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 2025

Report No. P25HQ0063-25-07
September 29, 2025

HIGHLIGHTS

AUDIT OF THE EAC'S COMPLIANCE WITH FISMA FOR FISCAL YEAR 2025

Report No. P25HQ0063-25-07 September 29, 2025

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 2025 in support of the Federal Information Security Modernization Act of 2014 (FISMA).

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

- 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 audit determined that the EAC's information security program and practices were effective for fiscal year 2025. However, some exceptions were identified. Specifically, the EAC had not:

- Developed and implemented an IT staffing contingency plan.
- Updated all information technology policies and procedures.
- Integrated cybersecurity risk management into enterprise risk management.
- Implemented procedures to ensure that the systems and services provided by outside entities meet FISMA requirements.
- Implemented a process to detect and prevent the use of untrusted removable media or justified why one is not needed.
- Established a monitoring mechanism to track progress on its continuing monitoring strategy.
- Completed annual contingency plan testing.
- Employed mechanisms to automate the testing of system contingency plans.

What Was Recommended

The audit made seven recommendations to improve EAC's security posture, and three from the prior year remain open.

U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL

DATE: September 29, 2025

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 2025 (Report No. P25HQ0063-25-07)

This memorandum transmits the final report on the U.S. Election Assistance Commission's Compliance with the Federal Information Security Modernization Act (FISMA) for Fiscal Year 2025. The Office of Inspector General contracted RMA Associates, LLC, an independent certified public accounting firm, to conduct the audit. The contract required that the audit be performed in accordance with U.S. generally accepted government auditing standards.

RMA is responsible for the attached auditor's report dated September 29, 2024, and the conclusions expressed therein. While the Office of Inspector General coordinated and monitored RMA's performance under the contract, we did not evaluate their adherence to standards and therefore do not express an opinion on the EAC's compliance with FISMA.

The report contains 7 recommendations. Please keep us informed of the actions taken to resolve them, 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 Donald L. Palmer, Chairman
Commissioner Thomas Hicks, Vice Chair
Commissioner Christy McCormick
Commissioner Benjamin W. Hovland

RMA Associates
Auditors. Consultants. Advisors.

United States Election Assistance Commission

Federal Information Security Modernization Act of 2014

Performance Audit Report for Fiscal Year 2025

RMA | Associates
Auditors. Consultants. Advisors.

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

September 29, 2025

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

Re: United States Election Assistance Commission Federal Information Security Modernization Act of 2014 Performance Audit Report for Fiscal Year 2025

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) 2025. 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 of the core metrics and supplemental metrics outlined in the *FY 2025 Inspector General (IG) FISMA Reporting Metrics v2.0*. The performance audit fieldwork was conducted in Washington, DC, from April 9, 2025, to August 1, 2025.

Based on the results of our performance audit, we determined that the EAC's information security program and practices were effective for FY 2025, as the criteria assessed for EAC's information security program met the maturity level of Consistently Implemented. Our assessment of the information security program identified one new finding associated with the 10 FISMA Metric Domains. Further, seven of 10 prior FISMA performance audit recommendations were closed.

Our report includes **Appendices I**: Status of Prior Year Recommendations, **II:** Management Response, **III**: Evaluation of Management Response, and **IV**: Glossary of Acronyms. Further details of our findings and recommendations are included in the accompanying report.

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 the guidelines established by the OMB, Department of Homeland Security (DHS), and National Institute of Standards and Technology (NIST). We selected and assessed all three FISMA reportable systems from the EAC's FISMA inventory of information systems.

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

For FY 2025, OMB required Inspector Generals to assess 25 metrics from FY *2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025, including both core and supplemental metrics. These metrics are coordinated and agreed upon by the Council of the Inspectors General on Integrity and Efficiency, the Chief Information Security Officer, OMB, and the Cybersecurity and Infrastructure Security Agency. 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 FY 2025 IG 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. The *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025, classifies information security programs and practices into five maturity levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

We have also prepared responses to the OMB's M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* guidance, encouraging agencies to shift towards a continuous assessment process for their annual independent assessment using *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025 and the submission of 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 obtained from the EAC on or before August 1, 2025. We are not obligated to update our report or revise the information contained therein to reflect events occurring after August 1, 2025.

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

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

Table of Contents

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) information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires Federal agencies to conduct an annual independent performance audit for evaluation of their information security programs and practices to determine the effectiveness of these programs and practices, and to report the results of the performance audits 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 the FISMA performance audit requirement. 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 of the core metrics and supplemental metrics outlined in the *FY 2025 Inspector General (IG) FISMA Reporting Metrics v2.0*, dated April 3, 2025.

As part of our performance audit, we responded to the FY 2025 20 core and five supplemental metrics specified in OMB's *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025.[1] These metrics provide reporting requirements across the function areas to be addressed in the independent assessment of agencies' information security programs.[2] We also considered applicable EAC and OMB policies and guidelines, as well as the National Institute of Standards and Technology (NIST) standards, where applicable.

Background

United States Election Assistance Commission

The EAC was established by the Help America Vote Act of 2002 (HAVA). 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 of information on election administration. 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. The law also established the Technical Guidelines Development Committee to assist the EAC in the development of voluntary voting system guidelines. The EAC also holds public meetings and hearings to inform the public about its progress and activities.

[1] OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the *IG FISMA Reporting Metrics* in consultation with the Federal Chief Information Officers Council.
[2] Refer to the section titled, *Objective, Scope, and Methodology* for more details.

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

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 agencies, including the EAC, have an independent OIG that is authorized by law to conduct audits and investigations to prevent and detect fraud, waste, and abuse to promote the economy, efficiency, effectiveness, and to safeguard the integrity of the EAC programs and operations.

Federal Information Security Modernization Act of 2014

Title III of the *E-Government Act*, entitled the *Federal Information Security Management Act of 2002*, required each Federal agency to develop, document, and implement an agency-wide program to provide security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources. FISMA amended the *Federal Information Security Management Act of 2002* and provided several modifications that modernize Federal security practices to address evolving security concerns. These changes resulted in less overall reporting, strengthened the use of continuous monitoring in systems, and increased focus on the agencies for compliance and reporting that is more concentrated on the issues caused by security incidents.

FISMA, along with the *Paperwork Reduction Act of 1995* and the *Information Technology Management Reform Act of 1996* (also known as the Clinger-Cohen Act), explicitly emphasizes a risk-based approach to cost-effective security. In support of and reinforcing this legislation, OMB, through Circular No. A-130, *Managing Information as a Strategic Resource*, requires executive agencies within the Federal government to:

- Plan for security;
- Ensure that appropriate officials are assigned security responsibilities;
- Periodically review the security controls in its systems; and
- Authorize system processing prior to operations and periodically after that.

These management responsibilities presume that responsible agency officials understand the risks and other factors that could adversely affect the organization's missions. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information and systems, and make informed judgments and investments that appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct the Commission's day-to-day operations and accomplish its stated mission with adequate security or security commensurate with risk, including the magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information.

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

FISMA provided OMB with oversight authority over agency security policies and practices and authorized the implementation of agency policies and practices for information systems to DHS.[3]

FISMA required the Secretary of DHS to develop and oversee the implementation of operational directives that require agencies to implement OMB standards and guidelines for safeguarding Federal information and systems from known or reasonably suspected information security threats, vulnerabilities, or risks. FISMA directed the Secretary to consult with and consider guidance developed by NIST to ensure operational directives do not conflict with NIST information security standards.[4] FISMA authorized the Director of OMB to revise or repeal operational directives not in accordance with the Director's policies.[5]

Additionally, FISMA directed Federal agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General of the U.S. Government Accountability Office (GAO). The reports are required to include: (1) threats and threat actors, vulnerabilities, and impacts of the incidents; (2) risk assessments of affected systems before the incidents; (3) the status of system compliance at the time of the incidents; (4) detection, response, and remediation actions; (5) total number of incidents; and (6) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information.[6]

Key Changes to the FY 2025 IG FISMA Metrics

One of the goals of the annual FISMA audits is to assess agencies' progress toward achieving objectives that strengthen Federal cybersecurity. The *IG FISMA Reporting Metrics v2.0* have been updated to determine agency progress in achieving the objectives, as follows:

- NIST *Cybersecurity Framework 2.0*: NIST published 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.

[3] FISMA, Pub. L. No. 113-283, 128 Stat. 3073, December 2014, https://www.congress.gov/bill/113th-congress/senate-bill/2521.
[4] Ibid.
[5] Ibid.
[6] Ibid.

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

In addition, to align with the CSF 2.0, the supply chain risk management (SCRM) domain was moved from the Identify function area to the Govern function area and renamed to 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 include 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.
- 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.

FY 2025 Core and Supplemental IG Metrics

OMB's *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025, specified the FY 2025 20 Core and five Supplemental IG Metrics. It directed IGs to report the assessed maturity levels of these metrics in CyberScope[7] no later than August 1, 2025. The FY 2025 FISMA IG Metrics were aligned with the six function areas in the NIST *Cybersecurity Framework 2.0* as follows:

- Govern, includes metrics pertaining to Cybersecurity Governance and Cybersecurity Supply Chain Risk Management;
- Identify, includes metrics pertaining to Risk and Asset Management;
- Protect, includes metrics pertaining to Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training;
- Detect, includes metrics pertaining to Information Security Continuous Monitoring;
- Respond, includes metrics pertaining to Incident Response; and
- Recover, includes metrics pertaining to Contingency Planning.

We evaluated the effectiveness of the EAC's information security programs and practices on a maturity model spectrum, in which the foundation levels ensure the development of sound policies and procedures. The FY 2025 IG Metrics classifies information security programs and practices into five maturity levels: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized (**Table 1**). Within the context of the maturity model, Levels 4 (Managed and Measurable) and 5 (Optimized) represent an effective level of security. It is important to note that OMB shifted its emphasis away from a purely compliance-based evaluation lens in favor of 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

[7] 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.

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

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.[8]

Table 1: IG Audit 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.
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 2025, IGs continued to focus on a calculated weighted average approach, wherein the average of the metrics in a particular domain will determine the effectiveness of individual function areas (govern, identify, protect, detect, respond, and recover) and the overall program. To provide IGs with additional flexibility and encourage evaluations 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 FY 2025 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 is Level 3 (Consistently Implemented) and the calculated core metric maturity of the remaining three function areas is Level 4 (Managed and Measurable), then the information security program rating would average a 3.60.[9]

Summary Performance Audit Results

We determined that, consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, the EAC's information security program and practices were

[8] *FY 2025 IG FISMA Reporting Metrics v2.0*, April 3, 2025, pages 7 - 9.
[9] *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

established and maintained for the six Cybersecurity Framework function areas[10] and 10 FISMA Metric Domains.[11] The overall maturity level of the EAC's information security program was determined as Consistently Implemented, as described in this report. We determined that the EAC's information security program and practices were effective for FY 2025.

NOTE: Based on the EAC's risk tolerance and threat models, RMA used discretion to determine the overall effectiveness of the EAC's information security program, in accordance with Cybersecurity Framework function area effectiveness (e.g., Identify, Protect), and the individual domain ratings (e.g., risk and asset management, configuration management). Using this approach, RMA determined that a particular domain, function area, and/or the EAC's information security program was effective even though the overall calculated maturity level was lower than 4.0.

RMA identified one new finding to address the weakness found in the function areas of Identify, Protect, and Recover. RMA made seven recommendations to address the finding.

The EAC made considerable progress in implementing the recommendations from the prior year. During FY 2025, the EAC resolved seven of 10 open recommendations from the FY 2022 to FY 2024 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: 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 results of the core metrics 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.

The EAC's FY 2025 calculated core metric, supplemental metric, assessed maturity averages, and assessed maturity level by function area are presented in **Table 2**.

[10] 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*.

[11] 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

Table 2: Overall Calculated Averages Maturity Calculation in FY 2025

Function Area	Core Metrics	FY 2025 Supplemental Metrics[12]	FY 2025 Assessed Maturity Average[13]	FY 2025 Assessed Maturity
Govern[14]	4.00	3.67	3.71	Consistently Implemented
Identify	3.80	1.00	3.40	Consistently Implemented
Protect	4.13	-	4.13	Managed and Measurable
Detect	3.00	4.00	3.00	Consistently Implemented
Respond	4.50	-	4.50	Managed and Measurable
Recover	3.50	-	4.00	Managed and Measurable
Overall Maturity	**3.82**	**2.89**	**3.79**	**Consistently Implemented**

The maturity level for the 10 FISMA Metric Domains is presented in **Table 3**.

Table 3: EAC's FY 2025 Maturity Levels

• Cybersecurity Governance	Consistently Implemented (Level 3)
• Cybersecurity Supply Chain Risk Management	Managed and Measurable (Level 4)
Govern – Cybersecurity Governance and Cybersecurity Supply Chain Risk Management	**Consistently Implemented (Level 3)**
Identify – Risk and Asset Management	**Consistently Implemented (Level 3)**
• Configuration Management	Managed and Measurable (Level 4)
• Identity and Access Management	Managed and Measurable (Level 4)
• Data Protection and Privacy	Consistently Implemented (Level 3)
• Security Training	Optimized (Level 5)
Protect – Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training	**Managed and Measurable (Level 4)**
Detect – Information Security Continuous Monitoring	**Consistently Implemented (Level 3)**
Respond – Incident Response	**Managed and Measurable (Level 4)**
Recover – Contingency Planning	**Managed and Measurable (Level 4)**
Overall	**Consistently Implemented (Level 3)**
Overall	**Effective[15]**

Cybersecurity Governance

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

EAC continuously monitored its cybersecurity risk management program in near real-time, leveraging predictive analytics and threat intelligence to proactively adjust strategies. In addition, the EAC's leadership held personnel accountable and enforced organizational cybersecurity

[12] Protect, Respond, and Recover only consist of Core Metrics.
[13] The FY 2025 Assessed Maturity Average was calculated by averaging the Core and Supplemental Metrics. The calculated averages were truncated to determine the maturity level. In determining maturity levels and the overall effectiveness of Council's information security program, RMA focused on the results of the Core Metric and made a risk-based determination of overall program and function level effectiveness.
[14] The Govern Function Area was introduced in FY 2025.
[15] RMA made a risk-based determination of overall program and function level effectiveness.

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

requirements. However, the EAC had not developed a formal process for tracking progress toward target cybersecurity profiles.

RMA's testing found exceptions in the Cybersecurity Governance domain, and the existing controls were not operating as intended. We concluded that the EAC's Cybersecurity Governance controls in place were not effective.

Cybersecurity Supply Chain Risk Management

We determined that the EAC's overall maturity level for the C-SCRM domain was Managed and Measurable.

The EAC established a C-SCRM policy and procedures, which were communicated to stakeholders. The EAC made progress in closing the prior year's recommendation by identifying qualitative and quantitative metrics on service level agreements held with third parties, then performed an analysis with monthly reporting received from those third parties to identify metrics that could be measured and documented, on either a monthly or quarterly basis. Hence, RMA determined that FY 2024 Recommendation 1 is closed.[16] In addition, the EAC conducted counterfeit training for designated personnel to effectively identify counterfeit system components, including hardware, software, and firmware. Hence, RMA determined that FY 2024 Recommendation 3 is closed.[17]

Although EAC made progress on closing prior year recommendations, it had not developed and implemented 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. A recommendation addressing this finding was issued in the FY 2024 FISMA audit report.[18] Because that recommendation remains open, we are not making a new recommendation.

RMA's testing found no exceptions, and the controls were operating as intended. We concluded the EAC's C-SCRM controls in place were effective.

Risk and Asset Management

We determined that the EAC's overall maturity level for the Risk and Asset Management domain was Consistently Implemented. We identified two weaknesses. One issue was related to outdated standards and guidance references in their policies and procedures.[19] Second, EAC had not

[16] *Audit of the U.S. Election Assistance Commission's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2024* (Audit Report No. P24HQ0052-24-15, September 24, 2024), Recommendation 1.
[17] Ibid, Recommendation 3.
[18] Ibid, Recommendation 2.
[19] RMA found policies and procedure issue for other FISMA domains; however, for reporting purpose it was only mentioned once.

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

integrated cybersecurity risk management information into enterprise reporting tools (such as governance, risk management, and compliance tools), as appropriate.

Based on NIST Special Publication (SP) 800-53, Revision 5.1.1, "*Security and Privacy Controls for Information Systems and Organizations*," there are 18 controls specifically addressing policies and procedures. The first control of each control family specifies that the organization reviews and updates the current policy and procedures in an Assignment: organization-defined frequency:

> a. Reviews and updates the current:
> 1. Control policy [*Assignment: organization-defined frequency*]; and
> 2. Control procedures [*Assignment: organization-defined frequency*].

Also, OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

> Purpose: This Circular defines management's responsibilities for enterprise risk management (ERM) and internal control. The Circular provides updated implementation guidance to Federal managers to improve accountability and effectiveness of Federal programs as well as mission support operations through implementation of ERM practices and by establishing, maintaining, and assessing internal control effectiveness. The Circular emphasizes the need to integrate and coordinate risk management and strong and effective internal control into existing business activities and as an integral part of managing an Agency.

OMB Circular No. A-130, *Managing Federal Information as a Strategic Resource*, Appendix I, states the following in Section 3, *General Requirements*:

> a. Agencies shall implement an agency-wide risk management process that frames, assesses, responds to, and monitors information security and privacy risk on an ongoing basis across the three organizational tiers (i.e., organization level, mission or business process level, and information system level).
> b. Agencies shall develop, implement, document, maintain, and oversee agency-wide information security and privacy programs including people, processes, and technologies to:
> 1. Provide for agency information security and privacy policies, planning, budgeting, management, implementation, and oversight.

EAC management indicated that staffing challenges within the information technology division led to increased workloads for key personnel. Additionally, competing organizational priorities diverted attention and resources, contributing to delays in implementing necessary improvements across the applicable FISMA domains.

Without updating policies and procedures and implementing an automated risk management solution across the enterprise, staff may follow obsolete or non-compliant practices, increasing the risk of not meeting current federal requirements (e.g., NIST SP 800-53 Revision 5.1.1). This can

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

lead to audit findings and a weakened security posture. In addition, key risk indicators may be siloed or overlooked, leading to poor visibility into enterprise risks and delayed decision-making. This weakens the EAC's ability to manage threats strategically and hinders accountability and prioritization.

RMA recommends the Chief Information Officer:

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.
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.
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.

RMA also noted the EAC had not drafted guidance on managing and governing the EAC's metadata, processes, procedures, roles, and responsibilities related to data assets. EAC's Risk Management Framework outlined roles and processes for risk management, including preparation, categorization, implementation, authorization, and monitoring. The EAC actively managed and measured its information systems to maintain comprehensive inventories and security across its platforms. For hardware, the EAC employed automated systems to track the lifecycle of hardware assets connected to the network, including mobile devices. The EAC denied access to mobile device users not complying with security updates, in accordance with the EAC's policies. In software management, the EAC used automated systems to manage the inventory of software assets and associated licenses. The EAC's security measures included preventing unauthorized software execution and enhancing the security of mobile and other applications.

The EAC made progress in closing the prior year's recommendation by updating its Plan of Action and Milestones (POA&M) procedures and associated reports in accordance with Federal requirements. Hence, RMA confirmed that FY 2023 Recommendation 4 is closed.[20]

RMA's testing found exceptions in the Risk and Asset Management domain, and the existing controls were not operating as intended. We concluded that the EAC's Risk and Asset Management controls in place were not effective.

[20] *Audit of the U.S. Election Assistance Commission's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2023* (Audit Report No. O23HQ0029-23-07, August 94, 2023), Recommendation 4.

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

Configuration Management

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

The EAC established Configuration Management guidelines through its Configuration Management policies and procedures. The EAC's Configuration Management policy outlined processes for identifying, managing, monitoring, and reporting configuration management activities. The EAC used a Security Content Automation Protocol tool to view configuration settings and status on all workstations and devices in the system. The EAC managed its flaw remediation process and used an automated process for ingesting vulnerabilities. The EAC made progress in closing the prior year's recommendations by remediating vulnerabilities in the network identified, according to the agency's policy, and documenting the results or accepting the risks associated with those vulnerabilities. In addition, the EAC developed and implemented a remediation plan for vulnerabilities that cannot be remediated within the policy-recommended timeframes. Hence, RMA confirmed that FY 2022 Recommendations 1 and 2[21] are closed.

RMA's testing found no exceptions, and the controls were operating as intended. We concluded that the EAC's Configuration Management controls in place were effective.

Identity and Access Management

We determined that the EAC's overall maturity level for the Identity and Access Management domain was Managed and Measurable.

The EAC employed for strong authentication mechanisms for privileged and non-privileged users of the EAC's physical and logical assets. The EAC used various automated mechanisms to track all users with their devices on the network. Personal Identity Verification (PIV) management was enabled through group policies, and all users were required to use a PIV card to authenticate to the network. RMA determined that the EAC met the privileged identity and credential management logging requirements at the Maturity Event Logging Level 2 standard, in accordance with OMB's M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident* (August 27, 2021). In addition, RMA observed that the EAC demonstrated progress toward implementing Event Logging Level 3 (EL3) advanced requirements for user behavior monitoring, which enables the detection and alerting of privileged user compromise. Hence, RMA confirmed that FY 2024 Recommendation 4[22] is closed.

[21] *Audit of the U.S. Election Assistance Commission's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2022* (Audit Report No. O22HQ0006-23-02, November 3, 2022), Recommendations 1 and 2.

[22] *Audit of the U.S. Election Assistance Commission's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2024* (Audit Report No. P24HQ0052-24-15, September 24, 2024), Recommendation 4.

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

RMA's testing found no new exceptions, and the controls were operating as intended. We concluded that the EAC's Identity and Access Management controls in place were effective.

Data Protection and Privacy

We determined that the EAC's overall maturity level for the Data Protection and Privacy domain was Consistently Implemented. We identified one new weakness in the Data Protection and Privacy domain, in addition to not remedying the prior year's weakness.

The EAC had data loss prevention policies and retention policies in place. However, the EAC did not prevent or detect untrusted removable media.

NIST SP 800-53 Revision 5.1.1, Security and Privacy Controls for Information Systems and Organizations, MP-7 MEDIA USE, page 176, requires:
Control:

a. [Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls].

Discussion: System media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, flash drives, compact discs, digital versatile discs, and removable hard disk drives. Non-digital media includes paper and microfilm. Media use protections also apply to mobile devices with information storage capabilities. In contrast to [Media Protection] MP-2, which restricts user access to media, MP-7 restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives.

EAC management indicated that staffing challenges within the information technology division led to increased workloads for key personnel. Additionally, competing organizational priorities diverted attention and resources, which contributed to delays in implementing necessary improvements across the applicable FISMA domains.

Not preventing untrusted removable media increases the likelihood of malware infections or data exfiltration through rogue Universal Serial Bus or portable drives. This creates a serious threat vector for ransomware, data breaches, or operational disruption.

RMA recommends the Chief Information Officer:

4. Implement a process to detect and prevent the use of untrusted removable media on the EAC's network.
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.
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.

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

We noted that the EAC completed the data exfiltration exercise in the past 12 months. Hence, RMA confirmed that FY 2024 Recommendation 5 is closed.[23][24]

The EAC had defined and communicated policies and procedures regarding the protection of 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.

RMA's testing found exceptions in the Data Protection and Privacy domain, and the existing controls were not operating as intended. We concluded that the EAC's Data Protection and Privacy controls in place were not effective.

Security Training

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

The EAC had defined its workforce's processes for assessing knowledge, skills, and abilities. Additionally, the EAC addressed the gaps in its identified knowledge, skills, and abilities through targeted training. The EAC's personnel collectively possess a training level such that the EAC demonstrated that security incidents resulting from personnel actions or inactions are reduced over time.

RMA's testing found no exceptions, and the controls were operating as intended. We concluded that the EAC's Security Training controls in place were effective.

Information Security Continuous Monitoring

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

The EAC developed an Information Security Continuous Monitoring Strategy and defined the process of performing ongoing control assessments and monitoring organization-defined metrics. Since the EAC developed the strategy in FY 2025, it has not established a monitoring mechanism to track the progress of ongoing lessons learned. A recommendation addressing this finding was

[23] Ibid, Recommendation 5.
[24] EAC is in the process of completing their annual exfiltration exercise for FY 2025. Hence, RMA is not issuing any new recommendation.

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

issued in the FY 2024 FISMA audit report.[25] Because that recommendation remains open, we are not making a new recommendation.

The EAC prepared Authorization to Operate packages for its systems and maintained system-level continuous monitoring, including performing security control assessments and updating security plans. The EAC's authorization processes include automated analysis tools and manual expert analysis, as appropriate. The EAC monitored and measured the integrity and security posture of all owned and associated assets.

RMA's testing found an exception in the Information Security Continuous Monitoring domain, and the existing controls were not operating as intended. We concluded that the EAC's Information Security Continuous Monitoring controls in place were not effective.

Incident Response

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

The EAC's Incident Response policy addressed incident handling. In addition, the EAC defined the policies and procedures that the EAC personnel must adhere to when an incident is detected. EAC used an automated mechanism to detect and track events with taxonomy, while also monitoring and analyzing qualitative and quantitative performance measures to assess the effectiveness of its incident detection and analysis policies and procedures. The EAC also implemented processes to remediate vulnerabilities that may have been exploited on the target system(s) and recover system operations.

RMA's testing found no exceptions, and the controls were operating as intended. We concluded that the EAC's Incident Response controls in place were effective.

Contingency Planning

We determined that the EAC's overall maturity level for the Contingency Planning domain was Managed and Measurable. We identified one new weakness in the Contingency Planning domain, in addition to not addressing the prior year's weaknesses.

The EAC did not conduct the annual information system contingency plan testing and exercise.

NIST SP 800-53 Revision 5.1.1, Security and Privacy Controls for Information Systems and Organizations, CP-4 CONTINGENCY PLAN TESTING, page 119, requires:
Control:

a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests].

[25] Ibid, Recommendation 6.

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

b. Review the contingency plan test results; and
c. Initiate corrective actions, if needed.

Discussion: Methods for testing contingency plans to determine the effectiveness of the plans and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

EAC management indicated that staffing challenges within the information technology division led to increased workloads for key personnel. Additionally, competing organizational priorities diverted attention and resources, which contributed to delays in implementing necessary improvements across the applicable FISMA domains.

Without testing the contingency plan, the EAC could not verify the effectiveness of its disaster recovery or business continuity plans. In a real emergency, this may result in prolonged downtime, data loss, or ineffective response due to unproven procedures.

RMA recommends the Chief Information Officer:

7. Schedule and complete annual contingency planning tests. Retain supporting documentation to demonstrate compliance during audits.

We also noted that the EAC had not employed automated mechanisms to test system contingency plans more thoroughly and effectively. A recommendation addressing this finding was issued in the FY 2024 FISMA audit report.[26] Because that recommendation remains open, we are not making a new recommendation.

The EAC's contingency plan adhered to the guidelines established in NIST SP 800-53 Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*, ensuring that all necessary measures were in place to recover and sustain critical information technology services in the event of a significant business interruption. The EAC had consistently incorporated the results from its Business Impact Analysis into strategy and plan development efforts. The EAC's Enterprise Risk Management Strategy outlines the strategic objectives, contributing projects and programs, and risk scenarios associated with each strategic goal.

Even with prior year open recommendations and finding exceptions, the controls were operating as intended. We concluded that the EAC's Contingency Planning controls in place were effective.

[26] Ibid, Recommendation 7.

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

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 practices were effective for FY 2025 though the overall maturity level of the EAC's information security program was Consistently Implemented. Although our assessment of the EAC's information security program identified exceptions 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 by the EAC for each of the core metrics and supplemental metrics outlined in the *FY 2025 IG FISMA Reporting Metrics v2.0*, dated April 3, 2025. 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 ten FISMA Metric Domains:

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

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 for the EAC, and the review covered FY 2025 as of August 1, 2025. We assessed all 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 9, 2025, and August 1, 2025. 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 the following: (1) NIST SP 800-53, Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*; (2) NIST SP 800-53A, Revision 5.1.1, *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.

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

We conducted interviews with the EAC officials and reviewed the legal and regulatory requirements stipulated in FISMA. We also examined documents supporting the information security program and practices. Where appropriate, we compared documents, such as the EAC's information technology policies and procedures, to requirements stipulated in NIST Special Publications. Additionally, we conducted tests of system processes to assess the design and operating effectiveness of these controls.

We applied the following criteria for performing the EAC's FY 2025 FISMA audit.

NIST Federal Information Processing Standards (FIPS) and SPs

- *NIST Cybersecurity Framework (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 800-53, Revision 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-53A, Revision 5.1.1, *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 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-83, Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- 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 800-128, *Guide for Security-Focused Configuration Management of Information Systems*

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

- 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-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*
- 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 Memorandum M-17-09, *Management of Federal High Value Assets*
- OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CISP) for the Federal Civilian Government*
- 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*

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

GAO

- Standards for Internal Control in the Federal Government, September 2014

Cybersecurity and Infrastructure Security Agency

- Binding Operational Directive (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 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy*
- BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*
- 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) 24-02, *Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System*
- ED 24-01 *Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*
- ED 22-03 *Mitigate VMware Vulnerabilities*
- ED 21-04, *Mitigate Windows Print Spooler Service Vulnerability*
- ED 21-03, *Mitigate Pulse Connect Secure Product Vulnerabilities*
- ED 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*
- ED 21-01, *Mitigate SolarWinds Orion Code Compromise*
- ED 20-04, *Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday*
- ED 20-03, *Mitigate Windows DNS Server Remote Code Execution Vulnerability from July 2020 Patch Tuesday*
- ED 20-02, *Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday*
- ED 19-01, *Mitigate DNS Infrastructure Tampering*

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	EAC Position on Status	Auditor's Position on Status
(FY 2024 Audit Report P24HQ0052-24-15) 1	We recommend that the Chief Information Security Officer identify qualitative and quantitative metrics on service level agreements held with third parties, then perform an analysis with monthly reporting received from those third parties to identify metrics that can be measured and documented, on either a monthly or quarterly basis, to ensure that EAC is receiving all contracted services.	**Closed**	**Agree** **See Cybersecurity Supply Chain Risk Management section.**
(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.	**Open**	**Agree** **See Cybersecurity Supply Chain Risk Management section.**
(FY 2024 Audit Report P24HQ0052-24-15) 3	We recommend that the Chief Information Security Officer provides annual Anti-Counterfeit Training for IT staff with SCRM responsibilities.	**Closed**	**Agree** **See Cybersecurity Supply Chain Risk Management section.**
(FY 2024 Audit Report P24HQ0052-24-15) 4	We recommend that the Election Assistance Commission's Chief Information Officer implement EL3 logging requirements in accordance with the Office of Management and Budget memorandum M-21-31.	**Closed**	**Agree** **See Identity and Access Management section.**
(FY 2024 Audit Report P24HQ0052-24-15) 5	We recommend that the Election Assistance Commission's Chief Information Officer perform the breach tabletop exercises annually, which includes a data-exfiltration exercise.	**Closed**	**Agree** **See Data Protection and Privacy 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**	**Agree** **See Information Security Continuous Monitoring section.**

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

Audit Report and Recommendation No.	Audit Recommendations	EAC Position on Status	Auditor's Position on Status
(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**	**Agree** **See Contingency Planning section.**
(FY 2023 Audit Report O23HQ0029-23-07) 4	We recommend the EAC Office of Chief Information Officer (OCIO) update its POA&M procedures and, in coordination with management, develop and maintain POA&M reports based on Federal requirements.	**Closed**	**Agree** **See Risk and Asset Management section.**
(FY 2022 Audit Report O22HQ0006-23-02) 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.	**Closed**	**Agree** **See Configuration Management section**.
(FY 2022 Audit Report O22HQ0006-23-02) 2	We recommend EAC OCIO develop and implement a flaw remediation plan for vulnerabilities that cannot be remediated within the policy recommended timeframes.	**Closed**	**Agree** **See Configuration Management section**.

Appendix II: Management Response

TO: U.S. Election Assistance Commission, Acting Inspector General, Sarah Dreyer
FROM: U.S. Election Assistance Commission, CIO/CISO, Jessica Bowers
DATE: August 28, 2025
SUBJECT: Response to Draft FISMA Audit Report FY2025

The Office of the Chief Information Officer (OCIO) provides the following responses to the Inspector General's FY2025 FISMA audit findings and recommendations.

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

   Management Response: Agree

   The EAC has developed a skills analysis matrix to identify skills gaps with OCIO personnel with any existing or planned technologies. Additionally, OCIO has identified opportunities for cross training of personnel to develop additional depth and mitigate the risk of future gaps due to attrition. For areas where gaps may persist, the EAC utilizes expert contractor support and has agreements in place to cover all relevant areas.

   Estimated completion date: October 2025

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.**

   Management Response: Agree

   The EAC will incorporate automated alerting into its monitoring systems to ensure that policies and procedures are reviewed and updated in accordance with its timeliness requirements.

   Estimated completion date: November 2025

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.**

Management Response: Agree

The EAC's current governance, risk, and compliance tool is being deprecated by its vendor at the end of calendar year 2025. The EAC has begun the process of creating internal tools to replace this functionality and plans to integrate continuous monitoring of cybersecurity risk into enterprise risk management as part of this effort.

Estimated completion date: February 2026

4. **Implement a process to detect and prevent the use of untrusted removable media.**

   Management Response: Agree

   The EAC performs monitoring the use of removable media devices with alerting for suspicious activity and active blocking for the copying of PII or running of executable programs. The EAC believes these robust protections mitigate the risks inherent to untrusted removable media but will investigate the purchase of trusted removable media devices for all personnel, pending the availability of funding. If the purchase is not feasible, the EAC will describe the risk acceptance in its documentation along with the compensating controls enacted to protect EAC information and resources.

   Completion date: December 2025

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.**

   Management Response: Agree

   As mentioned in response #4 above, the EAC will document its acceptance of risk in its documentation along with compensating controls enacted to protect EAC information and resources.

   Estimated completion date: December 2025

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.**

   Management Response: Agree

   The EAC implements robust endpoint detection and response tools that automatically identify and remove vulnerabilities introduced by the use of untrusted removable media. This includes blocking the reading or writing of PII or running of any executable programs from the removable media. The EAC will ensure that these compensating controls are fully documented in all relevant policies and procedures.

Estimated completion date: December 2025

7. **Schedule and complete annual contingency planning tests. Retain supporting documentation to demonstrate compliance during audits.**

   Management Response: Agree

   The EAC conducts annual contingency planning exercises; however, these have been scheduled out of alignment with annual FISMA audit activities, typically occurring in the later months of the fiscal year. The EAC has rescheduled its annual exercises to better align with the audit schedule to improve visibility into its exercise findings.

   Estimated completion date: February 2026

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 findings and all seven of our recommendations. After reviewing the EAC's response, we consider them to be responsive to our recommendations and the actions taken and planned should resolve the issues identified in the report. Therefore, the seven recommendations 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
DNS	Domain Name System
C-SCRM	Cybersecurity Supply Chain Risk Management
ED	Emergency Directive
EL	Event Logging
EAC	Election Assistance Commission
ERM	Enterprise Risk Management
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
HAVA	Help America Vote Act of 2002
IG	Inspector General
IT	Information Technology
MP	Media Protection
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OCIO	Office of Chief Information Officer
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
RMA	RMA Associates, LLC
SCRM	Supply Chain Risk Management
SP	Special Publication
ZTA	Zero Trust Architecture

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