U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL

FINAL REPORT:

EAC COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT FISCAL YEAR 2017

EAC IG Report No.
I-PA-EAC-02-17
November 2017

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

Memorandum

Date: November 22, 2017

To: Matthew Masterson, Chairman
U.S. Election Assistance Commission

From: Patricia Layfield
Inspector General

Subject: Final Report – Fiscal Year 2017 U.S. Election Assistance Commission Compliance with the Requirements of the Federal Information Security Modernization Act (Assignment No. I-PA-EAC-02-17)

The Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA), 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 (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 47 of 60 security controls selected for testing within the information system CLA tested. Although EAC generally had policies for its information security program, its implementation of those policies was not fully effective to preserve the confidentiality, integrity, and availability of EAC'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.

CLA made eleven recommendations to assist EAC in strengthening its information security program:

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). (New)

2. EAC management should refine the process to renew interconnection documentation and monitor renewal timeframes going forward. (New)

3. EAC management, in coordination with GSA, should ensure current and signed Authorizations to Operate (ATOs), which do not create any gaps in coverage, are issued for the GSA Enterprise Network Services (ENS). (New)

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. (Repeat Modified)

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 CDM. (New)

6. The ACIO should document any deviations from the U.S. Government Configuration Baseline (USGCB) to include business justifications for each deviation. (New)

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. (Modified Repeat)

8. EAC management should document and implement a formal procedure for documenting the review of Service Organization Control (SOC) reports for applicable third party systems at a defined frequency. (New)

9. The ACIO should review and update the Continuity of Operations 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 Information Technology inventory checks. (New)

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. (New)

11. The ACIO should update the Plan of Action and Milestones (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. (New)

EAC management did not disagree with the findings and recommendations; however, they asserted that several of the issues discussed in the report are not under the direct control of EAC as a result of its significant dependence on GSA for network support and some of the necessary documentation. With regard to other issues, EAC has contracted with an industry and FISMA expert to aid in the development of many policies, procedures, and other means of correcting the identified weaknesses.

EVALUATION OF CLA'S AUDIT PERFORMANCE

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

- Reviewed CLA'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 periodic meetings with EAC management to discuss progress, findings, and recommendations;
- Reviewed CLA's draft audit report;
- Performed other procedures we deemed necessary; and
- Coordinated issuance of the audit report.

CLA is responsible for the attached auditor's report and the conclusions expressed in the report. The EAC OIG does not express any opinion on EAC's effectiveness of internal control or compliance with laws and regulations.

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. In addition, 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 Thomas Hicks, Vice-Chair
Commissioner Christy McCormick
Brian Newby, Executive Director
Henry Botchway, Senior IT Specialist

Attachment

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

Fiscal Year 2017

Final Report

CliftonLarsonAllen LLP
CLAconnect.com

November 15, 2017

Ms. Patricia Layfield
Inspector General
U.S. Election Assistance Commission
1335 East West Highway
Suite # 4300
Silver Spring, MD 20910

Dear Ms. Layfield:

Enclosed is the report of the *Audit of the Election Assistance Commission's (EAC) Fiscal Year 2017 Compliance with the Federal Information Security Modernization Act of 2014 (FISMA).*[1] The EAC Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP 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 selected information systems in support of FISMA. The audit included testing of certain management, technical, and operational controls outlined in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

For this audit, we reviewed EAC's General Support System, the Enterprise Network. The Enterprise Network provides the infrastructure that supports mission-critical and mission important applications as well as administrative and minor applications. Audit fieldwork was conducted at EAC's headquarters in Silver Spring, Maryland from June 9, 2017, to October 13, 2017.

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 47 of 60 security controls selected for testing for the information systems tested. Although EAC generally had policies for its information security program, its implementation of those policies was not fully effective to preserve the confidentiality, integrity, and availability of EAC'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

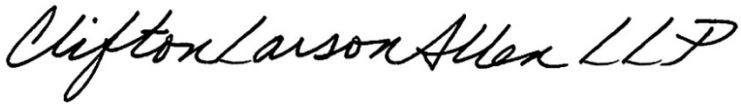
[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

information security program that need to be improved. We are making 11 recommendations to assist EAC in strengthening its information security program.

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 EAC and appreciate the opportunity to serve you. We will be pleased to discuss any questions or concerns you may have regarding the contents of this report.

Very truly yours,



CLIFTONLARSONALLEN LLP

Table of Contents

Summary of Results

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

The act also requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) a security incident response capability is 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 Office of Management and Budget 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 Office of Inspector General (OIG) engaged us, CliftonLarsonAllen LLP (CLA), 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 selected 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 EAC's general support system (GSS), the Enterprise Network. The GSS is the framework network architecture that supports network security, Internet, and e-mail access.

Results

The audit concluded that EAC generally complied with FISMA requirements by implementing 47 of the 60 security controls reviewed[2] for the selected information system. For example, EAC:

- Developed a security assessment plan which captures NIST Special Publication 800-53 controls, provides a mechanism for ongoing security control assessments, and incorporates the tracking and remediation of noted weaknesses.

- Deployed security tools to assist with vulnerability and configuration management processes.

- Reduced the volume of critical and high risk vulnerabilities from the prior year.

[2] See Appendix III – Summary of Results of Each Control Reviewed.

- Hired a Certified Authorization Professional (CAP) to provide management consulting services on FISMA compliance and Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM).

- Executed a successful succession and transition plan for the Chief Information Officer (CIO) position to appoint an Acting CIO from within the agency.

Although EAC generally had policies and procedures for its information security program, the implementation of those policies for 47 of 60 selected security controls was not fully effective to preserve the confidentiality, integrity, and availability of EAC's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, the audit identified several areas in EAC's information security program that needed to be improved. Specifically EAC needs to:

- Enforce Personal Identity Verification (PIV) Cards for local network authentication.

- Maintain active interconnection agreements.

- Maintain and review assessment and authorization packages.

- Mitigate network vulnerabilities to strengthen controls over vulnerability management.

- Strengthen controls surrounding audit logging and monitoring.

- Improve procedures for third party contractor system oversight.

- Update and test continuity plans.

- Strengthen management of plans of actions and milestones (POA&Ms).

Consequently, EAC's operations and assets are at risk of unauthorized access, misuse and disruption. We have made 11 recommendations (including two recommendations repeated from FY 2016) to assist EAC in strengthening its information security program.

Detailed findings appear in the following section. Appendix I describes the audit scope and methodology.

Audit Findings

1. EAC Needs to Enforce Personal Identity Verification (PIV) Cards for Local Network Authentication

National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* the following regarding identification and authentication:

The organization:

(12) "Identification and Authentication | Acceptance of PIV Credentials"
The information system accepts and electronically verifies PIV credentials. PIV credentials are those credentials issued by federal agencies that conform to NIST Federal Information Processing Standard (FIPS) 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in Homeland Security Presidential Directive (HSPD) 12 to enable agency-wide use of PIV credentials.

EAC did not implement multifactor authentication for local and network access for privileged user accounts and for network access for non-privileged accounts. Currently, multifactor authentication was only implemented for remote access to the network.

EAC's organizational implementation plan for enforcing PIV card architecture remains in progress. EAC is undergoing discussion with General Services Administration (GSA) to identify a formal timeline.

Without multifactor authentication for local and network access for privileged user accounts, there is an increased risk of unauthorized access by an unauthorized user. Unauthorized privileged access can allow an individual to inappropriately create, delete and modify users and services running on the network as well as gain access to all data stored on the network. In addition, without multifactor authentication for network access for non-privileged user accounts, there is increased risk of unauthorized access to EAC information and information systems by an unauthorized user decreasing the confidentiality and integrity of data.

Recommendation 1: *We recommend that Acting Chief Information Officer 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 GSA. (New)*

Management Response: The EAC has been working with GSA for an extended period to attempt to enable PIV Cards for this purpose. It is hoped that this work will lead to successful implementation within the next three months, but the EAC has a significant dependency upon GSA for timely completion of this effort. Once implemented, the EAC will be able to ensure that all employees and contractors are required to use their PIV cards when accessing agency networks and data.

CLA Evaluation of Response: We encourage EAC to continue working with GSA and making additional progress in FY 2018 towards implementation of corrective actions.

2. EAC Should Enhance Current Documentation Regarding Interconnections

NIST SP 800-53, Revision 4, security control AC-20, states the following regarding the use of external information systems:

The organization:

Establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating and/or maintaining external information systems, allowing authorized individuals to:

a) Access the information system from external information systems; and
b) Process, store, or transmit organization-controlled information using external information systems.

In addition, security control CA-3, states the following in regards to the use of system interconnections:

The organization:

a) Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
b) Documents, for each interconnection, the interface characteristics, security requirements and the nature of the information communicated; and
c) Reviews and updates Interconnection Security Agreements [*Assignment: organization-defined frequency*].

Interconnection documentation such as the Memorandum of Understanding (MOU) between GSA and EAC expired September 30, 2016 and therefore is not currently in effect. EAC did not ensure they were under a current interconnection agreement. Upon notification of this issue, EAC management contacted GSA to renew the interconnection documentation. The renewed interconnection agreement was provided however the approval date of September 14, 2017 was at the latter part of the performance period ending September 30, 2017. Thus, this agreement was only in effect for the last two weeks of the fiscal year.

By maintaining system interconnections with out-of-date agreements covering processing, storage, security and data transmission controls from GSA to EAC systems, there is an increased risk that responsibilities for these controls could be misconstrued and/or inadequately implemented.

Recommendation 2: *We recommend that EAC management refine their process to renew interconnection documentation and monitor renewal timeframes going forward. (New)*

Management Response: EAC is currently working with GSA to resolve this deficiency. GSA, by federal law, is required to support the EAC, upon the request of the Commission (Help America Vote Act, Section 205(d), regardless of the signature status of a Memorandum of Understanding. While we agree that GSA's documentation should be

current, this appears to be an observation more pertinent to GSA, not the EAC. Part of the support GSA must provide is the specific documentation as it relates to the interconnections. The EAC cannot compel GSA to enhance its current documentation regarding interconnections with the EAC, but the EAC will use this finding to escalate discussions with GSA leadership.

CLA Evaluation of Response: We encourage EAC to continue working with GSA and making additional progress in FY 2018 towards implementation of corrective actions.

3. EAC Needs to Finalize their Security Assessment and Authorization Packages and Ensure Timely Renewal

NIST SP 800-53, Revision 4, security control CA-6, states the following regarding security authorization:

The organization:

a) Assigns a senior-level executive or manager as the authorizing official for an information system;
b) Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
c) Updates the security authorization [*Assignment: organization-defined frequency*].

OMB Memorandum A-130, *Responsibilities for Protecting and Managing Federal Information Resources,* states the following:

4) Specific Requirements;
d. Authorization to Operate and Continuous Monitoring

Agencies shall:
1) Designate senior Federal officials to formally authorize an information system to operate and authorize agency-designated common controls for use;
2) Complete an initial authorization to operate for each information system and all agency-designated common controls based on a determination of, and explicit acceptance of, the risk to agency operations and assets, individuals, other organizations, and the Nation, and prior to operational status;
3) Transition information systems and common controls to an ongoing authorization process when eligible for such a process and with the formal approval of the respective authorizing officials;
4) Reauthorize information systems and common controls as needed, on a time- or event-driven basis in accordance with agency risk tolerance;
5) Develop and maintain an ISCM strategy to address information security risks and requirements across the organizational risk management tiers;
6) Implement and update, in accordance with organization-defined frequency, the ISCM strategy to reflect the effectiveness of deployed controls; significant changes to information systems; and adherence to Federal statutes, policies, directives, instructions, regulations, standards, and guidelines;

7) Ensure that all selected and implemented controls are addressed in the ISCM strategy and are effectively monitored on an ongoing basis, as determined by the agency's ISCM program; and
8) Establish and maintain an ISCM program.

The GSA Enterprise Network Services (ENS) Authorization to Operate (ATO) which encompasses the subnet of the GSA Wide Area Network (WAN) where EAC's Local Area Network (LAN) resides expired in March 2016. Although a new ATO was issued by GSA on August 21, 2017, there was a significant portion of the fiscal year (October 2016 – August 2017) in which EAC's LAN was not operating under an ATO.

EAC did not ensure they were under a current ATO with GSA, upon expiration of the previous authorization decision.

Without EAC information systems authorized to operate, the Authorizing Official (AO) cannot be held accountable for accepting the risk to operate these systems. Further, the security posture of EAC systems may not be at an acceptable level of risk to operate, and the agency may be exposed to unmitigated security risk, potentially compromising EAC's information or information systems.

Recommendation 3: *We recommend that EAC management, in coordination with GSA, ensure current and signed ATOs are issued for ENS which do not create any gaps in coverage. (New)*

Management Response: Similar to the previous two Audit Findings, the EAC believes this pertains more to GSA, not the EAC. However, separate from the ATO agreement issue related to this finding, the EAC has taken separate action to contract with an industry and FISMA expert to conduct an independent effort to complete all SA&A documentation by December 31, 2017.

CLA Evaluation of Response: We encourage EAC to continue working with GSA and making additional progress in FY 2018 towards implementation of corrective actions.

4. EAC Needs to Further Strengthen Controls Over Vulnerability Management

NIST Special Publication 800-53, Revision 4, states the following regarding vulnerability management:

CM-6 "Configuration Settings" states that the organization:

a) Establishes and documents configuration settings for information technology products employed within the information system using [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 deviation from established configuration settings for [organization-defined information system components] based on [organization-defined operational requirements]; and

d) Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

SI-2 “Flaw Remediation” states that 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 [Assignment: organization-defined time period] of the release of the updates; and
d) Incorporates flaw remediation into the organizational configuration management process.

SA-22 “Unsupported System Components” states that the organization:

Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

Support for information system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components (e.g., when vendors are no longer providing critical software patches), provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

As a result of our testing, we noted that EAC was not in compliance with the United States Government Configuration Baseline (USGCB) standards. Specifically, the independent scans performed indicated an average compliance level of 43%. USGCB defines secure baselines for government furnished workstations. Deviations from recommended settings could affect controls over the confidentiality, integrity, and availability of data.

Based on independent non-credential scans of the EAC network and credentialed scan of Windows servers, we identified instances of critical and high risk vulnerabilities in the areas of unsupported systems and patch management.

Unsupported systems may be susceptible to older vulnerabilities and exploits which vendors have addressed with current supported versions. Vulnerabilities may exist on unsupported systems that cannot be detected due to lack to vendor support and notification. Unmitigated vulnerabilities on the EAC network can compromise the confidentiality, integrity, and availability of information on the network. For example:

- An attacker may leverage known vulnerabilities to execute arbitrary code.
- EAC Systems may not be accessible by authorized personnel.
- EAC data may be lost, stolen, or compromised.

Although EAC's configuration management process was not effective in remediating system configuration vulnerabilities, EAC has taken steps to implement network scanning and remediation of vulnerabilities through the gradual deployment of Department of Homeland Security (DHS) Continuous Diagnostics and Monitoring (CDM) tools in concert with existing in-house and GSA contracted information security architecture.

By not implementing stronger configuring security settings and remediating patch vulnerabilities in a timely manner this could enable an attacker to exploit a vulnerability to read, modify, and/or delete financial and sensitive information, disrupt operations, or launch attacks against other systems at EAC. In addition, unsupported or outdated versions of software allow EAC systems to remain exposed to known high risk vulnerabilities for an extended period of time.

Recommendation 4: *We recommend that the Acting Chief Information Officer implement corrective actions to resolve critical and high risk vulnerabilities identified related to patching, software upgrades and configuration weaknesses for those systems identified within the detailed scanning results. (Repeat Modified)*

Recommendation 5: *We recommend that the Acting Chief Information Officer implement a process to scan 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 CDM. (New)*

Recommendation 6: *We recommend that the Acting Chief Information Officer document any deviations from the USGCB baseline (e.g. GSA gold image) to include business justifications for each deviation. (New)*

Management Response: EAC has contracted with an industry and FISMA expert to aid in the development of many policies and procedures, including the management of configuration settings. This agency has not developed in-house applications so we believe there are no real configuration management changes or flaws. ("Flaws" are identified when software is not working as intended and users alert IT of those flaws, whereby they are then remediated via a formal change management process. Because none of the software in the EAC environment was developed in-house, flaws, by definition, don't exist in the EAC environment).

However, the EAC does recognize that our scans results need to be remediated more timely. As it relates to the USGCB compliance checks, the EAC has upgraded and deployed its patch management utility and is currently tweaking the utility based on the amount of false positive results. Within the next two months, the EAC will ensure our software is in compliance with those requirements. Lastly, we are also in the process of upgrading our servers and Active Directory policies, which will remediate the small number of actual deficiencies.

The EAC expects that all of our SA&A documentation will be completed by the end of December 31, 2017 which will include documented business justification of any deviation from USGCB configuration.

CLA Evaluation of Response: Although management indicated that "flaws" were not applicable since EAC does not utilize in-house developed software, the "flaw" criteria stated in the finding also relates to the timely installation of patches as part of the

vulnerability management process. We encourage EAC to continue making additional progress in FY 2018 towards implementation of corrective actions.

5. EAC Should Strengthen its Audit Log Review Process

NIST SP 800-53, Revision 4, security control AU-6, states the following regarding audit review, analysis and reporting:

The organization:

a) Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity].

Although EAC had a contract with GSA to monitor firewall logs for viruses and malicious traffic, and had developed an audit and monitoring policy, this policy was not formally reviewed and revised since 2014. The contract with GSA did not outline the frequency of audit log reviews or responsibilities around monitoring activities specific to EAC. Although various audit logs collected are manually reviewed on an ad hoc basis it's dependent on the availability of personnel tasked with balancing diverse roles.

Thus, given the lack of defined audit frequency and responsibilities as part of a formal process to review audit logs, there is an increased potential of security incidents and security breaches to occur undetected.

Recommendation 7: *We recommend that Acting Chief Information Officer revise and implement the EAC-CIO-2010-009 Auditing and Monitoring SOP to outline the frequency of audit log reviews and responsibilities around all monitoring activities*. *(Modified Repeat)*

Management Response: All of our audit events have been reviewed, and EAC has selected which audit events will be generated monthly--those events are already being reviewed on a monthly basis.

CLA Evaluation of Response: Management needs to continue maturing their audit log review process as part of their information security continuous monitoring program, and making additional progress in FY 2018 towards implementation of corrective actions.

6. Policies and Procedures Regarding Third Party Systems Could be Improved

NIST SP 800-53, Revision 4, security control AC-20, states the following regarding external information systems:

The organization:

(1) Use of External Information Systems | Limits on Authorized Use" states that the organization permits authorized individuals to use an external information system to access the information or to process, store, or transmit organization-controlled information only when the organization:

a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

EAC has not defined and maintained a formalized procedure requiring the regular review of independent assessments, such as Service Organization Control (SOC) reports, to gain reasonable assurance that external, third party managed information system's internal controls are appropriately designed and operating effectively.

Currently, SOC reports are reviewed by EAC management without formally documenting the results of the review.

Without the review of SOC reports, complementary user entity controls (CUECs) that may be relevant to EAC may not be documented and implemented in order for the service provider's controls to operate as intended. In addition, risks from exceptions noted in the report may impact EAC's environment requiring contemplation, documentation and/or implementation of mitigating factors.

Recommendation 8: *We recommend that the EAC management document and implement a formal procedure for documenting the review of SOC reports for applicable third party systems at a defined frequency. (New)*

Management Response: EAC has already contracted with an external service provider and we are expecting that all of our SA&A documentation will be completed by the end of December 31, 2017. This includes policies regarding third party systems.

CLA Evaluation of Response: We encourage EAC to continue making additional progress in FY 2018 towards implementation of corrective actions.

7. EAC Needs to Update and Test Contingency Plans

NIST SP 800-53, Revision 4, security control CP-1, states the following regarding contingency planning and procedures:

The organization:
b) Reviews and update the current:
   1. Contingency planning policy [*Assignment: organization-defined frequency*].

In addition, security control CP-2, states the following regarding contingency planning:

The organization

(3) Plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation. Organizations may choose to carry out this control enhancement through business impact analyses.

(8) Identifies critical information system assets supporting essential missions and business functions. Organizations may choose to carry out this control enhancement through business impact analyses. Refer to NIST SP 800-34 *Contingency Planning Guide for Federal Information Systems* for more on business impact analyses.

Further, security control CP-4, states the following regarding contingency plan testing:

The organization:
a) Tests the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests*] to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b) Reviews the contingency plan test results; and
c) Initiates corrective actions, if needed.

EAC-CIO-2010-027 *COOP* Section K, states the following regarding Test, Training and Exercise (TT&E):

This continuity plan will be tested at least annually. The functions to be tested include:
- The ability to perform agency essential functions remotely.
- The internal and external interoperability of the communication systems, including both secure and unsecured systems (monthly).
- The telephone tree, the staff alert and notification procedures and Emergency Communications (quarterly).

The EAC *Continuity of Operations Plan (COOP)* was not reviewed and updated within the last 12 months. In addition, the supporting business impact analysis (BIA) was not updated and/or performed within the last 12 months. Further, the COOP was not tested during FY 2017. The contingency planning strategy was in the process of being refined in partnership with GSA and Iron Mountain.

If essential missions, key business functions and critical assets are not identified and prioritized on the basis of risk, with recovery time objective and recovery point objectives defined the COOP supporting a business impact analysis may become stale and inaccurate over time. Plan effectiveness and organizational readiness to execute the plan cannot be completely and accurately established without testing the plan.

Recommendation 9: *We recommend the Acting Chief Information Officer reviews and updates the COOP at least annually. We also recommend that EAC management review the business impact analysis supporting the COOP for accuracy semi-annually in alignment with the existing IT inventory checks. (New)*

Recommendation 10: *We recommend that Acting Chief Information Officer 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. (New)*

Management Response: The EAC tested contingencies in 2017, but agrees that the plans should be updated and even more structure can be applied. The EAC already has contracted with an industry and FISMA expert in this regard and we are expecting that all

of our SA&A documentation will be completed by the end of December 31, 2017. This includes policies regarding contingencies.

CLA Evaluation of Response: No documentation was provided to substantiate contingency plan testing performed during FY 2017. Contingency plan testing should be conducted on an annual basis. We encourage EAC to continue making additional progress in FY 2018 towards implementation of corrective actions.

8. EAC Needs to Strengthen its Management of Plans of Action and Milestones (POA&Ms)

NIST SP 800-53, Revision 4, security control CA-5, states the following regarding plans of action and milestones:

The organization:

a) Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b) Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

EAC-CIO-2010-001 *IT Security Plan,* Section 13.2f of Risk Management, states the following:

POA&Ms are the authoritative agency management tool for managing system risk and used in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in agency programs and systems.

In addition, Section 13.10 Plan of Action and Milestones (POA&Ms), states the following:

Capture all information security program and system weaknesses that require mitigation in the POA&M. POA&Ms shall be updated quarterly.

POA&Ms were not effectively managed and reviewed on a quarterly basis in accordance with EAC policy. Specifically, we noted the following:

- One of five POA&Ms was past its expected completion date.
- Two of five POA&Ms did not have item numbers and start dates and were past their expected completion dates.
- One of five POA&Ms did not have an item number, start date, expected completion date and a course of action.
- One of five POA&Ms did not have an item number, status notes, assignment, start date, designated level of risk, expected completion date and a course of action.

Policies and procedures regarding plans of actions and milestones were not formally reviewed and revised since 2014. The remediation and tracking of POA&Ms identified by EAC is performed on an ad hoc basis and depends on availability of personnel tasked with balancing diverse roles.

POA&Ms are used by the AO to evaluate corrective action plans and estimated timeframes for remediation of control weaknesses, and to monitor the progress of remediation. Without current and complete information within POAMs, plans for corrective action could be delayed, leaving EAC susceptible to system security risks.

Recommendation 11: *We recommend that the Acting Chief Information Officer update the POA&M report to cover all information from required fields and to benchmark the state of corrective action and identify next steps. We also recommend that the Acting Chief Information Officer maintain and review POA&Ms in line with the frequency defined by EAC policy. We further recommend that Acting Chief Information Officer ensure all known control weaknesses are documented in the POA&Ms. (New)*

Management Response: EAC has already contracted with an external service provider and we are expecting that all of our SA&A documentation will be completed by the end of December 31, 2017. This includes all policies related to the SA&A activities. Once the SA&A is finalized with an authorization to operate (ATO), the controls will be assessed and any deficiencies will be documented as a POA&M.

CLA Evaluation of Response: We encourage EAC to continue making additional progress in FY 2018 towards implementation of corrective actions.

Appendix I

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 certain security controls for selected information systems in support of FISMA.

The audit included the testing of certain management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* We assessed EAC's performance and compliance with FISMA in the following areas:

- Access Controls
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Media Handling
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Information Integrity
- System and Services Acquisition

For this audit, we reviewed the EAC network general support system. See Appendix V for a listing of selected controls. The audit also included a vulnerability assessment of EAC's general support system and evaluation of EAC's process for identifying and correcting/mitigating technical vulnerabilities. In addition, the audit included a follow up on prior year audit recommendations (Refer to Appendix IV) to determine if EAC made progress in implementing any recommended improvements in EAC's vulnerability management program.

The audit was conducted at EAC's headquarters in Silver Spring, Maryland from June 9, 2017, to October 12, 2017.

Methodology

To determine if EAC's information security program met FISMA requirements, we conducted interviews with EAC officials and contractors and reviewed legal and regulatory requirements

stipulated in FISMA. We also reviewed documents supporting the information security program. These documents included, but were not limited to, EAC's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) patch management procedures; and (5) change control documentation. Where appropriate, we compared documents, such as EAC's information technology policies and procedures, to requirements stipulated in NIST special publications. In addition, we performed tests of system processes to determine the adequacy and effectiveness of those controls and completed a vulnerability assessment of the EAC network.

In testing for the adequacy and effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk, and the significance or criticality of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review. In some cases, this resulted in selecting the entire population. However in cases that we did not select the entire audit population, the results cannot be projected, and if projected, may be misleading.

Appendix II

Status of Prior Year Findings

The following table provides the status of the FY 2016 FISMA audit recommendations.

No.	FY 2016 Audit Recommendation	EAC Status	Auditor's Position on Status
1	EAC management implement corrective actions to resolve critical and high risk weaknesses identified related to patching, software upgrades, and configuration weaknesses for those systems identified within the detailed scanning results provided by CLA, and implement a process to scan on a regular basis and remediate weaknesses noted from those scans.	In Progress	Open and repeated in FY 2017, Finding #1
2	EAC management document and implement a formalized standard operating procedure to review audit logs.	In Progress	Open and repeated in FY 2017, Finding #2

Appendix I

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 certain security controls for selected information systems in support of FISMA.

The audit included the testing of certain management, technical, and operational controls outlined in National Institute of Standards and Technology Special Publication NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* We assessed EAC's performance and compliance with FISMA in the following areas:

- Access Controls
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Media Handling
- Program Management
- Risk Assessment
- Security Assessment and Authorization
- System and Information Integrity
- System and Services Acquisition

For this audit, we reviewed the EAC network general support system. See Appendix V for a listing of selected controls. The audit also included a vulnerability assessment of EAC's general support system and evaluation of EAC's process for identifying and correcting/mitigating technical vulnerabilities. In addition, the audit included a follow up on prior year audit recommendations (Refer to Appendix IV) to determine if EAC made progress in implementing any recommended improvements in EAC's vulnerability management program.

The audit was conducted at EAC's headquarters in Silver Spring, Maryland from June 9, 2017, to October 12, 2017.

Methodology

To determine if EAC's information security program met FISMA requirements, we conducted interviews with EAC officials and contractors and reviewed legal and regulatory requirements

ELECTION ASSISTANCE COMMISSION

FY 2017 FISMA EVALUATION

Appendix III

Control No.	Control Name	Is Control Effective?
CP-6	Alternate Storage Sites	Yes
CP-7	Alternate Processing Sites	Yes
CP-9	Information System Backup	Yes
CP-10	Information System Recovery & Reconstitution	Yes
IA-1	Identification and Authentication Policy and Procedures	Yes
IA-2	Identification and Authentication (Organizational Users)	Not Effective, See Finding 3
IA-3	Device Identification and Authentication	Yes
IA-5	Authenticator Management	Yes
IR-1	Incident Response Policy and Procedures	Yes
IR-4	Incident Handling	Yes
IR-5	Incident Monitoring	Yes
IR-6	Incident Reporting	Yes
IR-8	Incident Response Plan	Yes
MP-1	Media Protection Policy and Procedures	Yes
MP-2	Media Access	Yes
MP-4	Media Storage	Yes
MP-5	Media Transport	Yes
MP-6	Media Sanitization	Yes
RA-1	Risk Assessment Policy and Procedures	Yes
RA-2	Security Categorization	Yes
RA-3	Risk Assessment	Yes
RA-5	Vulnerability Scanning	Not Effective, See Finding 1
SA-9	External Information Systems	Not Effective, See Finding 6
SC-7	Boundary Protection	Yes
SI-2	Flaw Remediation	Not Effective, See Finding 1
PM-1	Information Security Program Plan	Yes
PM-3	Information Security Resources	Yes
PM-4	Plan of Action and Milestones Process	Yes
PM-5	Information System Inventory	Yes
PM-9	Risk Management Strategy	Yes
PM-10	Security Authorization Process	Yes

Appendix IV

Management Comments

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

Memorandum

Date: November 6, 2017

To: Patricia Layfield, Inspector General

From: Brian D. Newby, Executive Director BDN

Re: Response to Draft Audit Report—US Election Assistance Commission Compliance with the Requirements of the Federal Information Security Management Act Fiscal Year 2017

The Election Assistance Commission (EAC) is pleased that the FY2017 FISMA audit concluded that EAC has generally complied with FISMA requirements. In the summary audit report, the auditors evaluated the effectiveness of EAC's information security program and practices, as well as compliance with the FISMA and related information security policies, procedures, standards and guidelines. As the draft report reflects, EAC generally had sound controls for its information security program in place.

We were further gratified to see that the auditors noted the progress made since the Fiscal Year 2016 audit, and feel compelled to stress that the EAC is less vulnerable to security threats than a year ago. Even since the summary audit report was drafted, the EAC is even more secure, based on activities completed and underway.

Despite extremely modest resources, the EAC aspires to be a model agency in terms of information security compliance. Therefore, the EAC takes seriously all of the items mentioned, and generally agrees with the findings.

However, as noted in the response that follows, several of these items pertain, in our view, more to the General Services Administration (GSA) than to the EAC.

GSA supports many agencies, and the EAC is one of the smaller agencies GSA supports. GSA supports the EAC pursuant to Section 205 (d) of the Help America Vote Act:

> *"Upon the request of the Commission, the Administrator of General Services shall provide to the Commission, on a reimbursable basis, the administrative support services that are necessary to enable the Commission to carry out its duties under this Act."*

The EAC attempts to work closely with GSA. The EAC definitely could benefit from more urgency from GSA, but EAC cannot compel GSA in this regard. Perhaps this audit report will allow the EAC to better broach the need for GSA urgency with GSA's senior leaders, but, in the end, some of the items reported simply pertain more to GSA than the EAC.

Further, the EAC utilizes GSA for software builds, imaging, and patching. The EAC is very diligent with system scans to identify outdated programs or missing software patches. The current FISMA audit recognizes the EAC's progress in this regard, somewhat, but leaves the impression that much work remains. This is not the case. EAC noted several false positives in the scanning efforts and worked to communicate this with the audit team. The finding that the report "identified instances of critical and high risk vulnerabilities in the area of unsupported systems and patch management," implies a much more significant issue than that which exists. During last year's FISMA audit process, the EAC began

Telephone: 301-563 – 3959 bnewby@eac.gov

formalizing a process to scan and remediate vulnerabilities; in fact, the EAC found that nearly all instances identified by the auditors in 2017 were false positives which involved patches that actually had been applied, items that were part of the GSA image loads, or items in out-of-production servers that are in the process of being replaced.

The EAC understands that the need to secure information technology requires continued focus, and the EAC is vigilantly upgrading its FISMA status and processes so that all potential indicators, rather than just the smaller audit sample, will demonstrate compliance with the expectations of the FISMA standards.

Thus, EAC's information security represents much more of a good news story than in previous years, and we expect the IT environment to be even more secure in the coming months. The audit actually confirms this, but some word choices, along with the GSA items, could portray a different picture upon first glance.

Thank you for you for giving us the opportunity to provide feedback on the audit recommendations.

Copy to: Henry Botchway, Acting Interim CIO
Cliff Tatum, General Counsel
Annette Lafferty, CFO

Telephone: 301-563 - 3959 bnewby@eac.gov

Appendix V

Evaluation of Management Comments

We agree that EAC has undertaken remediation efforts during FY 2017 to strengthen internal controls over its information security program with emphasis on vulnerability management.

We encourage EAC to continue working to address findings through consideration and implementation of recommendations noted within the report, to include coordination with GSA as needed.

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 detect and prevent 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 can be requested by e-mail. (eacoig@eac.gov)

Mail orders should be sent to:

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

Phone: 301-734-3105
Fax: 301-734-3115

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

By 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