United States Election Assistance Commission Office of Inspector General

Fiscal Year 2020 EAC Compliance with the Federal Information Security Modernization Act

Report No. I-PA-EAC-02-20

OFFICE OF THE INSPECTOR GENERAL
US ELECTION ASSISTANCE COMMISSION
633 3RD STREET, NW, SUITE 200
WASHINGTON, DC 20001

Memorandum

Date: December 15, 2020

To: Benjamin W. Hovland, Chairman
U.S. Election Assistance Commission

From: *Patricia Layfield*
Inspector General

Subject: Final Report – Fiscal Year 2020 U.S. Election Assistance Commission Compliance with the Requirements of the Federal Information Security Modernization Act (Assignment No. I-PA-EAC-02-20)

The Office of Inspector General (OIG) engaged Brown & Company, CPAs (Brown), an independent certified public accounting firm, to conduct an audit of the U.S. Election Assistance Commission's (EAC's) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) and related information security policies, procedures, standards, and guidelines. The audit included assessing the EAC's effort to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the EAC.

Results of Audit

The audit concluded that EAC generally complied with FISMA requirements by implementing security controls, based on Brown's testing of selected controls on the EAC systems Brown tested. Those tests were designed to obtain sufficient, appropriate evidence to provide a reasonable basis for Brown's findings and conclusions, based on their audit objectives.

Although EAC generally had policies for its information security program, its implementation of those policies for selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, the audit identified areas in EAC's information security program that need to be improved.

Brown & Co. made five recommendations to assist EAC in strengthening its information security program:

- Issue an Authorization to Operate (ATO) for its Microsoft Azure implementation.
- Ensure the Data Owners sign user access recertifications.
- Implement web and email security enhancements required by Binding Operational Directive 18-01.
- Maintain an accurate inventory of hardware assets for its operating environment.
- Consistently monitor controls to ensure its objectives outlined in its ISCM strategy is consistently implemented.

EAC management generally agreed with the findings and recommendations. OIT has developed planned corrective actions to implement the recommended controls.

In accordance with *Government Auditing Standards*, Brown also followed up on the status of the recommendations contained in prior FISMA audit reports. They found that EAC had completed corrective actions on all but five of those recommendations (see Appendix II, page 12). The 2018-2019 recommendations that remain uncorrected are:

- Remediate configuration related vulnerabilities in the network identified, and document the results or document acceptance of the risks of those vulnerabilities. (2018)
- Review and approve the Agency's information security policies and procedures on an annual basis. (2018)
- Implement a remediation plan and commit resources to update all EAC-wide information security policies and procedures on the frequency required by NIST SP 800-53, Rev. 4. (2018)
- Develop an annual specialized training schedule that identifies individuals who need training. (2019)
- Track the training schedule to ensure individuals receive assigned training according to the agency's policy. (2019)

EVALUATION OF BROWN'S AUDIT PERFORMANCE

To fulfill our responsibilities under *Government Auditing Standards* and other related requirements, the OIG:

- Reviewed Brown's approach and planning of the audit;
- Evaluated the qualifications and independence of the auditors;
- Monitored the progress of the audit at key points;
- Coordinated or participated in periodic meetings with Brown and EAC management to discuss progress, findings, and recommendations;
- Reviewed Brown's draft audit report;
- Performed other procedures we deemed necessary; and

- Coordinated issuance of the audit report.

Brown is responsible for the attached auditor's report and the findings and conclusions expressed in the report. The work the EAC OIG performed in evaluating Brown's conduct of the audit was not sufficient to support an opinion on the effectiveness of internal control or compliance with laws and regulations, thus EAC OIG does not express any opinion on EAC's internal controls or compliance.

REPORT DISTRIBUTION

The Inspector General Act of 1978, as amended, requires semiannual reporting to Congress on all reports issued, actions taken to implement recommendations, and recommendations that have not been implemented. Therefore, we will report the issuance of this audit report in our next semiannual report to Congress. The distribution of this report is not restricted and copies are available for public inspection. Pursuant to the IG Empowerment Act of 2016, the EAC OIG will post this audit report on the OIG website within 3 days of its issuance to EAC management. The OIG will also post the report to Oversight.gov.

If you have any questions regarding this report, please call me at (202) 853-2760.

cc: Commissioner Donald L. Palmer, Vice-Chair
Commissioner Thomas Hicks
Commissioner Christy McCormick
Mona Harrington, Executive Director

Attachment

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

Fiscal Year 2020
December 14, 2020

Prepared by

**Brown & Company Certified Public Accountants
and Management Consultants, PLLC
6401 Golden Triangle Drive, Suite 310
Greenbelt, Maryland 20770**

BROWN & COMPANY

CERTIFIED PUBLIC ACCOUNTANTS AND MANAGEMENT CONSULTANTS, PLLC

Ms. Patricia L. Layfield
U.S. Election Assistance Commission
Office of the Inspector General
1335 East-West Highway, Suite 4300
Silver Spring, MD 20901

Dear Ms. Layfield:

Enclosed is the audit report on the United States Election Assistance Commission's (EAC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). The EAC Office of the Inspector General (OIG) contracted with the independent certified public accounting firm of Brown & Company CPAs and Management Consultants, PLLC (Brown & Company), to conduct the audit in support of the FISMA requirement for an annual evaluation of EAC Office of Information Technology (OIT) information security program.

The objective of this performance audit was to determine whether EAC OIT implemented selected security controls for certain information systems in support of FISMA. The audit included the testing of selected management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

For this audit, we reviewed selected controls from EAC's General Support System. The audit also included a review of vulnerability assessments on internal systems and an evaluation of the EAC OIT process to identify and mitigate information systems vulnerabilities. Audit fieldwork was performed at EAC's headquarters in Silver Spring, MD from May 12, 2020 through September 30, 2020.

Our audit was performed in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit concluded that EAC OIT generally complied with FISMA requirements by implementing selected security controls for tested systems. Although EAC OIT generally had policies for its information security program, its implementation of those policies for selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction.

Consequently, the audit identified areas in EAC OIT information security program that needed to be improved. We are making five recommendations to assist EAC OIT in strengthening its information security program. In addition, findings related to recommendations from prior years were not yet fully implemented.

This report is for the purpose of concluding on the audit objective described above. Accordingly, this report is not suitable for any other purpose.

We appreciate the assistance we received from the staff of EAC and the opportunity to serve you. We will be pleased to discuss any questions you may have.

Brown & Company

December 14, 2020
Greenbelt, Maryland

Table of Contents

Summary of Results

The Federal Information Security Modernization Act of 2014[1] (FISMA), requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems[2], including those provided or managed by another agency, contractor, or other sources. Because the United States Election Assistance Commission (EAC) is a federal agency, it is required to comply with federal information security requirements.

FISMA also requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capabilities are established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the U.S. Office of Management and Budget (OMB) and to congressional committees on their information security program's effectiveness. FISMA has also established that the standards and guidelines issued by the National Institute of Standards and Technology (NIST) are mandatory for federal agencies.

The EAC's OIG engaged Brown & Company CPAs and Management Consultants, PLLC (Brown & Company) to conduct an audit in support of the FISMA requirement for an annual evaluation of EAC OIT information security program. This performance audit's objective was to determine whether EAC OIT implemented certain security controls for selected information systems in support of FISMA.

Our audit was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

For this audit, we reviewed selected controls from EAC's General Support System.

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283— December 18, 2014) amends the Federal Information Security Management Act of 2002.
[2] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Results

Although, EAC OIT generally has policies for its information security program, its implementation of those policies for security controls reviewed was not fully effective to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, the audit identified areas in the EAC OIT information security program that needed to be improved. Specifically, EAC OIT needs to:

1. Issue an Authorization to Operate (ATO) for its Microsoft Azure implementation.
2. Ensure the Data Owners sign user access recertifications.
3. Implement web and email security enhancements required by Binding Operational Directive 18-01.
4. Maintain an accurate inventory of hardware assets for its operating environment
5. Consistently monitor controls to ensure its objectives outlined in its ISCM strategy is consistently implemented.

This report makes five recommendations to assist EAC OIT in strengthening its information security program. In addition, as illustrated in Appendix II, findings related to five prior years' recommendations had not yet been fully implemented, and therefore, new recommendations were not made. Detailed findings appear in the following section.

Audit Findings

1. EAC OIT did not issue an ATO for its Microsoft Azure prior to deployment into production.

NIST SP 800-53, Revision 4 (Rev. 4), defines "Authorization to Operates" (ATO) as

> The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

NIST Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy*, Revision 2, 3.6 "Authorize" states:

> Authorization packages include security and privacy plans, security and privacy assessment report, plans of action and milestones, and an executive summary.

EAC OIT has implemented policies and procedures for security assessment and authorization to facilitate the implementation of information systems along with security controls in its network environment. EAC OIT did not conduct a security assessment and authorization for some of the information systems in our sample. Specifically, the Microsoft Azure system was in operation without an ATO.

Competing priorities of other activities within the OIT department have caused the delay in conducting a security assessment and authorization for its Microsoft Azure system.

The delay of conducting security assessment and authorization minimizes the agency's effectiveness to monitor risk associated with the implementation.

Recommendation 1: We recommend EAC OIT prepare an authorization package for its Microsoft Azure system that includes a security and privacy plan, security and privacy assessment report, plans of action and milestones, and an executive summary.

Management's Response:

EAC Response: Agree. EAC OIT has prepared an authorization package and submitted the ATO letter.

Auditor's Evaluation of Management's Response:

EAC's management concurred with the recommendation. EAC issued the Microsoft Azure Commercial IaaS ATO letter dated August 3, 2020.

Management's full response is provided in Appendix IV.

2. EAC OIT needs to ensure the Data Owners sign user access recertifications.

NIST SP 800-53, Revision 4 (Rev. 4), *Security and Privacy Controls for Federal Information Systems and Organizations,* Control AC-5, “Separation of Duties” addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Failure to implement adequate separation of duties increases the risk that malicious activity by system users remains undetected.

EAC OIT has implemented policies and procedures for the separation of duties to facilitate the implementation of information systems along with security controls in its network environment. Specifically, *EAC-CIO-2010-004 Access Control Procedural Guide* states:

> System Owners and Data Owners are responsible for the accuracy and currency of the account credentials and authorizations for each user who is granted access. The documentation should clearly indicate what rights have been granted, when the accounts and the authorizations were last reviewed, and who granted and reviewed them. System Owners and Data Owners must at least annually review and validate accounts and authorizations to ensure the continued need for access.

We examined twenty-two (22) user access recertifications and noted all submissions, excepted one, were signed by the System Owner, Acting Chief Information Officer (CIO). However, the submissions did not include signatures of Data Owners.

This control weakness occurred because OIT did not enforce its policy requiring Data Owners to review and validate user access accounts.

Separation of duties reduces the risk of potential abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion.

Recommendation 2: We recommend EAC OIT ensure Data Owners sign user access recertifications.

Management’s Response:

EAC Response: Agree. EAC OIT shall ensure that Data Owner access recertifications contain both signatures and dates signed. The form has been updated and EAC OIT is obtaining new certification signatures with dates.

Auditor’s Evaluation of Management’s Response:

EAC’s management concurred with the recommendation.

Management’s full response is provided in Appendix IV.

3. EAC OIT has not implemented web and email security enhancements required by Binding Operational Directive 18-01.

Department of Homeland Security (DHS)'s *Binding Operational Directive 18-01* "Enhance Email and Web Security," October 16, 2017, requires federal agency to implement email authentication technologies to detect and mitigate fraudulent email and requires that all publicly accessible Federal websites and web services only provide service through a secure connection.

Email Security:

We reviewed the DHS Cybersecurity and Infrastructure Security Agency (CISA) *Trustworthy Email Report,* May 16, 2020*,* and noted that EAC had not implemented email security controls required by Binding Operational Directive 18-01. Specifically, EAC OIT has not implemented Domain-based Message Authentication, Reporting and Conformance (DMARC) policy for email authentication technologies to detect and mitigate fraudulent emails.

The DMARC policy of "reject" provides the strongest protection against spoofed email, ensuring that unauthenticated messages are rejected at the mail server, even before delivery.

Web Security:

We reviewed the *DHS CISA HTTPS Report,* May 16, 2020*,* and noted that EAC had not implemented email security controls required by *Binding Operational Directive 18-01*. Specifically, EAC OIT has not implemented HTTP Strict Transport Security (HSTS) for one of its public-facing websites. EAC OIT has not implemented HSTS for its Vote by Mail website (votebymail.gov). HSTS ensures browsers always use an https:// connection, and removes the ability for users to click through certificate-related warnings.

HSTS reduces insecure redirects, and protects users against attacks that attempt to downgrade connections to plain HTTP.

These conditions occurred because EAC OIT lacks monitoring controls for remediating security weaknesses identified in the DHS CISA Trustworthy *Email Report and HTTPS Report.*

Recommendation 3: We recommend EAC OIT implement DMARC policy and HSTS security controls required by DHS *Binding Operational Directive 18-01*.

Management's Response:

EAC Response: Agree. The votebymail.gov website is used as a redirect to the primary EAC website, eac.gov. The eac.gov website enforces HTTPS and utilizes HSTS in accordance with BOD 18-01. EAC OIT recognizes the need to add this capability even to redirect domains and is working with its web hosting provider to add HSTS headers to our redirect domains and add them to the Chrome preload list, as specified in the BOD.

Auditor's Evaluation of Management's Response

EAC's management concurred with the recommendation.

Management's full response is provided in Appendix IV.

4. EAC OIT did not maintain an accurate inventory of hardware assets for its operating environment.

OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, requires agencies to ensure that physical devices, software applications, hardware platforms, and systems within the organization are inventoried when obtained and that inventories are updated on an ongoing basis.

NIST SP 800-53 Rev. 4, CM-8 "Information System Component Inventory", requires organizations to develop and document an inventory of information system components that accurately reflects current information systems, includes all components within the systems' authorization boundaries, and allows for tracking and reporting.

EAC OIT uses several methods for maintaining inventory of information systems and software. GFI Langobard is used to discover and identify IT devices on EAC's network; thereby creating an asset inventory of every device on EAC's network. The WASP inventory application is used to tag and track the physical location of IT equipment, identify asset type, logging serial numbers, and document other data. EAC's procedures require EAC OIT to conduct physical inventory annually that requires system users to submit inventory verification forms listing assets in their possession.

The auditors traced a sample of eleven (11) 2020 Inventory Verification forms from a population of forty-one (41) forms to the IT 2020 system inventory report. The sample selection consisted of forty-one (41) assets. Of the forty-one assets tested, we noted ten (10) incidents were assets reported on the forms did not agree with the inventory report. Therefore, EAC OIT did not reconcile physical inventory to its inventory system report to accurately reflect the agency's operating environment.

Also, EAC OIT did not update hardware asset inventory records upon employees' separation from the agency. Specifically, records showed that one employee who separated from the agency still had a mobile device "in-use"; however, the device was assigned to another employee.

This condition occurred because EAC OIT lacks monitoring controls for maintaining inventory for hardware assets. Without accurate and complete inventories of the hardware assets connected to the agency's network, the agency may not be able to identify and properly mitigate hardware issues. In addition, the agency may not ensure proper accountability over agency assets and risk paying for unused or underutilized IT equipment or hardware.

Recommendation 4*:* We recommend EAC OIT reconcile its physical inventory to its inventory system report and update inventory records for separated employees to reflect the EAC operating environment accurately.

Management's Response:

EAC Response: Agree. Due to COVID-19 mandated remote work, inventory work conducted this year was also done remotely via user-reported manual inventory. The EAC shall implement controls to better reflect actual inventory and reconcile user-reported inventory against the agency's master inventory list. EAC OIT has rectified the discrepancies noted by the auditors.

Auditor's Evaluation of Management's Response:

EAC's management concurred with the recommendation.

Management's full response is provided in Appendix IV.

5. EAC OIT does not consistently monitor controls to ensure its objectives outlined in its ISCM strategy is consistently implemented.

NIST SP 137 *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* September 2011, defines ISCM as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. ISCM, a critical step in an organization's Risk Management Framework (RMF), gives organizational officials access to security-related information on demand, enabling timely risk management decisions, including authorization decisions.

In addition, OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*, November 2013, states that agencies are required to implement continuous monitoring of security controls.

EAC OIT has developed an ISCM strategy that addresses the monitoring of security controls at the agency, business unit, and information system level. At the information system level, the ISCM strategy establishes processes for monitoring security controls for effectiveness and reporting any findings. However, in practice, EAC OIT is not monitoring controls to ensure its objectives outlined in its ISCM strategy is consistently implemented. Specifically, we noted that EAC OIT did not:

- Conduct weekly and quarterly vulnerability scans for information systems and hosted applications;
- Remediate high-risk vulnerabilities within 30 days and moderate-risk vulnerabilities within 90 days of discovery.
- Update policy and procedure documents for *Audit and Accountability Policy, Procurement Handbook, Security Incident Hand Book, Media Sanitation and Privacy Handbook* policy to reflect the agency's current operating environment to include MS Azure.

These control weaknesses occurred, in part, because the ISCM process did not include a process to measure the effectiveness or efficiency of monitoring activities stated in the agency's policy.

Continuous monitoring of threats, vulnerabilities, and security control effectiveness provides situational awareness for risk-based support of ongoing authorization decisions. ISCM performance metrics are used to assess, respond, and monitor risk across the organization. The focus of ISCM metrics is to provide adequate information about security control effectiveness, and organizational security status t0 allow officials to make informed, timely security risk management decisions.

Recommendation 5: We recommend EAC OIT prepare performance metrics that measure the effectiveness or efficiency of its information security program and security controls the EAC employs in support of its programs.

Management's Response:

EAC Response: Agree. The EAC has increased the breadth of its automated monitoring systems to cover all network endpoints. Additionally, the EAC has recently implemented an enterprise risk management solution tailored to its cloud environment to monitor and report compliance with all relevant security controls. All EAC OIT documentation has been updated to reflect the EAC's move the MS Azure cloud environment.

Auditor's Evaluation of Management's Response:

EAC's management concurred with the recommendation.

Management's full response is provided in Appendix IV.

Appendix I – Scope, Methodology and Criteria

Scope

We conducted this audit in accordance with generally accepted government auditing standards, as specified in the Government Accountability Office's *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was designed to determine whether EAC OIT implemented selected security controls for certain information systems in support of the FISMA Act of 2014.

Our overall objective was to evaluate EAC OIT security program and practices, as required by FISMA. Specifically, we reviewed the status of the following areas of EAC OIT security program in accordance with DHS FISMA Inspector General reporting requirements:

- Risk Management;
- Configuration Management;
- Identity, Credential, and Access Management;
- Data Protection and Privacy;
- Security Training;
- Information Security Continuous Monitoring;
- Incident Response; and
- Contingency Planning.

In addition, we evaluated the status of EAC's IT security governance structure and the Agency's system security assessment and authorization (SA&A) methodology. We also followed up on outstanding recommendations from prior FISMA audits (see Appendix II) and performed audit procedures on EAC's internal and on external systems. The audit also included a review of vulnerability assessments of EAC-managed internal system and an evaluation of EAC OIT process for identifying and mitigating technical vulnerabilities.

Methodology

We reviewed EAC's general FISMA compliance efforts in the specific areas defined in DHS's guidance[3] and the corresponding reporting instructions. We also audited an internal system and EAC's SA&A process. We considered the internal control structure for EAC's systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls over EAC's internal system and contractor-owned and managed systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. Our understanding of these systems' internal controls was used to evaluate the degree to which the appropriate internal controls were

[3] OMB M-20-04 Fiscal Year 2019-2020 *Guidance on Federal Information Security and Privacy Management Requirements,* November 19, 2019.

designed and implemented. When appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

We assess internal controls, deemed significant to our audit, which include the following:

- Risk Assessment:
    - Define Objectives and Risk Tolerances
    - Identify, Analyze, and Respond to Risks
    - Identify, Analyze, and Respond to Change

- Control Activities:
    - Design Control Activities
    - Implement Control Activities

- Information and Communication:
    - Communicate Internally
    - Communicate Externally

- Monitoring:
    - Perform Monitoring Activities
    - Evaluate Issues and Remediate Deficiencies.

To accomplish our audit objective, we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA;
- Reviewed documentation related to EAC OIT information security program, such as security policies and procedures, system security plans, and risk assessments;
- Tested system processes to determine the adequacy and effectiveness of selected controls;
- Reviewed the status of recommendations in the fiscal years 2017, 2018, and 2019 FISMA audit reports; and
- Reviewed the network vulnerability assessment of the EAC OIT internal system.

Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the set of internal controls for EAC's systems taken as a whole.

Criteria

The criteria used in conducting this audit included:

- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*;
- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*;
- NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*;
- NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*;
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program;*
- NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations;*
- NIST SP 800-61*, Rev. 1, Computer Security Incident Handling Guide;*
- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information;*
- NIST SP 800-128*, Guide for Security-Focused Configuration Management of Information Systems;*
- NIST SP 800-137*, Information Security for Continuous Monitoring for Federal Information Systems and Organizations;*
- *NIST Framework for Improving Critical Infrastructure Cybersecurity, V 1.1;*
- *Chief Financial Officers Council and the Performance Improvement Council release the Playbook: Enterprise Risk Management (ERM);*
- *Federal Acquisition Regulation (FAR); FAR Case 2007-004, Common Security Configurations;*
- *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control;*
- *OMB Circular A-130, Managing Information as a Strategic Resource, July 28, 2016*
- *OMB Memorandum M-08-05, Implementation of Trusted Internet Connections;*
- *OMB Memorandum M-08-22, Guidance on the Federal Desktop Core Configuration (FDCC);*
- *OMB Memorandum M-18-02, Guidance on Federal Information Security and Privacy Management Requirements; and*
- *SECURE Technology Act, Federal Acquisition Supply Chain Security;*
- *US-CERT Incident Notification Guidelines.*

The audit was conducted at EAC's headquarters in Silver Spring, MD, from May 8, 2020 through September 30, 2020.

Appendix II – Status of Prior Years Findings

The following table provides the status of the Fiscal Year (FY) 2017, 2018 and 2019 audit recommendations.

No.	FY 2017[4], 2018[5] and 2019[6] Audit Recommendations	Status	Auditor's Position on Status
1.	**FY 2017 FISMA audit recommendation No. 9:** The EAC Chief Information Officer (CIO) should review and update the Continuity of Operation Plan (COOP) at least annually, and EAC management should review the business impact analysis supporting the COOP for accuracy semi-annually in alignment with the existing IT inventory checks.	Closed	Agree
2.	**FY 2018 FISMA audit recommendation No. 1:** EAC Chief Information Officer to develop and implement an Enterprise Risk Management Strategy that will include a risk profile, risk management committee, risk appetite/tolerance levels, risk register, responding to risk, monitoring risk and utilizing an automated solution to view risks across the organization.	Closed	Agree
3.	**FY 2018 FISMA audit recommendation No. 3:** EAC OIT to remediate configuration-related vulnerabilities in the network identified, and document the results or document acceptance of the risks of those vulnerabilities.	Open	Agree
4.	**FY 2018 FISMA audit recommendation No. 6:** EAC to review and approve Agency's information security policies and procedures on an annual basis.	Open	Agree

[4] The *Election Assistance Commission Implemented Controls in Support of FISMA For Fiscal Year 2017, But Improvements Are Needed* (EAC IG Report No. I-PA-EAC-02-17, November, 2017).

[5] The *Election Assistance Commission's Compliance with the Federal Information Security Modernization Act of 2014 (*EAC IG Report No. I-PA-EAC-02-18, November, 2018).

[6] The *Election Assistance Commission's Compliance with the Federal Information Security Modernization Act of 2014 (*EAC IG Report No. I-PA-EAC-02-19, December 9, 2019).

No.	FY 2017[4], 2018[5] and 2019[6] Audit Recommendations	Status	Auditor's Position on Status
5.	**FY 2018 FISMA audit recommendation No. 7:** EAC to implement a remediation plan to commit resources to update all EAC-wide information security policies and procedures on the frequency required by NIST SP 800-53, Rev. 4.	Open	Agree
6.	**FY 2019 FISMA audit recommendation No. 1:** We recommend EAC OIT conduct physical inventory annually to the level of information deemed necessary for effective accountability of inventory specifications that include physical location, component owners, manufacturer, device type, model, and serial number.	Closed	Agree
7.	**FY 2019 FISMA audit recommendation No. 2:** We recommend the EAC OIT prioritize and implement the use of multifactor authentication for network access for privileged accounts.	Closed	Agree
8.	**FY 2019 FISMA audit recommendation No. 3:** We recommend EAC OIT implement a SCAP tool to help maintain an up-to-date, complete, accurate and readily available view of configuration settings for all information components connected to the agency's network.	Closed	Agree
9.	**FY 2019 FISMA audit recommendation No. 4:** We recommend EAC OIT develop an annual specialized training schedule that identifies individuals who need training. The training program should include training objectives, specific appropriate training to ensure IT staff gains specific knowledge, skills, and abilities required to perform tasks in their work role.	Open	Agree
10.	**FY 2019 FISMA audit recommendation No. 5:** We recommend EAC OIT track the training schedule to ensure individuals receive assigned training according to the agency's policy.	Open	Agree

Appendix III - Acronyms

Acronyms	
ATO	Authorization to Operate
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CM	Configuration Management
COOP	Continuity of Operation Plan
DHS	U.S. Department of Homeland Security
DMARC	Domain-based Message Authentication, Reporting and Conformance
EAC	Election Assistance Commission
ERM	Enterprise Risk Management
FAR	Federal Acquisition Regulation
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
HTTP	Hypertext Transfer Protocol
HSTS	Strict Transport Security
IG	Inspector General
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OIT	Office of Information Technology
OMB	U.S. Office of Management and Budget
REV	Revision
SA&A	Security Assessment and Authorization
SCAP	Security Content Automation Protocol
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team

Appendix IV – Management's Comments

U.S. ELECTION ASSISTANCE COMMISSION

633 3rd St. NW, Suite 200
Washington, DC 20001

TO: Inspector General (EAC) Patricia Layfield

FROM: Jessica Bowers, Acting CIO

DATE: December 2, 2020

SUBJECT: Response to Draft Audit Report FY 2020

EAC OIT did not issue an ATO for its Microsoft Azure prior to deployment into production.

EAC OIT has implemented policies and procedures for security assessment and authorization to facilitate the implementation of information systems along with security controls in its network environment. EAC OIT did not conduct a security assessment and authorization for some of the information systems in our sample. Specifically, the Microsoft Azure system was in operation without an ATO.

Competing priorities of other activities within the OIT department have caused the delay in conducting a security assessment and authorization for its Microsoft Azure system.

The delay of conducting security assessment and authorization minimizes the agency's effectiveness to monitor risk associated with the implementation.

EAC Response: Agree

EAC OIT has prepared an authorization package and submitted the ATO letter as part of our PBCs via max.gov as of September 22, 2020.

2. Finding: EAC OIT needs to ensure the Data Owners sign user access recertifications.

EAC OIT has implemented policies and procedures for the separation of duties to facilitate the implementation of information systems along with security controls in its network environment. Specifically, EAC-CIO-2010-004 Access Control Procedural Guide states:

> System Owners and Data Owners are responsible for the accuracy and currency of the

account credentials and authorizations for each user who is granted access. The documentation should clearly indicate what rights have been granted, when the accounts and the authorizations were last reviewed, and who granted and reviewed them. System Owners and Data Owners must at least annually review and validate accounts and authorizations to ensure the continued need for access.

We examined twenty-two (22) user access recertifications and noted all submissions, excepted one, were signed by the System Owner, Acting Chief Information Officer (CIO). However, the submissions did not include signatures of Data Owners.

This control weakness occurred because OIT did not enforce its policy requiring Data Owners to review and validate user access accounts.

Separation of duties reduces the risk of potential abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion.

EAC Response: Agree

EAC OIT shall ensure that Data Owner access recertifications contain both signatures and dates signed. The form has been updated and EAC OIT is obtaining new certification signatures with dates.

3. Finding: EAC OIT has not implemented web and email security enhancements required by Binding Operational Directive 18-01.

EAC OIT has not implemented HTTP Strict Transport Security (HSTS) for one of its public-facing websites. EAC OIT has not implemented HSTS for its Vote by Mail website (votebymail.gov). HSTS ensures browsers always use an https:// connection, and removes the ability for users to click through certificate-related warnings.

HSTS reduces insecure redirects, and protects users against attacks that attempt to downgrade connections to plain HTTP.

These conditions occurred because EAC OIT lacks monitoring controls for remediating security weaknesses identified in the DHS CISA Trustworthy Email Report and HTTPS Report.

EAC Response: Agree.

The votebymail.gov website is used as a redirect to the primary EAC website, eac.gov. The eac.gov website enforces HTTPS and utilizes HSTS in accordance with BOD 18-01. EAC

OIT recognizes the need to add this capability even to redirect domains and is working with its web hosting provider to add HSTS headers to our redirect domains and add them to the Chrome preload list, as specified in the BOD.

4. Finding: EAC OIT did not maintain an accurate inventory of hardware assets for its operating environment.

EAC OIT uses several methods for maintaining inventory of information systems and software. GFI LANguard is used to discover and identify IT devices on EAC's network; thereby creating an asset inventory of every device on EAC's network. The WASP inventory application is used to tag and track the physical location of IT equipment, identify asset type, logging serial numbers, and document other data. EAC's procedures require EAC OIT to conduct physical inventory annually that requires system users to submit inventory verification forms listing assets in their possession.

The auditors traced a sample of eleven (11) 2020 Inventory Verification forms from a population of forty-one (41) assets. Of the forty-one assets tested, we noted ten (10) incidents were assets reported on the forms did not agree with the inventory report. Therefore, EAC OIT did not reconcile physical inventory to its inventory system report to accurately reflect the agency's operating environment.

Also, EAC OIT did not update hardware asset inventory records upon employees' separation from the agency. Specifically, records showed that one employee who separated from the agency still had a mobile device "in-use"; however, the device was assigned to another employee.

This condition occurred because EAC OIT lacks monitoring controls for maintaining inventory for hardware assets. Without accurate and complete inventories of the hardware assets connected to the agency's network, the agency may not be able to identify and properly mitigate hardware issues. In addition, the agency may not ensure proper accountability over agency assets and risk paying for unused or underutilized IT equipment or hardware.

EAC Response: Agree

Due to COVID-19 mandated remote work, inventory work conducted this year was also done remotely via user-reported manual inventory. The EAC shall implement controls to better reflect actual inventory and reconcile user-reported inventory against the agency's master inventory list. EAC OIT has rectified the discrepancies noted by the auditors.

U.S. ELECTION ASSISTANCE COMMISSION

633 3rd St. NW, Suite 200
Washington, DC 20001

5. Finding: EAC OIT does not consistently monitor controls to ensure its objectives outlined in its ISCM strategy is consistently implemented.

EAC OIT has developed an ISCM strategy that addresses the monitoring of security controls at the agency, business unit, and information system level. At the information system level, the ISCM strategy establishes processes for monitoring security controls for effectiveness and reporting any findings. However, in practice, EAC OIT is not monitoring controls to ensure its objectives outlined in its ISCM strategy is consistently implemented. Specifically, we noted that EAC OIT did not:

- Conduct weekly and quarterly vulnerability scans for information systems and hosted applications;
- Remediate high-risk vulnerabilities within 30 days and moderate-risk vulnerabilities within 90 days of discovery.
- Update policy and procedure documents for *Audit and Accountability Policy, Procurement Handbook, Security Incident Hand Book, Media Sanitation and Privacy Handbook* policy to reflect the agency's current operating environment to include MS Azure.

These control weaknesses occurred, in part, because the ISCM process did not include a process to measure the effectiveness or efficiency of monitoring activities stated in the agency's policy.

Continuous monitoring of threats, vulnerabilities, and security control effectiveness provides situational awareness for risk-based support of ongoing authorization decisions. ISCM performance metrics are used to assess, respond, and monitor risk across the organization. The focus of ISCM metrics is to provide adequate information about security control effectiveness, and organizational security status to allow officials to make informed, timely security risk management decisions.

EAC Response: Agree

The EAC has increased the breadth of its automated monitoring systems to cover all network endpoints. Additionally, the EAC has recently implemented an enterprise risk management solution tailored to its cloud environment to monitor and report compliance with all relevant security controls. All EAC OIT documentation has been updated to reflect the EAC's move the MS Azure cloud environment.

APPENDIX IV

U.S. ELECTION ASSISTANCE COMMISSION

633 3rd St. NW, Suite 200
Washington, DC 20001

Sincerely,

Jessica Bowers

Jessica Bowers
Acting CIO/CISO
U.S. Election Assistance Commission

OIG's Mission

Prevent fraud, waste, and abuse; promote economy and efficiency in EAC programs; and support the mission of the EAC by reporting on current performance and accountability and by fostering sound program management to help ensure effective government operations.

Obtain Copies of OIG Reports

Retrieve OIG reports on the OIG website, https://www.eac.gov/inspector-general/

Request copies by e-mail to: eacoig@eac.gov

Send mail orders to:

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

To order by phone: Voice: (866) 552-0004

Report Fraud, Waste or Abuse Involving the EAC or Help America Act Funds

By mail :

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

By e-mail:	eacoig@eac.gov
OIG Hotline	866-552-0004 (toll free)
On-line Complaint Form	https://www.eac.gov/inspector-general/file-a-complaint/

Inspector General

U.S. Election Assistance Commission

This report, as well as other OIG reports and testimony, are available on the internet at:
[EAC OIG Reports Page]()