U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL

Final Report:

EAC Compliance with the Federal Information Security Modernization Act Fiscal Year 2018

EAC IG Report No.
I-PA-EAC-02-18
November 2018

U.S. ELECTION ASSISTANCE COMMISSION
1335 EAST-WEST HIGHWAY, SUITE 4300
SILVER SPRING, MD 20910
OFFICE OF THE INSPECTOR GENERAL

Memorandum

Date: November 28, 2018

To: Thomas Hicks, Chairman
U.S. Election Assistance Commission

Patricia L. Layfield

From: Patricia Layfield
Inspector General

Subject: Final Report – Fiscal Year 2018 U.S. Election Assistance Commission Compliance with the Requirements of the Federal Information Security Modernization Act (Assignment No. I-PA-EAC-02-18)

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 nine recommendations to assist EAC in strengthening its information security program:

1. 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.

2. Document an information security architecture to provide a disciplined and structured methodology for managing risk.

3. Remediate configuration related vulnerabilities in the network identified, and document the results or document acceptance of the risks of those vulnerabilities.

4. Define and implement a process for conducting assessment of the knowledge, skills, and abilities of EAC's cybersecurity workforce.

5. Conduct a baseline assessment of the EAC's cybersecurity workforce that includes (1) the percentage of personnel with IT, cybersecurity, or other cyber-related job functions who hold certifications; (2) the level of preparedness of other cyber personnel without existing credentials to take certification exams; and (3) a strategy for mitigating any gaps identified with appropriate training and certification for existing personnel.

6. Review and approve EAC's information security policies and procedures on an annual basis.

7. Implement a remediation plan to commit resources to update all EAC-wide information security policies and procedures on the frequency required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4.

8. Develop a Business Impact Analysis.

9. Incorporate the results from the Business Impact Analysis into the analysis and strategy development efforts for the Agency's Continuity of Operations Plan (COOP).

EAC management generally agreed with the findings and recommendations; however, they noted in their response to Recommendation #1, they had already instituted many of the policies and procedures that would correspond to the FISMA Enterprise Risk Strategy requirements (see page 4 of Brown's report).

In accordance with *Government Auditing Standards*, Brown also followed up on the status of the recommendations contained in the 2017 FISMA audit report. They found that EAC had completed corrective actions on all but three of those recommendations (see Appendix II, page 14). The 2017 recommendations that remain uncorrected are:

- The Acting Chief Information Officer (ACIO)[1] should complete the formal timeline and implementation plan for enforcement of the use of PIV cards for two-factor authentication at the local network layer through its partnership with the General Services Administration (GSA).
- EAC management should document and implement a formal procedure for documenting the review of Service Organization Control reports for applicable third-party systems at a defined frequency.
- The ACIO should review and update the 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.

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

[1] Since the issuance of the prior year report, EAC has hired a full-time, permanent Chief Information Officer (CIO), who has assumed responsibility for the corrective actions.

- 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 (301) 734-3104.

cc: Commissioner Christy McCormick, Vice-Chair
Brian Newby, Executive Director
Mona Harrington, Chief Information Officer

Attachment

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

Fiscal Year 2018
EAC IG Report No.
I-PA-EAC-02-18
November 20, 2018

Prepared by

Brown & Company
Certified Public Accountants and Management Consultants,
PLLC
1101 Mercantile Lane, Suite 122
Largo, Maryland 20774
(240-770-4903)

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 final 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 contracted with the independent certified public accounting firm of Brown & Company CPAs to conduct the audit in support of the FISMA requirement for an annual evaluation of EAC's information security program.

The objective of this performance audit was to determine whether EAC 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 vulnerability assessment of internal systems and an evaluation of EAC's process for identifying and mitigating information systems vulnerabilities. Audit fieldwork was performed at EAC's headquarters in Silver Spring, MD from June 21, 2018 through October 22, 2018.

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 generally complied with FISMA requirements by implementing selected security controls for tested systems. 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 needed to be improved. We are making nine recommendations to assist EAC 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.

Sincerely,

Brown & Company CPAs
and Management Consultants, PLLC

Brown & company

November 20, 2018
Largo, 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 source. 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 the effectiveness of their information security program. In addition, FISMA has established that the standards and guidelines issued by the National Institute of Standards and Technology (NIST) are mandatory for federal agencies.

The EAC's Office of the Inspector General engaged us, Brown & Company CPAs and Management Consultants, PLLC, to conduct an audit in support of the FISMA requirement for an annual evaluation of EAC's information security program. The objective of this performance audit was to determine whether EAC 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

We concluded that EAC generally complied with FISMA by implementing 53 of 60[3] security controls reviewed for selected information systems. For example, EAC did the following:

- Categorized its information systems and the information processed, stored or transmitted in accordance with federal guidelines, and designated senior-level officials within the organization to review and approve the security categorizations.
- Implemented system and service acquisition controls.
- Implemented change management policy and procedures.
- Implemented an effective program for incident handling and response.
- Maintained an effective training program for general, specialized, and privileged users.

Although EAC generally had policies for its information security program, its implementation of those policies for 7 of 60 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 EAC's information security program that needed to be improved. Specifically, EAC needs to:

- Fully develop and implement enterprise risk strategy.
- Consistently resolve known serious vulnerabilities within the organizational timeframe.
- Conduct a baseline assessment of the Agency's cybersecurity workforce.
- Review and approve Agency's information security policies and procedures on an annual basis.
- Develop a Business Impact Analysis (BIA).

As a result, EAC's operations and assets may be at risk of unauthorized access, misuse and disruption. This report makes nine recommendations to assist EAC in strengthening its information security program. In addition, as illustrated in Appendix II, findings related to 3 of 11 prior year's recommendations had not yet been fully implemented, and therefore, new recommendations were not made. Detailed findings appear in the following section.

[3] See Appendix III for summary of controls reviewed.

Audit Findings

1. The EAC Office of Information Technology Needs to Fully Develop and Implement Its Enterprise Risk Strategy that Corresponds to NIST SP 800-39.

NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, PM-9 “Risk Management Strategy” states the following:

> The organization:
>
> a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;
> b. Implements the risk management strategy consistently across the organization; and
> c. Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.
>
> Supplemental Guidance:
> An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization’s risk tolerance, and approaches for monitoring risk over time.

NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, PL-8 “Information Security Architecture” states the following:

> The organization:
>
> a. Develops an information security architecture for the information system that:
>
> 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
> 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
> 3. Describes any information security assumptions about, and dependencies on, external services;
>
> b. Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and

c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations, and organizational procurements/acquisitions.

NIST Special Publication 800-39, Managing Information Security Risk, Mission, and Information System View, states the following:

> "The Special Publication 800-39 provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems".

EAC Office of Information Technology (OIT) has defined its risk management policies and procedures in Information Technology (IT) Risk Management and Risk Management Framework, revised on June 30, 2014. However, EAC has not fully developed its Enterprise Risk Management (ERM) Strategy to include 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.

In addition, EAC does not utilize an information security architecture to provide a disciplined and structured methodology for managing risk. The primary purpose of the information security architecture is to ensure that mission/business process-driven information security requirements are consistently and cost effectively achieved in organizational information systems and the environments in which those systems operate are consistent with the organizational risk management strategy.

EAC OIT did not have adequate resources (people, processes and technology) to fully develop ERM strategy and information security architecture.

The lack of an Enterprise Risk Management strategy and information security architecture reduces the degrees of security, privacy, reliability, and cost-effectiveness for the missions and business functions being carried out by organizations.

Recommendation 1: We recommend 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.

Recommendation 2: We recommend EAC Chief Information Officer to document an information security architecture to provide a disciplined and structured methodology for managing risk.

Management's Response

EAC's management provided the following response to the finding and recommendation:

***EAC Response**: Partially Agree. The EAC has instituted many policies and procedures that correspond with the FISMA Enterprise Risk Strategy (ERS) requirement. The EAC currently has approved and published a full Strategic Plan, 2018- 2022. In addition, the EAC has implemented a Security Assessment Report (SAR), and several other technical procedures that categorize and mitigate risk. Many of the required ERS initiatives are developed.*

Auditor's Evaluation of Management's Response
EAC's management concurred with the recommendations.

Management's full response is provided in **Appendix V**

2. EAC OIT did not Consistently Resolve Known Serious Vulnerabilities within the Organizational timeframe.

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* SI-2 "Flaw Remediation," states the following:

> The organization:
>
> a. Identifies, reports, and corrects information system flaws;
> b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
> c. Installs security-relevant software and firmware updates within organization-defined time period of the release of the updates; and
> d. Incorporates flaw remediation into the organizational configuration management process.

The Vulnerability Assessment is an automated assessment of Internet or intranet connected assets, including firewalls, routers, web and mail servers and other hosts residing within the provided IP address range. An independent internal vulnerability scan performed using Qualys on EAC's internal networks confirmed 47 "Serious," 27 "Medium," and 1 "Minimal" risk vulnerabilities related to patch and configuration management.

EAC OIT runs Nessus scans on a daily basis; however, vulnerabilities are not being remediated timely. Internal vulnerability scan performed by Brown and Company IT team on August 16, 2018 identified 47 serious vulnerabilities relating to the SSL/TLS server supports TLSv1.0.

For the above condition, EAC required additional resources to resolve serious vulnerabilities.

Unmitigated vulnerabilities on EAC's network can compromise the confidentiality, integrity, and availability of [4]EAC data. For example:

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

Recommendation 3: We recommend EAC OIT to remediate configuration related vulnerabilities in the network identified, and document the results or document acceptance of the risks of those vulnerabilities.

[444] *NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, SI-2 "Flaw Remediation,"* https://nvd.nist.gov/800-53/Rev4/control/SI-2

Management's Response

EAC's management provided the following response to the finding and recommendation:

> ***EAC Response**: Agree. It is important to note that all vulnerabilities were resolved before the end of the fiscal year. The EAC utilizes both IBM Big Fix, and Nessus Scanners regularly and has policies in place both to detect vulnerabilities and resolve them.*

Auditor's Evaluation of Management's Response

EAC's management concurred with the recommendations.

Management's full response is provided in **Appendix V.**

3. EAC OIT needs to conduct a Baseline Assessment of the Agency's Cybersecurity Workforce.

NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, PM-13 "Information Security Workforce," states:

> The organization establishes an information security workforce development and improvement program.
>
> Supplemental Guidance: Information security workforce development and improvement programs include, for example: (I) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. Such workforce programs can also include associated information security career paths to encourage: (I) information security professionals to advance in the field and fill positions with greater responsibility; and (ii) organizations to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals.

NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*

> Use of the NICE Framework's common lexicon enables employers to inventory and develop their cybersecurity workforce. The NICE Framework can be used by employers and organizational leadership to:
>
> - Inventory and track their cybersecurity workforce to gain a greater understanding of the strengths and gaps in Knowledge, Skills, and Abilities and Tasks performed;
> - Identify training and qualification requirements to develop critical Knowledge, Skills, and Abilities to perform cybersecurity Tasks;
> - Improve position descriptions and job vacancy announcements selecting relevant KSAs and Tasks, once work roles and tasks are identified;

- Identify the most relevant work roles and develop career paths to guide staff in gaining the requisite skills for those roles; and
- Establish a shared terminology between hiring managers and human resources staff for the recruiting, retention, and training of a highly-specialized workforce.

Federal Cybersecurity Workforce Assessment Act of 2015

This bill requires federal agencies to: (1) identify all personnel positions that require the performance of information technology, cybersecurity, or other cyber-related functions; and (2) assign a corresponding employment code to such positions using a coding structure that the National Institute of Standards and Technology must include in the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework.

***

Federal agencies must submit to Congress a report identifying: (1) the percentage of personnel with such job functions who currently hold industry-recognized certifications, (2) the preparedness of other civilian and non-civilian cyber personnel without existing credentials to pass certification exams, and (3) a strategy for mitigating any identified gaps with training and certification for existing personnel.

The agencies must establish procedures to identify all encumbered and vacant positions with such functions and assign the appropriate employment code to each position.

Annually through 2022, the agencies must submit a report to the U.S. Office of Personnel Management (OPM) that identifies cyber-related roles designated as critical needs in the agency's workforce. The OPM must provide agencies with guidance for identifying roles with acute and emerging skill shortages.

***

EAC has established and maintained its organization-wide security awareness and training program as roles-based training of system users with significant security responsibilities. However, EAC has not defined a process for conducting an assessment of the knowledge, skills, and abilities of its workforce to determine its awareness and specialized training needs.

Also, EAC did not conduct a baseline assessment of the Agency’s cybersecurity workforce that includes (1) the percentage of personnel with IT, cybersecurity, or other cyber-related job functions who hold certifications; (2) the level of preparedness of other cyber personnel without existing credentials to take certification exams; and (3) a strategy for mitigating any gaps identified with appropriate training and certification for existing personnel.

EAC did not have adequate resources (people, processes and technology) to conduct a baseline assessment of the Agency’s cybersecurity workforce.

EAC has not complied with the Federal Cybersecurity Workforce Assessment Act of 2015. The lack of a full cybersecurity workforce assessment increases the risk that cybersecurity workforce requirements are not aligned with the Agency’s strategic goals Plan. In addition, EAC will not have the mechanism to identify gaps between the current and future workforce competencies.

<u>Recommendation 4</u>: We recommend the EAC to define and implement a process for conducting assessment of the knowledge, skills, and abilities of EAC's cybersecurity workforce.

<u>Recommendation 5:</u> We recommend the EAC to conduct a baseline assessment of the Agency's cybersecurity workforce that includes (1) the percentage of personnel with IT, cybersecurity, or other cyber-related job functions who hold certifications; (2) the level of preparedness of other cyber personnel without existing credentials to take certification exams; and (3) a strategy for mitigating any gaps identified with appropriate training and certification for existing personnel.

<u>Management's Response</u>

EAC's management provided the following response to the finding and recommendation:

> ***EAC Response****: Agree. The EAC agrees that a baseline assessment is a good practice. Moreover, the EAC recognizes that a key component of mitigating and responding to cyber threats is having a qualified, well-trained cybersecurity workforce despite the agency's limited personnel. In an effort to improve the EAC security posture, the EAC recently hired a CIO that possess a Master of Science degree in Cyber Security from the Rochester Institute of Technology.*

<u>Auditor's Evaluation of Management's Response</u>

EAC's management concurred with the recommendations.

Management's full response is provided in **Appendix V.**

4. EAC's Information Security Policies, Procedures, and Security Plans were either outdated or incomplete.

NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, PL-2 "System Security Plan" states:

a) Develops a security plan for the information system that:

1. Is consistent with the organization's enterprise architecture;
2. Explicitly defines the authorization boundary for the system;
3. Describes the operational context of the information system in terms of missions and business processes;
4. Provides the security categorization of the information system including supporting rationale;
5. Describes the operational environment for the information system and relationships with or connections to other information systems;
6. Provides an overview of the security requirements for the system;
7. Identifies any relevant overlays, if applicable;
8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b) Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];

c) Reviews the security plan for the information system [Assignment: organization-defined frequency];
d) Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
e) Protects the security plan from unauthorized disclosure and modification.

EAC's *Information Technology Security Plan*, version 1, updated in 2010, requires EAC to develop a system security plan for the information system that is consistent with the organization's enterprise structure and that is updated to address changes to the information system/environment of operation. Further, EAC is required to review its information security policies and procedures on an annual basis and update as necessary to address risks and changes within its environment. However, we noted the following EAC *Information Technology Security Plan*, which is the Agency's System Security Plan (SSP), was not updated to implement current Federal Laws, Regulation and Polices that include:

- NIST SP 800-12, Rev. 1, *An Introduction to Information Security,* June 2017;
- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* December 2014*;*
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments,* September 2012;
- NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View,* March 2011;
- NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* December 2014*;*
- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,* February 3. 2011;
- Federal Cybersecurity Workforce Assessment Act of 2015;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance, December 2011;
- FIPS PUB 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors, April 2013;* and others criteria published after 2010.

Therefore, the system security plan did not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements and sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans.

In addition, EAC policies and procedures documents are not reviewed/updated on a timely basis, including, but not limited to, the following documents*: Management Implementation Plan; Access Control Procedural Guide; Configuration Management (CM); Auditing and Monitoring, IT Security Training and Awareness Program; Password Generation and Protection; IT Risk Management and Risk Management Framework; General Support System Security Risk Assessment Report; Information Technology General Rules of Behavior; FISMA Implementation; Plan of Action and Milestones (POA&M); Disaster Recovery Plan; IT Security Incident Handling; Termination and Transfers; Media Sanitization;* and *Federal Information Processing Standards (FIPS) 199.*

EAC did not have adequate resources (people, processes and technology) to properly develop a System Security Plan, and review/update other policies and procedures documents on a timely basis.

EAC-wide information security polices provide guidance over controls implemented over the information system. Outdated documentation can lead to a misunderstanding of the information system control environment. This can lead to improper control implementations, thus increasing the risk of systems failure or downtime.

Recommendation 6: We recommend EAC to review and approve Agency's information security policies and procedures on an annual basis.

Recommendation 7: We recommend 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.

Management's Response
EAC's management provided the following response to the finding and recommendation:

> ***EAC Response**: Agree. We are in the process of reviewing and updating security documents as needed despite EAC's limited resources.*

Auditor's Evaluation of Management's Response
EAC's management concurred with the recommendations.

Management's full response is provided in **Appendix V.**

5. EAC has not defined Processes for Conducting Organizational and System-level Business Impact Analysis.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems, Section 3.2 "Conduct the Business Impact Analysis´ states:

> The Business Impact Analysis (BIA) is a key step in implementing the CP controls in NIST SP 800-53 and in the contingency planning process overall. The BIA enables the Information Systems Contingency Plan Coordinator to characterize the system components, supported mission/business processes, and interdependencies. Three steps are typically involved in accomplishing the BIA:
>
> - Determine mission/business processes and recovery criticality.
> - Identify resource requirements.
> - Identify recovery priorities for system resources.

NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, CP-2(3) Contingency Plan | Resume Essential Missions / Business Functions, states

> The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

CP 2(4) *Contingency Plan* | *Resume All Missions / Business Functions*

> The organization plans for the resumption of all missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

CP-2(5) Contingency Plan | Continue Essential Missions / Business Functions

> The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

EAC's *Continuity of Operation Plan (COOP) Guidelines*, revised June 30, 2014, identifies essential missions and business functions and associated contingency requirements. However, EAC has not conducted an organizational and system-level BIAs to support the COOP. A BIA will identify all business functions and characterize the consequences of their loss. The BIA can then be used to establish EAC's continuity requirements and prioritize their recovery based on their Recovery Time Objective.

EAC lacks resources to conduct organizational and system-level BIA and incorporate the results into strategy and plan development efforts.

The lack of a BIA to support the COOP will increase the time period of resumption of all mission/business functions.

Recommendation 8: We recommend EAC OIT to develop a Business Impact Analysis.

Recommendation 9: We recommend EAC to incorporate the results from the Business Impact Analysis into the analysis and strategy development efforts for the Agency's COOP.

Management's Response
EAC's management provided the following response to the finding and recommendation:

> ***EAC Response****: Agree. The EAC OIT will develop a Business Impact Analysis by February 28, 2019. The EAC will incorporate the results from the Business Impact Analysis into the analysis and strategy development efforts for the Agency's COOP by March 31, 2019.*

Auditor's Evaluation of Management's Response
EAC's management concurred with the recommendations.

Management's full response is provided in **Appendix V.**

Scope and Methodology

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 implemented selected security controls for certain information systems[5] in support of the Federal Information Security Modernization Act of 2014.

Our overall objective was to evaluate EAC's security program and practices, as required by FISMA. Specifically, we reviewed the status of the following areas of EAC's IT security program in accordance with U.S. Department of Homeland Security's (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 system and on external systems. The audit also included a vulnerability assessment of EAC-managed internal system and an evaluation of EAC's 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 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 designed and implemented. When appropriate, we conducted compliance tests using judgmental

[5] See Appendix IV for a list of controls selected.

sampling to determine the extent to which established controls and procedures are functioning as required.

To accomplish our audit objective, we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA;
- Reviewed documentation related to EAC's 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 FISMA audit reports; and
- Completed a network vulnerability assessment of EAC's 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.

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*;
- National Institute of Standards and Technology (NIST) Special Publication (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;*
- *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Rev. 1, Computer Security Incident Handling Guide;*
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information;*
- *NIST Special Publication (SP) 800-128, Guide for Security-Focused Configuration Management of Information Systems;*
- *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, Information Security for Continuous Monitoring (ISCM) for Federal Information Systems and Organizations;*
- *NIST Framework for Improving Critical Infrastructure Cybersecurity, V 1.0;*
- *Chief Financial Officers Council (CFOC) and the Performance Improvement Council (PIC) release the Playbook: Enterprise Risk Management (ERM);*
- *Federal Acquisition Regulation; FAR Case 2007-004, Common Security Configurations*
- *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control;*
- *OMB Memorandum M-08-05, Implementation of Trusted Internet Connections (TIC).*

The audit was conducted at EAC's headquarters in Silver Spring, MD, from June 21, 2018 through October 22, 2018.

Status of Prior Year Findings

The following table provides the status of the FY 2017 Audit Recommendation

No.	Fiscal Year (FY) 2017[6] Audit Recommendations	Status	Auditor's Position on Status
1	**FY 2017 FISMA audit recommendation No. 1:** The Acting Chief Information Officer (ACIO) should complete the formal timeline and implementation plan for enforcement of the use of PIV cards for two-factor authentication at the local network layer through its partnership with the General Services Administration (GSA).	Open	Agree
2	**FY 2017 FISMA audit recommendation No. 2:** EAC management should refine the process to renew interconnection documentation and monitor renewal timeframes going forward.	Closed	Agree
3	**FY 2017 FISMA audit recommendation No. 3:** EAC management, in coordination with GSA, should ensure current and signed Authorizations to Operate, which do not create any gaps in coverage, are issued for the GSA Enterprise Network Service.	Closed	Agree
4	**FY 2017 FISMA audit recommendation No. 4:** The ACIO should implement corrective actions to resolve critical and high-risk vulnerabilities identified related to patching, software upgrades, and configuration weaknesses for those systems identified within detailed scanning results.	Closed	Agree
5	**FY 2017 FISMA audit recommendation No. 5:** The ACIO should implement a process to perform scans on a regular basis and remediate weaknesses noted from those scans that is built into the larger effort of implementing tools as part of DHS Continuous Diagnostic and Mitigation tools.	Closed	Agree
6	**FY 2017 FISMA audit recommendation No. 6:** The ACIO should document any deviations from the U.S. Government Configuration Baseline to include business justifications for each deviation.	Closed	Agree

[6] 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).

No.	Fiscal Year (FY) 2017[6] Audit Recommendations	Status	Auditor's Position on Status
7	**FY 2017 FISMA audit recommendation No. 7:** The ACIO should revise and implement the existing Auditing and Monitoring procedures to outline the frequency of audit log reviews and responsibilities around all monitoring activities.	Closed	Agree
8	**FY 2017 FISMA audit recommendation No. 8:** EAC management should document and implement a formal procedure for documenting the review of Service Organization Control reports for applicable third-party systems at a defined frequency.	Open	Agree
9	**FY 2017 FISMA audit recommendation No. 9:** The ACIO should review and update the 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.	Open	Agree
10	**FY 2017 FISMA audit recommendation No. 10:** The ACIO should test the COOP annually using a rotational testing schedule that includes review of the test results and response to corrective actions identified as part of lessons learned exercises subsequent to testing.	Closed	Agree
11	**FY 2017 FISMA audit recommendation No. 11:** The ACIO should update the POA&M report to cover all information from required fields, benchmark the state of corrective actions, and identify next steps. The ACIO should also maintain and review POA&Ms in line with the frequency defined by EAC policy and ensure all known control weaknesses are documented in the POA&Ms.	Closed	Agree

Summary of Controls Reviewed

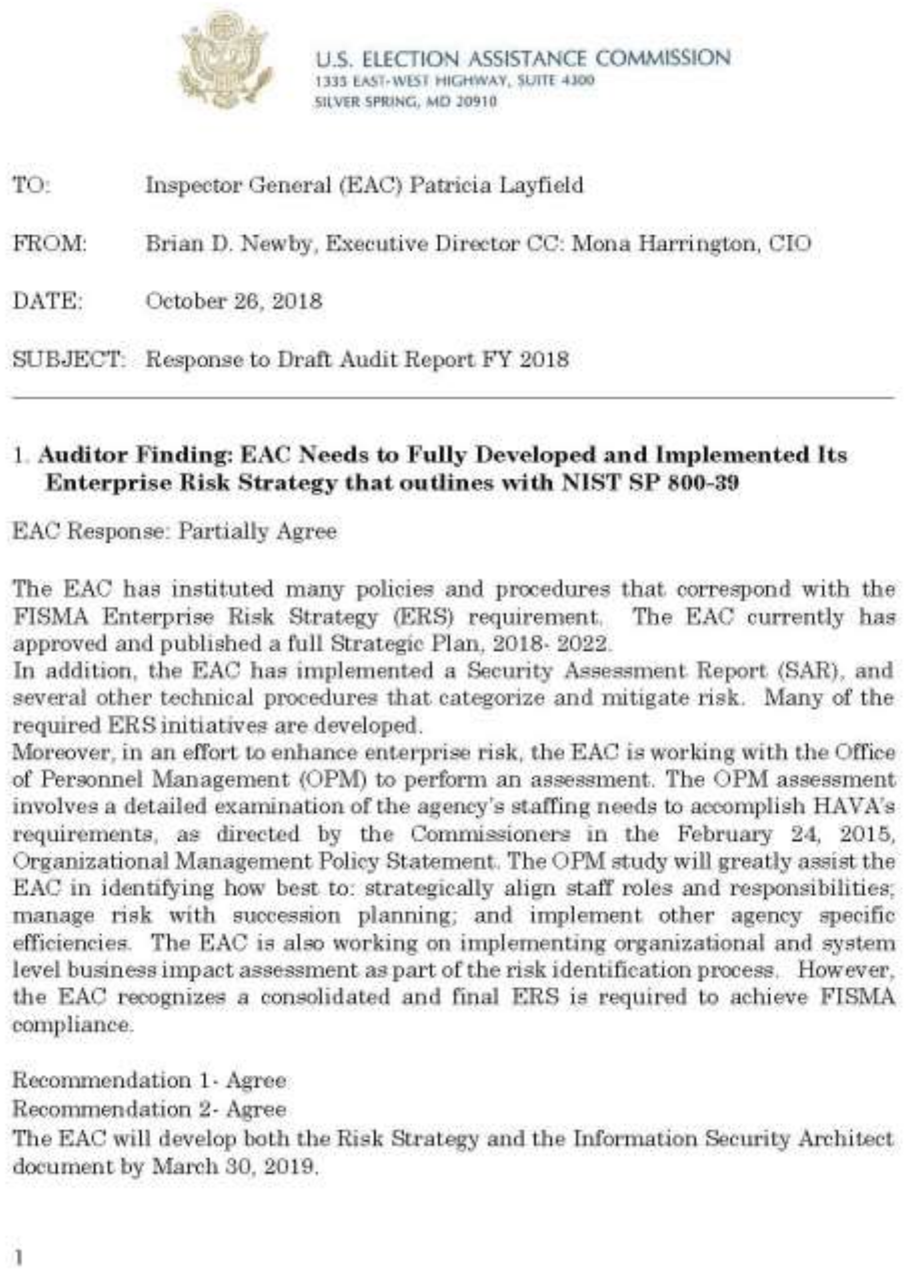
Control No.	Control Name	Is Control Effective?
CP-2	Contingency Plan	Not Effective, See Finding 5
CP-6	Alternative Storage Site	Yes
CP-7	Alternative Processing Site	Yes
CP-8	Telecommunications Services	Yes
CP-9	Information System Backup	Yes
IA-1	Identification & Authentication Policy and Procedures	Yes
IR-1	Incident Response Policy & Procedures	Yes
IR-4	Incident Handling	Yes
IR-6	Incident Reporting	Yes
MP-6	Media Sanitization	Yes
PL-2	System Security Plan	Not Effective, See Finding 4
PL-4	Rules of Behavior	Yes
PL-8	Information Security Architecture	Not Effective, See Finding 1
PM-5	Information System Inventory	Yes
PM-9	Risk Management Strategy	Not Effective, See Finding 1
PS-1	Personnel Security Policy and Procedures	Yes
PS-2	Position Risk Designation	Yes
PS-3	Personnel Screening	Yes
PS-6	Access Agreements	Yes
RA-1	Risk Assessment Policy and Procedures	Yes
RA-2	Security Categorization	Yes
SA-4	Acquisitions Process	Yes
SC-7	Boundary Protection	Yes
SC-8	Transmission Confidentiality and Integrity	Yes
SC-28	Protection of Information at Rest	Yes
SE-2	Privacy Incident Response	Yes
SI-2	Flaw remediation	Not Effective, See Finding 2
SI-3	Malicious Code Protection	Yes
SI-4	Information System Monitoring	Yes

Appendix IV

Acronyms

ACIO	Acting Chief Information Officer
BIA	Business Impact Analysis
CM	Configuration Management
COOP	Continuity of Operation Plan
CP	Contingency Plan
DHS	U.S. Department of Homeland Security
ERM	Enterprise Risk Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
IT	Information Technology
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OIT	Office of Information Technology
OMB	U.S. Office of Management and Budget
OPM	U.S. Office of Personnel Management
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SA&A	Security Assessment and Authorization
SP	Special Publication
SSP	System Security Plan

Management Comments



U.S. ELECTION ASSISTANCE COMMISSION
1335 EAST-WEST HIGHWAY, SUITE 4300
SILVER SPRING, MD 20910

TO: Inspector General (EAC) Patricia Layfield

FROM: Brian D. Newby, Executive Director CC: Mona Harrington, CIO

DATE: October 26, 2018

SUBJECT: Response to Draft Audit Report FY 2018

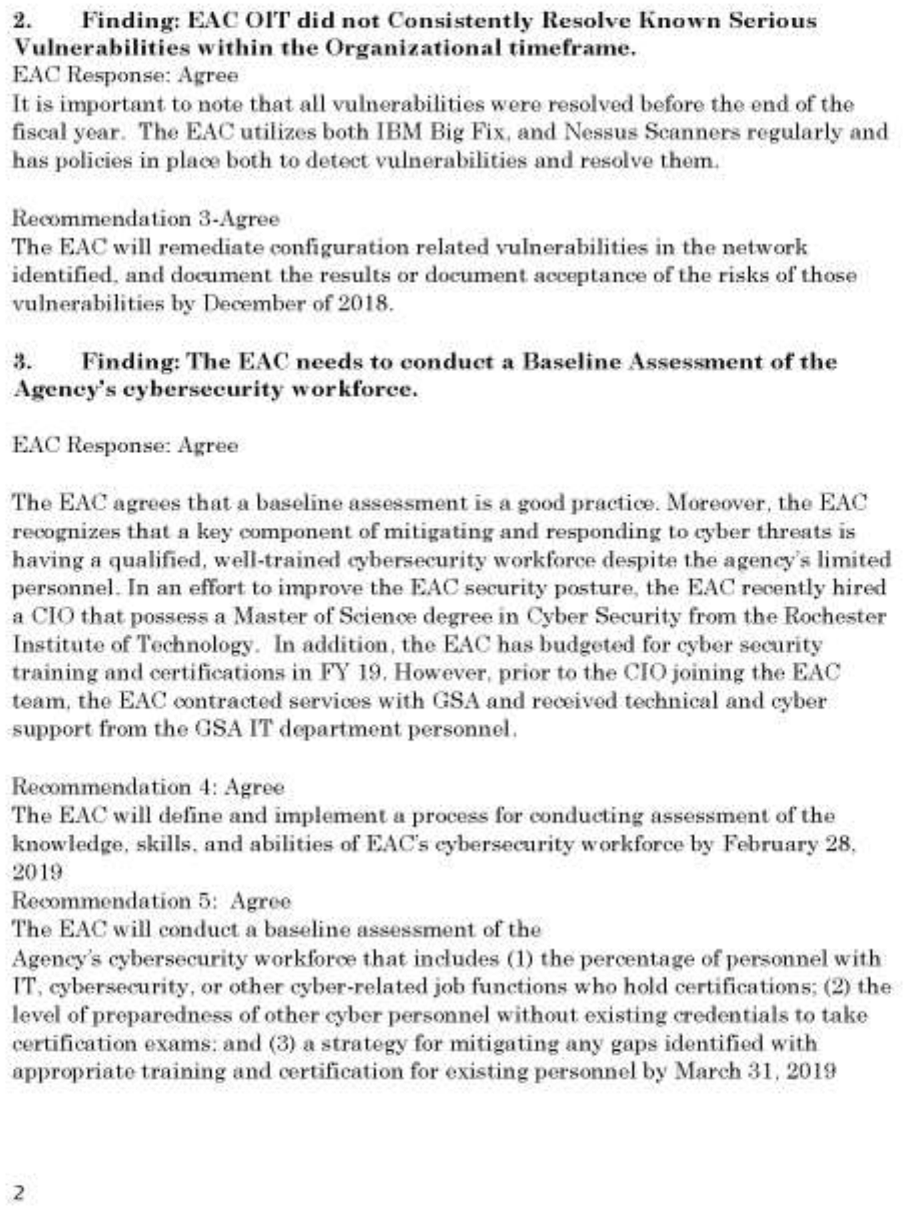
1. **Auditor Finding: EAC Needs to Fully Developed and Implemented Its Enterprise Risk Strategy that outlines with NIST SP 800-39**

EAC Response: Partially Agree

The EAC has instituted many policies and procedures that correspond with the FISMA Enterprise Risk Strategy (ERS) requirement. The EAC currently has approved and published a full Strategic Plan, 2018- 2022.
In addition, the EAC has implemented a Security Assessment Report (SAR), and several other technical procedures that categorize and mitigate risk. Many of the required ERS initiatives are developed.
Moreover, in an effort to enhance enterprise risk, the EAC is working with the Office of Personnel Management (OPM) to perform an assessment. The OPM assessment involves a detailed examination of the agency's staffing needs to accomplish HAVA's requirements, as directed by the Commissioners in the February 24, 2015, Organizational Management Policy Statement. The OPM study will greatly assist the EAC in identifying how best to: strategically align staff roles and responsibilities; manage risk with succession planning; and implement other agency specific efficiencies. The EAC is also working on implementing organizational and system level business impact assessment as part of the risk identification process. However, the EAC recognizes a consolidated and final ERS is required to achieve FISMA compliance.

Recommendation 1- Agree
Recommendation 2- Agree
The EAC will develop both the Risk Strategy and the Information Security Architect document by March 30, 2019.

1



2. Finding: EAC OIT did not Consistently Resolve Known Serious Vulnerabilities within the Organizational timeframe.
EAC Response: Agree
It is important to note that all vulnerabilities were resolved before the end of the fiscal year. The EAC utilizes both IBM Big Fix, and Nessus Scanners regularly and has policies in place both to detect vulnerabilities and resolve them.

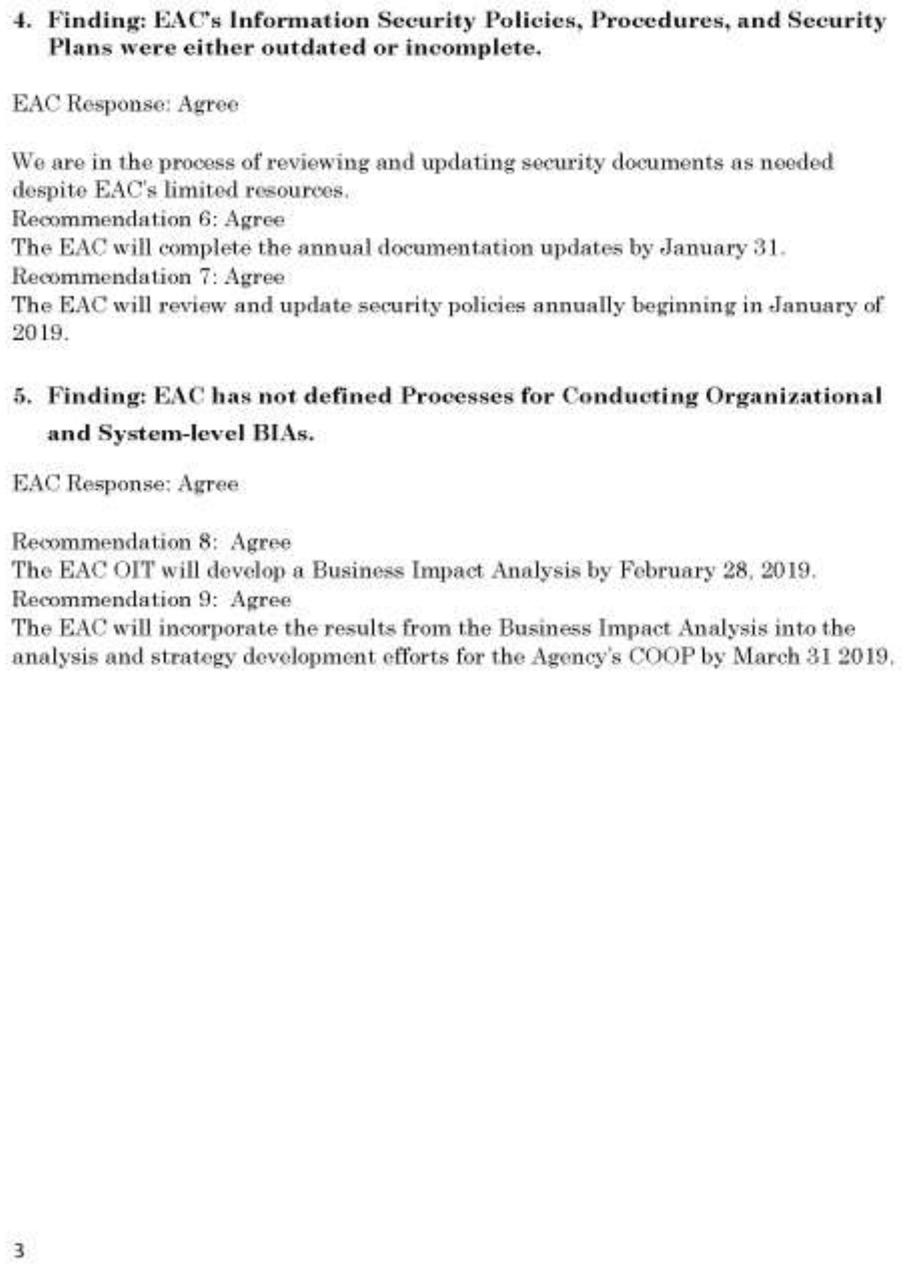
Recommendation 3-Agree
The EAC will remediate configuration related vulnerabilities in the network identified, and document the results or document acceptance of the risks of those vulnerabilities by December of 2018.

3. Finding: The EAC needs to conduct a Baseline Assessment of the Agency's cybersecurity workforce.

EAC Response: Agree

The EAC agrees that a baseline assessment is a good practice. Moreover, the EAC recognizes that a key component of mitigating and responding to cyber threats is having a qualified, well-trained cybersecurity workforce despite the agency's limited personnel. In an effort to improve the EAC security posture, the EAC recently hired a CIO that possess a Master of Science degree in Cyber Security from the Rochester Institute of Technology. In addition, the EAC has budgeted for cyber security training and certifications in FY 19. However, prior to the CIO joining the EAC team, the EAC contracted services with GSA and received technical and cyber support from the GSA IT department personnel.

Recommendation 4: Agree
The EAC will define and implement a process for conducting assessment of the knowledge, skills, and abilities of EAC's cybersecurity workforce by February 28, 2019
Recommendation 5: Agree
The EAC will conduct a baseline assessment of the
Agency's cybersecurity workforce that includes (1) the percentage of personnel with IT, cybersecurity, or other cyber-related job functions who hold certifications; (2) the level of preparedness of other cyber personnel without existing credentials to take certification exams; and (3) a strategy for mitigating any gaps identified with appropriate training and certification for existing personnel by March 31, 2019



4. Finding: EAC's Information Security Policies, Procedures, and Security Plans were either outdated or incomplete.

EAC Response: Agree

We are in the process of reviewing and updating security documents as needed despite EAC's limited resources.
Recommendation 6: Agree
The EAC will complete the annual documentation updates by January 31.
Recommendation 7: Agree
The EAC will review and update security policies annually beginning in January of 2019.

5. Finding: EAC has not defined Processes for Conducting Organizational and System-level BIAs.

EAC Response: Agree

Recommendation 8: Agree
The EAC OIT will develop a Business Impact Analysis by February 28, 2019.
Recommendation 9: Agree
The EAC will incorporate the results from the Business Impact Analysis into the analysis and strategy development efforts for the Agency's COOP by March 31 2019.

3

What is the OIG mission?

The OIG mission is to provide timely, high-quality professional products and services that are useful to OIG's clients. OIG seeks to provide value through its work, which is designed to enhance the economy, efficiency, and effectiveness in EAC operations so they work better and cost less in the context of today's declining resources. OIG also seeks to prevent or detect and investigate fraud, waste, abuse, and mismanagement in these programs and operations. Products and services include traditional financial and performance audits, contract and grant audits, information systems audits, and evaluations.

How can I obtain copies of OIG reports?

Copies of OIG reports are available at the EAC OIG website:

https://www.eac.gov/inspector-general/reports/

The reports are also available at Oversight.gov, a one-stop, publicly accessible, searchable website containing the latest public reports from the Federal Inspectors General who are members of the Council of the Inspectors General on Integrity and Efficiency:

https://www.oversight.gov/

Copies may also be requested directly from the OIG using the contact information below.

How can I report fraud, waste or abuse involving the U.S. Election Assistance Commission or Help America Vote Act Funds?

Mail: U.S. Election Assistance Commission
Office of Inspector General
1335 East-West Highway, Suite 4300
Silver Spring, MD 20910

E-mail: eacoig@eac.gov

OIG Hotline: 866-552-0004 (toll free)

FAX: 301-734-3115