U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL

Final Report:

EAC Compliance with the Federal Information Security Modernization Act Fiscal Year 2019

EAC IG Report No.
I-PA-EAC-02-19
December 2019

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

Memorandum

Date: December 31, 2019

To: Christy McCormick, Chairwoman
U.S. Election Assistance Commission

From: Patricia Layfield
Inspector General

Subject: Final Report – Fiscal Year 2019 U.S. Election Assistance Commission Compliance with the Requirements of the Federal Information Security Modernization Act (Assignment No. I-PA-EAC-02-19)

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:

- Conduct physical inventory to ensure accuracy of IT asset.
- Implement multifactor authentication for privileged accounts.
- Utilize the Security Content Automation Protocol (SCAP) Tools to monitor and control configuration settings.
- Develop an annual specialized training schedule to provide specialized security training for IT specialists and track the completion of training to ensure OIT meets its organizational training objectives.

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 the 2017 and 2018 FISMA audit reports. They found that EAC had completed corrective actions on all but three of those recommendations (see Appendix II, page 14). The 2017-2018 recommendations that remain uncorrected are:

- 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. (2017)
- 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. (2018)
- Document an information security architecture to provide a disciplined and structured methodology for managing risk. (2018)
- 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)

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 (301) 734-3104.

cc: Commissioner Benjamin W. Hovland, Vice-Chair
Commissioner Donald L. Palmer
Commissioner Thomas Hicks
Mona Harrington, Acting Executive Director and 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 2019
December 9, 2019
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 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 (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 vulnerability assessment of internal systems and an evaluation of EAC OIT process for identifying and mitigating information systems vulnerabilities. Audit fieldwork was performed at EAC's headquarters in Silver Spring, MD from May 6, 2019 through September 30, 2019.

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 9, 2019
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 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 OIG engaged us, 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. The objective of this performance audit 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 EAC OIT information security program that needed to be improved. Specifically, EAC OIT needs to:

- Conduct physical inventory to ensure accuracy of IT asset.
- Implement multifactor authentication for privileged accounts.
- Utilize the Security Content Automation Protocol (SCAP) Tools to monitor and control configuration settings.
- Provide specialized security training for IT specialists.

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 seven of 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 has not conducted physical inventory to ensure accuracy of IT asset.

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

> The organization:
>
> a. Develops and documents an inventory of information system components that:
>
> 1. Accurately reflects the current information system;
> 2. Includes all components within the authorization boundary of the information system;
> 3. Is at the level of granularity deemed necessary for tracking and reporting; and
> 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and
>
> b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].
>
> Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.

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 for tagging and tracking the physical location of IT equipment, identifying asset type, logging serial numbers and documenting other data. In addition, EAC OIT uses spreadsheets to track software installation. EAC’s procedures require EAC OIT to conduct physical inventory annually. However, EAC OIT did not conduct a physical inventory of EAC’s IT equipment in FY19.

EAC OIT planned to automate its manual process for conducting physical inventory of EAC’s IT equipment in FY19. However, EAC OIT did not implement an automated process for conducting a physical inventory and failed to conduct physical inventory to ensure the accuracy of EAC’s IT inventory.

The effect of not conducting physical inventory to maintain effective accountability of EAC's IT inventory, increases the risk of losing the ability to rapidly identify the location of a compromised or breached system that needs mitigation actions.

Recommendation 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.

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

> ***EAC Response:*** *Agree. EAC OIT shall conduct a 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, and model. EAC OIT has already conducted the yearly physical inventory and will develop a plan for timely review and sign off with end users.*

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

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

2. The EAC OIT has not implement multifactor authentication for network access to privileged accounts.

NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, IA-2 "Identification and Authentication (Organization Users)" states:

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Control Enhancements:

(1) Identification and Authentication | Network Access to Privileged Accounts

The information system implements multifactor authentication for network access to privileged accounts.

(3) Identification and Authentication | Local Access to Privileged Accounts

The information system implements multifactor authentication for local access to privileged accounts.

(6) Identification and Authentication | Network Access to Privileged Accounts - Separate Device

The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].

(8) Identification and Authentication | Network Access to Privileged Accounts - Replay Resistant.

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

(11) Identification and Authentication | Remote Access - Separate Device

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].

(12) Identification and Authentication | Acceptance of PIV Credentials

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

The EAC OIT developed and implemented a plan for the multifactor authentication (HSPD-12 PIV cards) for non-privileged users/accounts to access the agency's office, network and laptops, including remote access. However, EAC OIT has not implemented multifactor authentication for privileged user/accounts to access the agency's network.

EAC OIT has made progress in developing a plan and implementing multifactor authentication for non-privileged users/accounts. However, competing priorities of other activities within the IT department have caused the implementation of multifactor authentication for network access to privileged accounts to be delayed.

Lack of implementing multifactor authentication for privileged users/accounts increases the risk of exposing the agency's network to unauthorized access.

Recommendation 2: We recommend the EAC OIT prioritize and implement the use of multifactor authentication for network access for privileged accounts.

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

> ***EAC Response:*** *Agree. EAC OIT shall prioritize and implement the use of multifactor authentication for network access for privileged accounts. The use of multifactor authentication for network access is already in place for user accounts and is currently in the testing phase for administrative / privileged accounts.*

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 does not utilize the Security Content Automation Protocol (SCAP) Tools to monitor and control configuration settings.

The U.S. Office of Management and Budget, Guidance on the Federal Desktop Core Configuration (FDCC), M-08-22 memorandum, dated August 11, 2008, states:

> Both industry and government information technology providers must use SCAP validated tools with FDCC Scanner capability to certify their products operate correctly with FDCC configurations and do not alter FDCC settings.

NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, CM-6 "Configuration Settings," states:

> The organization:
>
> a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;
> b. Implements the configuration settings;
> c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and
> d. Monitors and controls change to the configuration settings in accordance with organizational policies and procedures.
>
> Supplemental Guidance: United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems.

NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, PM-4 "Plan of Action and Milestones Process," states:

> The organization:
>
> a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
>   1. Are developed and maintained;
>   2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
>   3. Are reported in accordance with OMB FISMA reporting requirements.

b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

EAC OIT has implemented policies and procedures for configuration settings and common secured configurations using US Government Configuration Baseline (USGCB) and the Center for Internet Security (CIS) recommended settings for its IT equipment. EAC OIT used BigFix to monitor and control configuration setting changes for Windows Servers and Microsoft Group Policies for Windows 10 workstations. EAC OIT discontinued the use of BigFix after an overseas company acquired the software. EAC OIT has not found a replacement for BigFix to monitor and control configuration setting changes for its IT equipment.

Competing priorities of other activities within the IT department have caused the delay of implementing a replace SCAP tool for monitoring and controlling configuration setting changes.

The lack of implementation of the SCAP validation software minimizes the agency's effectiveness to monitor and control changes to the configuration settings.

Recommendation 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.

Management's Response

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. EAC OIT shall 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.*

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 has not provided specialized security training for IT specialists.

NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, AT-3 "Role-based Security Training" states:

> The organization provides role-based security training to personnel with assigned security roles and responsibilities:
>
> a. Before authorizing access to the information system or performing assigned duties;
> b. When required by information system changes; and
> c. [Assignment: organization-defined frequency] thereafter.

> Supplemental Guidance: Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties.

NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, PM-14 “Testing, Training, and Monitoring” states:

> The organization:
>
> a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:
>   1. Are developed and maintained; and
>   2. Continue to be executed in a timely manner;
>
> b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

EAC OIT Information Technology Security Plan requires IT specialists to complete specialized IT security training as defined in the policy. In addition, EAC OIT has developed a security awareness training program which specifies that “additional training is appropriate for staff with specific obligations toward information security that are not satisfied by basic security awareness”. However, EAC OIT has not provided specialized IT security training for those with significant security responsibilities for FY 2019.

EAC OIT did not identify and develop a specialized IT training schedule and monitor the schedule to ensure the agency’s IT specialists obtained and completed training.

The lack of specialized IT security training for IT specialists increases the Agency’s inability to response to risk.

Recommendation 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.

Recommendation 5: We recommend EAC OIT track the training schedule to ensure individuals receive assigned training according to the agency’s policy.

Management’s Response

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

> ***EAC Response:*** *Agree. EAC OIT has identified and is currently developing a specialized IT training schedule which shall be monitored to ensure the agency’s IT specialists obtain and complete specialized IT security training.*

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[3] 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;
- 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 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 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

[3] 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 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 and 2018 FISMA audit reports; and
- Completed a network vulnerability assessment of 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*;
- 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 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 Memorandum M-08-05, Implementation of Trusted Internet Connections;*
- *SECURE Technology Act, Federal Acquisition Supply Chain Security;*
- *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*
- *US-CERT Incident Notification Guidelines.*

The audit was conducted at EAC's headquarters in Silver Spring, MD, from May 6, 2019 through September 30, 2019.

Appendix II – Status of Prior Years Findings

The following table provides the status of the FY 2017 and 2018 audit recommendations.

No.	Fiscal Years (FY) 2017[4] and 2018[5] 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.	Open	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.	Open	Agree
3.	**FY 2018 FISMA audit recommendation No. 2:** We recommend EAC Chief Information Officer to document an information security architecture to provide a disciplined and structured methodology for managing risk.	Closed	Agree
4.	**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] 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).

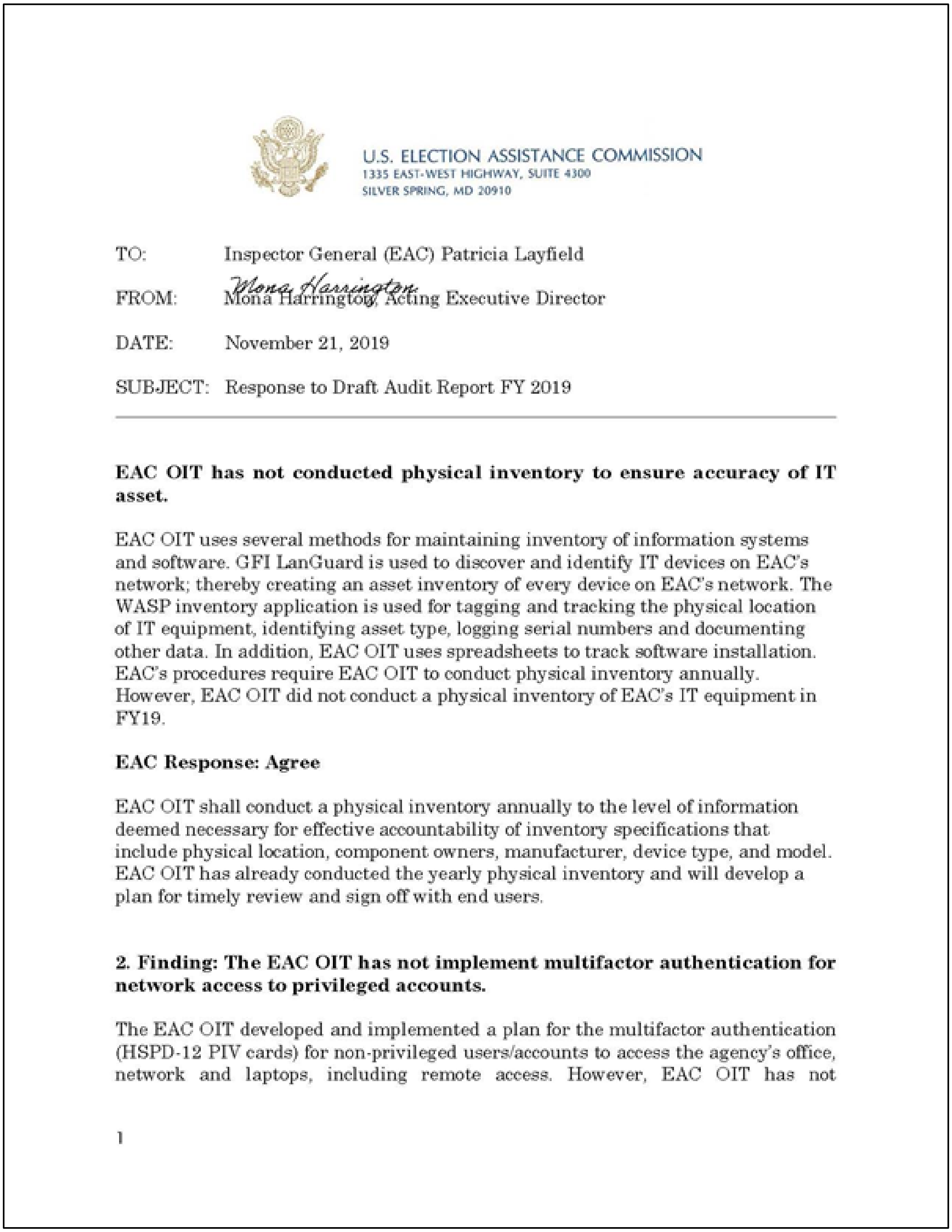
[5] The *Election Assistance Commission's Compliance with the Federal Information Security Modernization Act of 2014 (*EAC IG Report No. I-PA-EAC-02-18, November, 2018)

No.	Fiscal Years (FY) 2017[4] and 2018[5] Audit Recommendations	Status	Auditor's Position on Status
5.	**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
6.	**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
7.	**FY 2018 FISMA audit recommendation No. 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.	Closed	Agree

Appendix III - Acronyms

Acronyms	
CIO	Chief Information Officer
AT	Awareness and Training
CIS	Center for Internet Security
CM	Configuration Management
COOP	Continuity of Operation Plan
DHS	U.S. Department of Homeland Security
EAC	Election Assistance Commission
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
IA	Identification and Authentication
IG	Inspector General
IR	Incident Response
IT	Information Technology
NIST	National Institute of Standards and Technology
OIT	Office of Information Technology
OMB	U.S. Office of Management and Budget
PIV	Personal Identity Verification
PM	Program Management
POA&M	Plan of Action and Milestones
SA&A	Security Assessment and Authorization
SCAP	Security Content Automation Protocol
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline

Appendix IV – Management Comments



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

TO: Inspector General (EAC) Patricia Layfield

FROM: Mona Harrington
Mona Harrington, Acting Executive Director

DATE: November 21, 2019

SUBJECT: Response to Draft Audit Report FY 2019

EAC OIT has not conducted physical inventory to ensure accuracy of IT asset.

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 for tagging and tracking the physical location of IT equipment, identifying asset type, logging serial numbers and documenting other data. In addition, EAC OIT uses spreadsheets to track software installation. EAC's procedures require EAC OIT to conduct physical inventory annually. However, EAC OIT did not conduct a physical inventory of EAC's IT equipment in FY19.

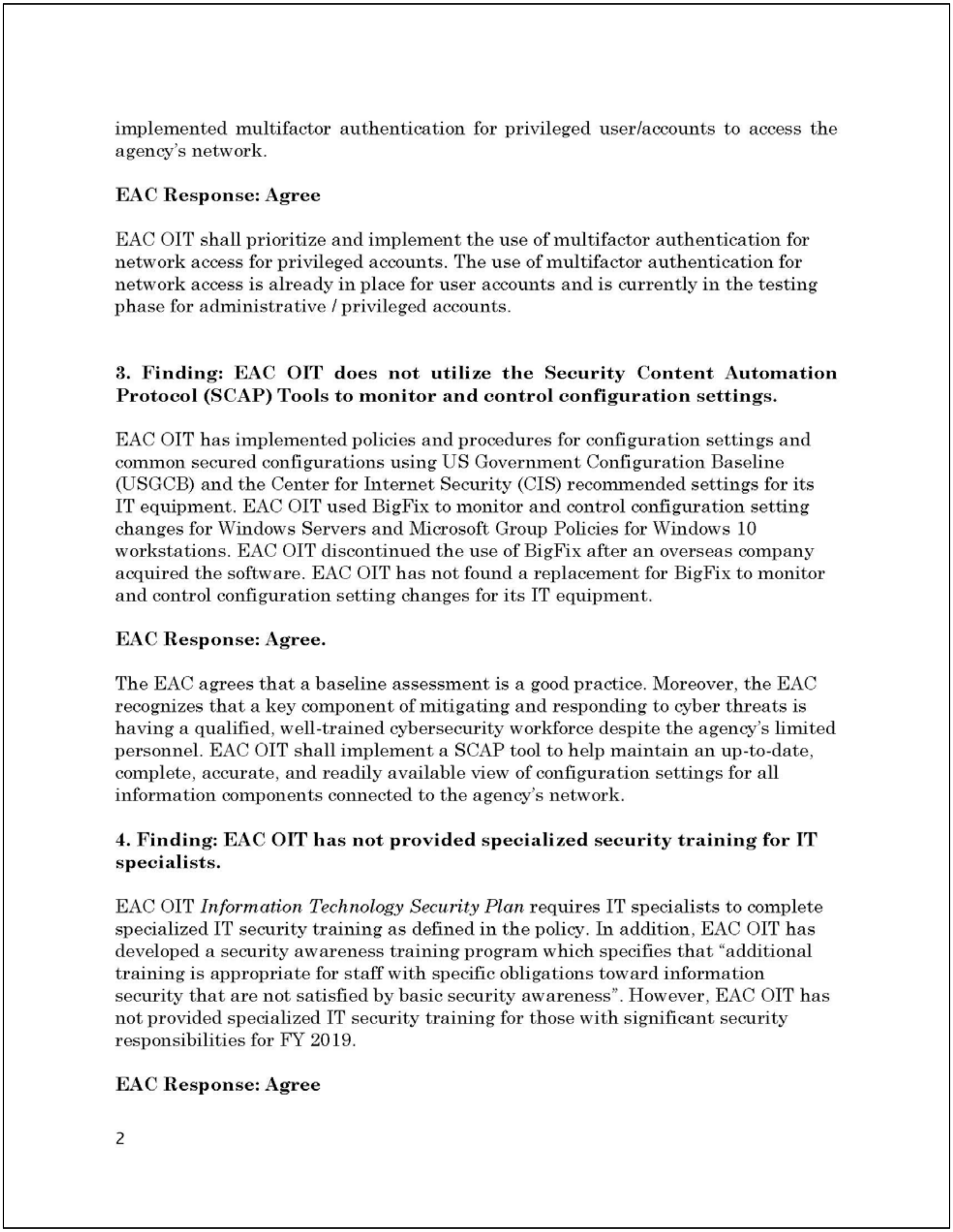
EAC Response: Agree

EAC OIT shall conduct a 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, and model. EAC OIT has already conducted the yearly physical inventory and will develop a plan for timely review and sign off with end users.

2. Finding: The EAC OIT has not implement multifactor authentication for network access to privileged accounts.

The EAC OIT developed and implemented a plan for the multifactor authentication (HSPD-12 PIV cards) for non-privileged users/accounts to access the agency's office, network and laptops, including remote access. However, EAC OIT has not

1



implemented multifactor authentication for privileged user/accounts to access the agency's network.

EAC Response: Agree

EAC OIT shall prioritize and implement the use of multifactor authentication for network access for privileged accounts. The use of multifactor authentication for network access is already in place for user accounts and is currently in the testing phase for administrative / privileged accounts.

3. Finding: EAC OIT does not utilize the Security Content Automation Protocol (SCAP) Tools to monitor and control configuration settings.

EAC OIT has implemented policies and procedures for configuration settings and common secured configurations using US Government Configuration Baseline (USGCB) and the Center for Internet Security (CIS) recommended settings for its IT equipment. EAC OIT used BigFix to monitor and control configuration setting changes for Windows Servers and Microsoft Group Policies for Windows 10 workstations. EAC OIT discontinued the use of BigFix after an overseas company acquired the software. EAC OIT has not found a replacement for BigFix to monitor and control configuration setting changes for its IT equipment.

EAC Response: Agree.

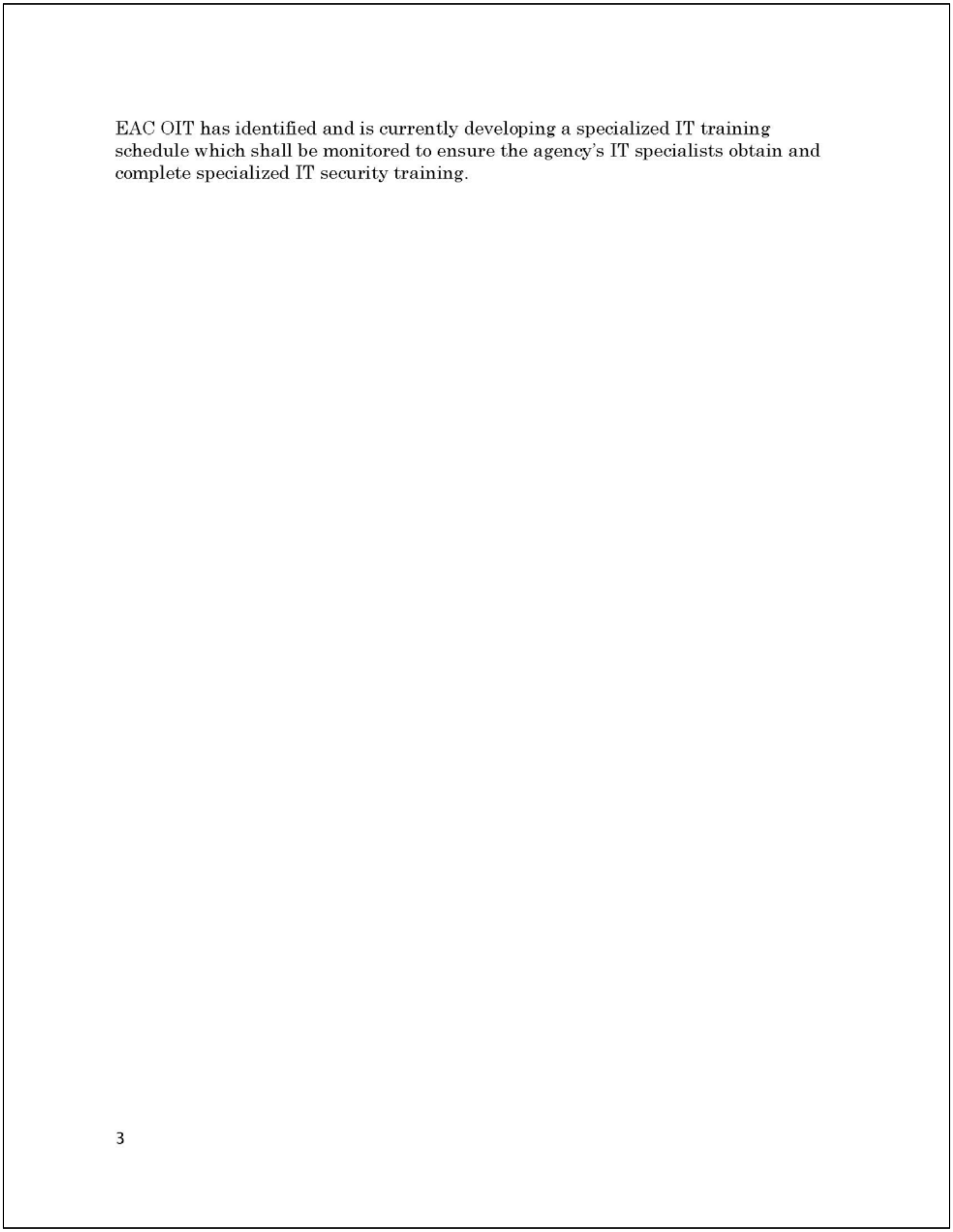
The EAC agrees that a baseline assessment is a good practice. Moreover, the EAC recognizes that a key component of mitigating and responding to cyber threats is having a qualified, well-trained cybersecurity workforce despite the agency's limited personnel. EAC OIT shall implement a SCAP tool to help maintain an up-to-date, complete, accurate, and readily available view of configuration settings for all information components connected to the agency's network.

4. Finding: EAC OIT has not provided specialized security training for IT specialists.

EAC OIT *Information Technology Security Plan* requires IT specialists to complete specialized IT security training as defined in the policy. In addition, EAC OIT has developed a security awareness training program which specifies that "additional training is appropriate for staff with specific obligations toward information security that are not satisfied by basic security awareness". However, EAC OIT has not provided specialized IT security training for those with significant security responsibilities for FY 2019.

EAC Response: Agree

APPENDIX IV



EAC OIT has identified and is currently developing a specialized IT training schedule which shall be monitored to ensure the agency's IT specialists obtain and complete specialized IT security training.

What is the OIG mission?

- The OIG audit 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 publicly accessible, searchable website containing the latest public reports from the Federal Inspectors General who are members of the Council of the Inspectors on Integrity and Efficiency: https://www.oversight.gov/

How can I report fraud, waste or abuse involving the EAC or HAVA 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