DHS to develop and oversee the implementation of operational directives to safeguard federal information and systems from known or reasonably suspected information security threats, vulnerabilities, or risks. It authorizes the Director of OMB to revise or repeal operational directives that do not comply with OMB policies.[4]

The Director of OMB directs the Secretary of DHS to consult with and consider guidance developed by NIST to ensure operational directives do not conflict with NIST information security standards.[5]

Additionally, FISMA directs federal agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General of the United States. Reports are required to include: (1) threats and threat factors, vulnerabilities, and impacts; (2) risk assessments of affected systems before and the status of compliance of systems at the time of major incidents; (3) detection, response, and remediation actions; (4) total number of incidents; and (5) a description

[3] Federal Information Security Modernization Act of 2014, Public Law No. 113-283, December 2014, https://www.congress.gov/bill/113th-congress/senate-bill/2521.
[4] Ibid, *Summary*.
[5] Ibid, *Summary*.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

of the number of individuals affected by and information exposed by major incidents involving a breach of personally identifiable information.[6]

Further, FISMA requires OMB to develop guidance for evaluating the effectiveness of information security programs and practices and determining what constitutes a major incident.[7]

Key Changes to the FY 2026 IG FISMA Reporting Metrics

For FY 2026, IGs and independent external auditors used the *FY 2025 IG FISMA Reporting Metrics v2.0* and associated implementation guidance. The FY 2026 audit did not introduce a new set of IG FISMA reporting metrics.

FY 2025 Change That Continues to Apply in FY 2026

One goal of the annual FISMA audits is to assess agencies' progress toward objectives that strengthen federal cybersecurity. The *FY 2025 IG FISMA Reporting Metrics v2.0* has been updated to measure agency progress toward achieving these objectives.

- NIST *Cybersecurity Framework 2.0*: NIST published the Cybersecurity Framework (CSF) Version 2.0, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's broader enterprise risk management strategy. A new IG FISMA function area (Govern) was created that includes a new domain (Cybersecurity Governance). In addition, new supplemental metrics were designed to assess the maturity of an organization's:
  - Use of cybersecurity profiles to understand, tailor, assess, prioritize, and communicate cybersecurity objectives.
  - Cybersecurity risk management strategy, which establishes an organization's priorities, constraints, risk tolerance, and appetite statements and is used to support operational risk decisions.
  - Processes and authorities to foster cybersecurity accountability, performance assessment, and continuous improvement.

To align with CSF 2.0, the supply chain risk management (SCRM) domain was moved from the Identify function area to the Govern function area and renamed Cybersecurity SCRM (C-SCRM) to better reflect the cybersecurity environment. Furthermore, a new domain in the Identify function area (Risk and Asset Management) was established to group metrics on system inventory and hardware, software, and data management.

- Zero Trust Architecture (ZTA) Implementation: The FY 2025 metrics included two new supplemental metrics critical to achieving ZTA objectives. These new metrics assess the maturity of an organization's (1) data management capabilities, and (2) ability to monitor and measure the integrity and security posture of all owned and associated assets.

[6] Ibid, *Summary*.
[7] Ibid, *Summary*.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

- Supplemental metrics for FY 2025: Five supplemental metrics, including metric numbers 1, 2, 3, 10 and 27, were in scope for the FY 2025 IG FISMA audit.
- Information System Level Risk Management: The core metric on information system level risk management (Metric 11, formerly Metric 5) was revised to focus on the maturity of agencies' implementation of the NIST risk management framework.

Summary Performance Audit Results

We determined that, consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards, the EAC's information security program and practices were established and maintained for the six Cybersecurity Framework function areas[8] and 10 FISMA Metric Domains.[9] The results of this work are summarized below by Function. We assessed the EAC's overall information security program at Consistently Implemented (Level 3). At this maturity level, policies, procedures, and strategies are consistently implemented; however, the EAC had not demonstrated quantitative and qualitative performance measurement across all areas to achieve a Managed and Measurable (Level 4). In determining overall effectiveness, we considered test results; maturity and implementation of controls across the six Cybersecurity Framework function areas; nature, significance, and potential security impact of the identified weaknesses; status of prior-year recommendations; the EAC's risk tolerance and threat environment; and its unique mission, resources, and operational challenges. FISMA reporting guidance permits IGs and independent external auditors to determine that an information security program is effective at a calculated maturity level below Level 4 when supported by the results of the audit and the agency's risk profile and operating environment. Based on the totality of the evidence, we determined that the EAC's information security program and practices were effective for FY 2026, notwithstanding an overall Consistently Implemented (Level 3) maturity level.

We identified one new finding to address the weakness found in the Identify function area. RMA made one recommendation to address the finding.

The EAC made progress in implementing the recommendations from the prior year. During FY 2026, the EAC closed four of 10 open recommendations from the FY 2024 and FY 2025 FISMA audits. **Appendix I**: Status of Prior Year Recommendations summarizes the status of prior-year recommendations.

We provided the EAC with a draft of this report for their review and comment. In a written response, management agreed with the results of our performance audit (refer to **Appendix II**:

[8] OMB, DHS, and CIGIE developed the FISMA Reporting Metrics in consultation with the federal Chief Information Officers Council. The ten FISMA Metric Domains were aligned with the six Cybersecurity Framework functions: (1) govern, (2) identify, (3) protect, (4) detect, (5) respond, and (6) recover as defined in the NIST *Cybersecurity Framework 2.0*.

[9] As described in the FISMA IG Reporting Metrics, the ten FISMA Metric Domains are: (1) Cybersecurity Governance, (2) Cybersecurity Supply Chain Risk Management, (3) Risk and Asset Management, (4) Configuration Management, (5) Identity and Access Management, (6) Data Protection and Privacy, (7) Security Training, (8) Information Security Continuous Monitoring, (9) Incident Response, and (10) Contingency Planning.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Management Response for the EAC's response in its entirety, and **Appendix III**: Evaluation of Management Response for our assessment of management's response).

RMA focused on the core metric results and used the calculated weighted averages of the supplemental metrics as a data point to support its risk-based determination of overall program- and function-level effectiveness.

Table 1 presents the maturity level for the 10 FISMA Metric Domains.

Table 1: EAC's FY 2026 Maturity Levels

Function and Domain	Maturity Level
Govern	**Consistently Implemented (Level 3)**
• Cybersecurity Governance	Consistently Implemented (Level 3)
• Cybersecurity Supply Chain Risk Management	Managed and Measurable (Level 4)
Identify – Risk and Asset Management	**Defined (Level 2)**
Protect	**Managed and Measurable (Level 4)**
• Configuration Management	Managed and Measurable (Level 4)
• Identity and Access Management	Optimized (Level 5)
• Data Protection and Privacy	Consistently Implemented (Level 3)
• Security Training	Optimized (Level 5)
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	**Consistently Implemented (Level 3)**
Overall	**Effective**[10]

The following paragraphs detail each domain's assessed maturity level and offer recommendations to the Chief Information Officer to remediate deficiencies.

Cybersecurity Governance

RMA determined that the EAC's overall maturity level for the Cybersecurity Governance domain was Consistently Implemented.

The EAC continuously monitored its cybersecurity risk management program in near real-time, leveraging predictive analytics and threat intelligence to proactively adjust strategies. The EAC also evaluated and adapted its cybersecurity roles and responsibilities to account for a changing cybersecurity landscape. The EAC established and communicated roles, responsibilities, and authorities related to cybersecurity risk management. Stakeholders were held accountable for carrying out their roles and responsibilities effectively. However, there was one open recommendation – FY 2025 Recommendation 1[11] regarding addressing potential future staffing challenges that may arise, whereby mitigating delays in implementing necessary improvements across the applicable FISMA domains. RMA did not make a new recommendation.

[10] RMA made a risk-based determination of overall program and function level effectiveness.
[11] Recommendation 1 in *Fiscal Year 2025 U.S. Election Assistance Commission Federal Information Security Modernization Act of 2014 Audit* (Audit Report No. P25HQ0063-25-07, September 29, 2025).

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Cybersecurity Supply Chain Risk Management

RMA determined that the EAC's overall maturity level for the Cybersecurity Supply Chain Risk Management (C-SCRM) domain was Managed and Measurable.

The EAC defined supply chain policies and procedures. The EAC managed supply chain risks by purchasing products from trusted, approved manufacturers. The EAC also monitored and analyzed qualitative and quantitative performance measures to assess the effectiveness of its C-SCRM strategy. In addition, the EAC closed FY 2024 Recommendation 2 by developing and implementing procedures to leverage the repository for software attestation and artifacts to obtain sufficient assurance that security and supply chain controls for systems or services provided by contractors or other entities meet FISMA requirements. We determined the EAC took appropriate action, and RMA considered the FY 2024 Recommendation 2[12] closed.

RMA's testing found no exceptions and controls operating as intended.

Risk and Asset Management

RMA determined that the EAC's overall maturity level for the Risk and Asset Management domain was Defined.

Information systems in the EAC's inventory were subject to the monitoring processes defined in the organization's Information Security Continuous Monitoring Strategy. They maintained a comprehensive and accurate inventory of their information systems. The EAC also consistently monitored the effectiveness of risk responses to ensure that risk tolerances were maintained at an appropriate level. While the EAC made progress in implementing continuous monitoring of governance, risk, and compliance tools, it did not integrate cybersecurity risk management into the enterprise risk management reporting tool. Also, the EAC had not defined a process to maintain an accurate inventory of data and corresponding metadata for its data types. Therefore, RMA determined that FY 2025 recommendations 1, 2, and 3[13] remained open.

Hardware and Software Taxonomy Policies and Procedures

In addition, while the EAC had developed an in-house asset inventory tool to address asset tracking needs, the EAC did not define, document, or implement policies, procedures, and processes to establish the use of standardized data elements and taxonomy for developing, maintaining, and updating an inventory of Executive Order (EO)-critical software, mobile applications, hardware assets, software assets, and associated licenses.

[12] Ibid.
[13] Recommendations 1, 2, 3 in *Fiscal Year 2025 U.S. Election Assistance Commission Federal Information Security Modernization Act of 2014 Audit* (Audit Report No. P25HQ0063-25-07, September 29, 2025).

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

NIST Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* CM-8 System Component Inventory, requires organizations to:

a. Develop and document an inventory of system components that:

   1. Accurately reflects the system;

   2. Includes all components within the system;

   3. Does not include duplicate accounting of components or components assigned to any other system;

   4. Is at the level of granularity deemed necessary for tracking and reporting; and

   5. Includes the following information to achieve system component accountability.

b. Review and update the system component inventory [Assignment: organization-defined frequency].

OMB Memorandum M-26-05, *Adopting a Risk-based Approach to Software and Hardware Security*, requires that:

> Agencies shall continue to maintain a complete inventory of software and hardware and develop software and hardware assurance policies and processes that match their risk determinations and mission needs.

The *FY 2025 Inspector General FISMA Reporting Metrics v2.0* provides the following guidance to assess an agency as having a Defined maturity:

> Metric 8 – Defined Maturity Level 2
>
> > The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) with the detailed information necessary for tracking and reporting.
>
> Metric 9 – Defined Maturity Level 2
>
> > The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including EO-critical, cloud, and mobile software and applications used in the organization's environment with the detailed information necessary for tracking and reporting.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Management prioritized developing and deploying the in-house asset inventory tool to address asset tracking needs; however, the EAC had not established a process to ensure supporting policies and procedures were developed, approved, and implemented alongside the deployment of new asset management capabilities. Consequently, the tool was fully implemented before the associated policies and procedures were finalized.

Without defined policies, procedures, and processes governing the use of the asset inventory tool and maintenance of inventory records, the EAC lacked assurance that hardware assets, software assets, software licenses, and EO-critical software and mobile applications were consistently identified, classified, tracked, and updated using standardized criteria. Consequently, inventory records may be incomplete, inaccurate, or outdated, limiting management's ability to effectively oversee assets connected to the organization's network and increasing the risk that unsupported, unmanaged, or unauthorized assets may not be identified in a timely manner.

RMA recommends the EAC's Chief Information Officer:

Recommendation 1: Develop, approve, and implement taxonomy policies and procedures governing the use of the agency's in-house asset inventory tool. The policies and procedures should require standardized data elements and taxonomy and define the specific inventory fields required to be captured and maintained within the tool.

Configuration Management

RMA determined that the EAC's overall maturity level for the Configuration Management domain was Managed and Measurable.

The EAC maintained qualitative and quantitative performance measures on the effectiveness of its configuration management plan. The EAC used automation to maintain an up-to-date, complete, accurate, and readily available view of the security configurations for information system components connected to the EAC's network. The EAC managed its vulnerabilities by using Security Content Automation Protocol-validated software scanning tools on all systems and providing scan reports. In addition, the EAC used automated mechanisms to detect unauthorized hardware, software, and firmware on its network and take immediate action to limit security impact and mitigate the spike in vulnerabilities. Our testing found no exceptions and controls operated as intended.

Identity and Access Management

RMA determined that the EAC's overall maturity level for the Identity and Access Management domain was Optimized.

EAC implemented single sign-on for its privileged and non-privileged users. In addition, they periodically reviewed and adjusted privileged user accounts and permissions, inventoried and validated the scope and number of privileged accounts, and ensured privileged user account

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

activities were logged and periodically reviewed. Our testing of the EAC's Identity and Access Management domain found no exceptions, and controls operated as intended.

Data Protection and Privacy

RMA determined that the EAC's overall maturity level for the Data Protection and Privacy domain was Consistently Implemented.

The EAC defined and communicated policies and procedures for protecting data at rest and data in transit through a media protection policy. The EAC used automated tools to protect personally identifiable information (PII) and other agency-sensitive data. The EAC used automated tools for monitoring all inbound and outbound network traffic to detect encrypted exfiltration, anomalous traffic patterns, and elements of PII. In addition, the EAC conducted phishing campaigns and used endpoint detection and response applications to monitor and log user activity and events.

The EAC made progress in closing FY 2025 recommendations 4 and 6[14] regarding removable media by implementing a process to detect and prevent the use of untrusted removable media on the EAC's network. While the EAC permits untrusted removable media on managed devices, it blocks such media from accessing the EAC network. However, the EAC was developing policies and procedures, as well as a clear business justification and risk acceptance process, for instances in which untrusted removable media must be introduced on managed devices. Therefore, RMA determined that FY 2025 recommendation 5 remains open.[15]

Security Training

RMA determined that the EAC's overall maturity level for the Security Training domain was Optimized.

The EAC performed roles and responsibilities related to security training, completed a workforce assessment, and provided annual security training. The EAC effectively allocated resources in a risk-based manner so stakeholders could implement security awareness training consistently. EAC addressed its identified knowledge, skills, and abilities gaps through talent acquisition. Our testing of the EAC's security training found no exceptions, and controls operated as intended.

Information Security Continuous Monitoring

We determined that the EAC's overall maturity level for the Information Security Continuous Monitoring (ISCM) domain was Consistently Implemented.

[14] Recommendations 4 and 6 in *Fiscal Year 2025 U.S. Election Assistance Commission Federal Information Security Modernization Act of 2014 Audit* (Audit Report No. P25HQ0063-25-07, September 29, 2025).
[15] Recommendation 5 in *Fiscal Year 2025 U.S. Election Assistance Commission Federal Information Security Modernization Act of 2014 Audit* (Audit Report No. P25HQ0063-25-07, September 29, 2025).

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

EAC monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its ISCM policies and strategy and made updates, as appropriate. In addition, the EAC used up-to-date cyber threat intelligence in log analysis tools to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise. EAC used results of security control assessments and monitoring to maintain ongoing authorizations of information systems, including maintaining system security plans.

We noted the EAC made progress in developing the ISCM strategy; however, the EAC did not document lessons learned to improve its ISCM program. Therefore, RMA noted FY 2024 recommendation 6[16] related to tracking lessons learned for the ISCM domain remains open.

Incident Response

RMA determined that the EAC's overall maturity level for the Incident Response domain was Managed and Measurable.

The EAC performed tabletop exercises yearly to evaluate the implementation of its incident response policies, and these exercises found the policies effective. The small organizational structure enabled the EAC to respond to and address security incidents quickly.

Contingency Planning

RMA determined that the EAC's overall maturity level for the Contingency Planning domain was Managed and Measurable.

EAC ensured that results of organizational Business Impact Analyses were integrated with enterprise risk management processes to consistently evaluate, record, and monitor the criticality and sensitivity of enterprise assets. We noted that the EAC conducted annual contingency plan tests and made progress by closing FY 2025 Recommendation 7.[17] While an interim reminder process was in place, the EAC needed to use an automated notification mechanism to test its system-level contingency plans thoroughly and effectively. Therefore, RMA determined that FY 2024 Recommendation 7[18] remains open.

Overall Conclusion

Consistent with applicable FISMA requirements, OMB policy, and guidance, and NIST standards and guidelines, we determined that the EAC's information security program and practices were established. They were maintained for the six Cybersecurity Framework function areas and 10 FISMA Metric Domains. We determined that the EAC's information security program and

[16] Recommendation 6 in *Fiscal Year 2024 U.S. Election Assistance Commission Federal Information Security Modernization Act of 2014 Audit* (Audit Report No. P24HQ0052-24-15, September 24, 2024).
[17] Recommendation 7 in *Fiscal Year 2025 U.S. Election Assistance Commission Federal Information Security Modernization Act of 2014 Audit* (Audit Report No. P25HQ0063-25-07, September 29, 2025).
[18] Recommendation 7 in *Fiscal Year 2024 U.S. Election Assistance Commission Federal Information Security Modernization Act of 2014 Audit* (Audit Report No. P24HQ0052-24-15, September 24, 2024).

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

practices were effective for FY 2026, though the overall maturity level was Consistently Implemented. Although our assessment identified exceptions and one new finding this year, we determined that the EAC's cybersecurity programs were sufficiently designed and operated as intended.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Objective, Scope, and Methodology

Objective

The objective of this performance audit was to evaluate the effectiveness of the EAC's information security program and practices, and to determine the maturity level achieved for each core and supplemental metric outlined in the *FY 2025 IG FISMA Reporting Metrics v2.0*. Specifically, the performance audit determined whether the EAC implemented an effective information security program by evaluating the six Cybersecurity Framework function areas as divided into 10 FISMA Metric Domains:

- **Govern**, which includes metrics pertaining to cybersecurity governance and cybersecurity supply chain risk management domains;
- **Identify**, which includes metrics pertaining to risk and asset management domain;
- **Protect**, which includes metrics pertaining to configuration management, identity and access management, data protection and privacy, and security training domain;
- **Detect**, which includes metrics pertaining to information security continuous monitoring domain;
- **Respond**, which includes metrics pertaining to incident response domain; and
- **Recover**, which includes metrics pertaining to contingency planning domain.

Scope

We conducted this performance audit 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The scope of the FISMA performance audit work was agency-wide, and the review covered FY 2026 as of July 31, 2026. We assessed three FISMA reportable systems from the EAC's inventory of information systems. The performance audit fieldwork was conducted at the EAC's headquarters in Washington, DC, between April 15, 2026 and July 31, 2026. This performance audit included steps to follow up on prior-year FISMA-related recommendations. **Appendix I**: Status of Prior Year Recommendations summarizes the status of prior year recommendations.

Methodology

The overall strategy of our performance audit considered: (1) NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*; (2) NIST SP 800-53A, Revision 5.2.0, *Assessing Security and Privacy Controls in Information Systems and Organizations*; (3) *FY 2025 IG FISMA Reporting Metrics v2.0*; and (4) the EAC's policies and procedures. We developed our testing procedures from NIST SP 800-53A, Revision 5.2.0.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

We interviewed EAC officials and reviewed the legal and regulatory requirements stipulated in FISMA. We also examined documents supporting the information security program and practices. We compared the EAC information technology policies and procedures to requirements stipulated in NIST SPs. Additionally, we conducted tests of system processes to assess the design and operating effectiveness of controls.

OMB's *FY 2025 IG FISMA Reporting Metrics v2.0* directed IGs to report maturity levels in CyberScope.[19] For each of the 20 core and five supplemental metric questions in *FY 2025 IG FISMA Reporting Metrics v2.0*, we assessed EAC's implementation against the applicable maturity-level criteria. We evaluated each criterion to determine whether it was satisfied. Those results formed the basis of the EAC's maturity level for each metric. We averaged the core and supplemental metrics separately to determine each domain's overall maturity level and assess the effectiveness of the EAC's information security program and functions.

We evaluated the effectiveness of the EAC's information security programs and practices on a maturity model spectrum, in which foundation levels ensure the development of sound policies and procedures. The FY 2026 IG Metrics classify information security programs and practices into five maturity levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized (**Table 2**). Within the maturity model, Levels 4 (Managed and Measurable) and 5 (Optimized) represent an effective level of security. OMB shifted its emphasis away from a purely compliance-based evaluation lens toward one more focused on risk management-based security outcomes. IGs can now consider both their own and the agency's assessments of effectiveness, depending on their unique missions, resources, and challenges, when determining the effectiveness of the information security program. IGs are encouraged to evaluate the metrics based on threat models, the risk tolerance of their respective agencies, and the practical security impact of control implementation rather than strictly forming their evaluation based on the presence or absence of controls. As such, IGs have the discretion to determine that an agency's information security program is effective even if the agency does not achieve Level 4.[20]

Table 2: FISMA Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad Hoc	Policies, procedures, and strategies were not formalized; activities were performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies were formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies were consistently implemented, but quantitative and qualitative effectiveness measures were lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies were collected across the organization and used to assess them and make necessary changes.

[19] CyberScope is a web-based platform to streamline the reporting of information security practices required under FISMA. As mandated by OMB and DHS, federal agencies must collect FISMA performance metrics data and upload the results into CyberScope.
[20] *FY 2025 IG FISMA Reporting Metrics v2.0*, April 3, 2025.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Maturity Level	Maturity Level Description
Level 5: Optimized	Policies, procedures, and strategies were fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

For FY 2026, IGs used the *FY 2025 IG FISMA Reporting Metrics v2.0* and focused on a calculated weighted average approach, wherein the average of metrics in a particular domain determined the effectiveness of individual function areas (govern, identify, protect, detect, respond, and recover) and the overall program. To give IGs more flexibility and encourage audits based on agencies' risk tolerance and threat models, calculated averages were not automatically rounded (i.e., rounded up or down based on mathematical rules) to a particular maturity level. In the calculated average scoring model, core metrics and supplemental metrics were calculated independently to determine a domain's maturity calculation and provide data points for assessing program and function area effectiveness. For example, if the calculated core metric maturity of two of the function areas was Level 3 (Consistently Implemented) and the calculated core metric maturity of the remaining four function areas was Level 4 (Managed and Measurable). The information security program rating would average 3.60.[21]

Table 3 presents the EAC's FY 2026 calculated core metric, supplemental metric, assessed maturity averages, and assessed maturity level by function area_Ref172213409.

Table 3: Overall Calculated Averages Maturity Calculation in FY 2026

Function Area	Core Metrics	Supplemental Metrics[22]	Assessed Maturity
Govern[23]	4.00	3.67	Consistently Implemented
Identify	3.20	1.00	Defined
Protect	4.25	-	Managed and Measurable
Detect	3.00	4.00	Consistently Implemented
Respond	4.50	-	Managed and Measurable
Recover	4.00	-	Managed and Measurable
Overall Maturity Overall	**3.83**	**2.89**	**Consistently Implemented Effective**

For FY 2026, the assessed maturity average was computed by averaging the core and supplemental metrics. RMA did not round the calculated averages when determining the maturity level. To determine maturity levels and the overall effectiveness of EAC's information security program, RMA focused on the core metric results and made a risk-based assessment of overall program and function-level effectiveness.

Since FY 2025, OMB and CIGIE have piloted a weighted-average approach to IG FISMA scoring that gives greater weight to certain foundational cybersecurity metrics and accounts for dependencies between them. The goal was to reflect cybersecurity effectiveness better, recognizing that areas such as Cybersecurity Governance and Risk and Asset Management support

[21] Ibid.
[22] Protect, Respond, and Recover only consist of Core Metrics.
[23] The Govern Function Area was introduced in FY 2025.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

the successful implementation of activities like continuous monitoring, configuration compliance, and ongoing authorizations. The weighted scoring was calculated automatically through CyberScope. According to *FY 2025 IG FISMA Reporting Metrics v2.0,* foundational metrics are metrics 1, 2, 3, 7, 8, 9, 10 and 33. The weighted average approach was: ((FY 2025 Foundational Metric Maturity x 2) + (FY 2025 Remaining Core x 1))/3.[24]

Criteria

We applied the following criteria for performing the EAC's FY 2026 FISMA audit.

NIST Federal Information Processing Standards (FIPS) and SPs

- *NIST CSF 2.0*
- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS Publication 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, Revision 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 800-40, Revision 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*
- NIST SP 800-50, Revision 1, *Building a Cybersecurity and Privacy Learning Program*
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-53A, Revision 5.2.0, *Assessing Security and Privacy Controls in Information Systems and Organizations*
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*
- NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST SP 800-61, Revision 3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*
- NIST SP 800-63-4, *Digital Identity Guidelines*
- NIST SP 800-83, Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*

[24] *FY 2025 IG FISMA Reporting Metrics v2.0*, April 3, 2025.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-161, Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
- NIST SP 800-181, Revision 1, *Workforce Framework for Cybersecurity* (*NICE Framework)*
- NIST SP 800-207, *Zero Trust Architecture*
- NIST SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1, Recommendations for Mitigating the Risk of Software Vulnerabilities*
- NIST Interagency Report 8011, *Automation Support for Security Control Assessments: Volume 1: Overview*
- NIST Interagency Report 8011, *Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management*
- NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*

OMB Policy Directives

- *FY 2025 IG FISMA Reporting Metrics v2.0*
- OMB Memorandum M-26-14, *Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats*
- OMB Memorandum M-26-05, *Adopting a Risk-based Approach to Software and Hardware Security*
- OMB Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*
- OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*
- OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*
- OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*
- OMB Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures*
- OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

- OMB Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*
- OMB Memorandum M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*
- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*

Cybersecurity and Infrastructure Security Agency

- Binding Operational Directive (BOD) 26-04, *Prioritizing Security Updates Based on Risk*
- BOD 26-02, *Mitigating Risk From End-of-Support Edge Devices*
- BOD 25-01, *Implementing Secure Practices for Cloud Services*
- BOD 23-02, *Mitigating the Risk from Internet-Exposed Management Interfaces*
- BOD 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*
- BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy*
- BOD 18-02, *Securing High Value Assets*
- BOD 18-01, *Enhance Email and Web Security*
- BOD 17-01, *Removal of Kaspersky-Branded Products*
- BOD 16-03, *2016 Agency Cybersecurity Reporting Requirements*
- BOD 16-02, *Threat to Network Infrastructure Devices*
- Emergency Directive (ED) 26-03, Version 1, *Mitigate Vulnerabilities in Cisco SD-WAN Systems*
- ED 26-01, *Mitigate Vulnerabilities in F5 Devices*
- ED 25-03, *Identity and Mitigate Potential Compromise of Cisco Devices*
- ED 25-02, *Mitigate Microsoft Exchange Vulnerability*
- ED 24-01, *Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Appendix I: Status of Prior Year Recommendations

Table 4: Status of Prior Year Recommendations

Audit Report and Recommendation No.	Audit Recommendations	Auditor's Position on Status
(FY 2024 Audit Report P24HQ0052-24-15) 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.	**Closed** **See Cybersecurity Supply Chain Risk Management section.**
(FY 2024 Audit Report P24HQ0052-24-15) 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.	**Open** **See Information Security Continuous Monitoring section.**
(FY 2024 Audit Report P24HQ0052-24-15) 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.	**Open** **See Contingency Planning section.**
(FY 2025 Audit Report P25HQ0063-25-07) 1	Develop and implement a contingency plan to address potential future staffing challenges that may arise, to mitigate delays in implementing necessary improvements across the applicable FISMA domains.	**Open** **See Risk and Asset Management section.**
(FY 2025 Audit Report P25HQ0063-25-07) 2	Establish and execute a monitoring plan to make sure that all information technology policies and procedures, including referenced standards and guidance, are reviewed and updated in accordance with the timeliness requirements defined by EAC policy.	**Open** **See Risk and Asset Management section.**
(FY 2025 Audit Report P25HQ0063-25-07) 3	Implement a continuous monitoring governance, risk, and compliance tool that enables the integration of cybersecurity risk management into the enterprise risk management reporting tool. Capture lessons learned to make any necessary adjustments to the process.	**Open** **See Risk and Asset Management section.**
FY 2025 Audit Report P25HQ0063-25-07) 4	Implement a process to detect and prevent the use of untrusted removable media on the EAC's network.	**Closed** **See Data Protection and Privacy section.**

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Audit Report and Recommendation No.	Audit Recommendations	Auditor's Position on Status
(FY 2025 Audit Report P25HQ0063-25-07) 5	Fully document and implement a process that includes a clear business reason for risk acceptance in the event that untrusted removable media must be introduced on the EAC's network.	**Open** **See Data Protection and Privacy section.**
(FY 2025 Audit Report P25HQ0063-25-07) 6	Develop compensating controls to reduce the risk that vulnerabilities can be exploited that are caused by the use of untrusted removable media on the EAC's network.	**Closed** **See Data Protection and Privacy section.**
(FY 2025 Audit Report P25HQ0063-25-07) 7	Schedule and complete annual contingency planning tests. Retain supporting documentation to demonstrate compliance during audits.	**Closed** **See Contingency Planning section**

Appendix II: Management Response

TO: U.S. Election Assistance Commission, Inspector General, Sarah Dreyer
FROM: U.S. Election Assistance Commission, CIO/CISO, Jessica Bowers
DATE: November 5, 2026
SUBJECT: Response to Draft FISMA Audit Report FY2026

The Office of the Chief Information Officer (OCIO) provides the following responses to the Inspector General's FY2026 FISMA audit findings and recommendations.

1. **Develop, approve, and implement taxonomy policies and procedures governing the use of the agency's in-house asset inventory tool. The policies and procedures should require standardized data elements and taxonomy and define the specific inventory fields required to be captured and maintained within the tool.**

   Management Response: Agree

   The EAC will develop and approve asset inventory policies and procedures that establish standardized data elements and taxonomy for hardware assets, software assets, software licenses, EO-critical software, and mobile applications. The procedures will define the specific fields required to be captured and maintained within the in-house asset inventory tool, the responsibilities for maintaining inventory records, and the frequency of inventory review and validation. The EAC will also update its process for deploying new security capabilities so that supporting policies and procedures are approved before the capability is placed into production.

   Estimated completion date: December 2026

Status of Open Prior-Year Recommendations

The OCIO provides the following updates on recommendations from prior FISMA audits that remain open.

FY 2025 Recommendation 1: Develop and implement a contingency plan to address potential future staffing challenges that may arise, to mitigate delays in implementing necessary improvements across the applicable FISMA domains.

Status: The FY 2025 audit attributed delays across several FISMA domains to staffing challenges and competing priorities within OCIO. The EAC will document and approve an OCIO staffing contingency plan that identifies the roles critical to the information security program, designates primary and backup personnel for each role, defines cross-training requirements, and establishes the conditions under which expert contractor support will be activated through existing agreements. The plan will be reviewed on an as needed basis.

The EAC will provide the approved plan, the supporting skills analysis matrix, and records of completed cross-training to the OIG to support closure.

Revised estimated completion date: March 2027

FY 2025 Recommendation 2: Establish and execute a monitoring plan to make sure that all information technology policies and procedures, including referenced standards and guidance, are reviewed and updated in accordance with the timeliness requirements defined by EAC policy.

Status: The FY 2025 audit identified outdated standards and guidance references in policies and procedures across multiple FISMA domains. The EAC will review each OCIO policy and procedure and update its references to current federal requirements, including the current release of NIST SP 800-53 and current OMB memoranda and CISA directives. The EAC will maintain an inventory of these documents that records the owner, approval date, last review date, and next required review date, with automated notifications to owners in advance of each due date. Because the FY 2026 report also cites the absence of a process to maintain an inventory of data and corresponding metadata, the EAC will issue guidance governing data assets and their metadata, including associated roles and responsibilities.

Revised estimated completion date: December 2026

FY 2025 Recommendation 3: Implement a continuous monitoring governance, risk, and compliance tool that enables the integration of cybersecurity risk management into the enterprise risk management reporting tool. Capture lessons learned to make any necessary adjustments to the process.

Status: The EAC has replaced its deprecated GRC tool with an internally developed application and has implemented continuous monitoring within it. Consistent with OMB Circular A-123, OMB Circular A-130, and NIST IR 8286, the EAC will maintain a cybersecurity risk register within this tool and will roll up cybersecurity risks, including plan of action and milestones items and accepted risks, into the enterprise risk register and enterprise risk management reporting on am as needed basis. The EAC will document lessons learned from the initial reporting cycles and adjust the process accordingly.

Revised estimated completion date: September 2027

FY 2025 Recommendation 5: Fully document and implement a process that includes a clear business reason for risk acceptance in the event that untrusted removable media must be introduced on the EAC's network.

Status: The EAC does not block untrusted removable media on the EAC network. The EAC instead mitigates the associated risk through compensating controls, including continuous monitoring by its endpoint detection and response solution, which detects and blocks malicious activity, and data loss prevention controls that prevent the exfiltration of sensitive information, including personally identifiable information. These controls allow the EAC to manage removable media risk through a risk-based decision-making approach

consistent with NIST SP 800-53 control MP-7. To address this recommendation, the EAC will formally document the business justification for permitting untrusted removable media and the associated risk acceptance by the Chief Information Officer, including the compensating controls on which that acceptance relies.

Revised estimated completion date: December 2026

FY 2024 Recommendation 6: Establish and implement a formal Information Security Continuous Monitoring Strategy and an effective monitoring mechanism to track the progress of ongoing lessons learned.

Status: The EAC developed its Information Security Continuous Monitoring (ISCM) strategy in FY 2025. The EAC will establish an ISCM lessons-learned register that records lessons identified from control assessments, ongoing authorization reviews, incident and exercise after-action reports, and metric reviews, along with the corrective action, owner, due date, and status of each. The EAC will review the register on an as needed basis, incorporate resulting changes into the ISCM strategy, and provide the register and evidence of its review to the OIG.

Revised estimated completion date: March 2027

FY 2024 Recommendation 7: Identify and employ an automated notification mechanism to test its system level contingency plans thoroughly and effectively.

Status: The EAC conducts annual contingency plan tests and currently uses an interim manual reminder process. The EAC will implement an automated mechanism that schedules system-level contingency plan tests, notifies responsible personnel in advance, tracks completion and test results, and escalates overdue tests. The EAC will retain the records generated by the mechanism to demonstrate that tests were scheduled and completed.

Revised estimated completion date: March 2027

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Appendix III: Evaluation of Management Response

The EAC concurred with our finding and recommendation. After reviewing the EAC's response, we consider it to be responsive to our recommendation, and the actions taken and planned should resolve the issues identified in the report. Therefore, the recommendation will remain open until the EAC provides documentation to verify appropriate actions have been taken.

4121 Wilson Blvd., Suite 1100
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Appendix IV: Glossary of Acronyms

BOD	Binding Operational Directive
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CSF	Cybersecurity Framework
DHS	Department of Homeland Security
C-SCRM	Cybersecurity Supply Chain Risk Management
ED	Emergency Directive
EO	Executive Order
EAC	Election Assistance Commission
ERM	Enterprise Risk Management
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
HAVA	Help America Vote Act of 2002
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
RMA	RMA Associates, LLC
SP	Special Publication



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