U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL

FINAL REPORT:

U.S. Election Assistance Commission

Compliance with the Requirements of the Federal Information Security Management Act

Fiscal Year 2016

NO. I-PA-EAC-02-16
NOVEMBER 2016

U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL
1335 East West Highway - Suite 4300
Silver Spring, MD 20910

Memorandum

November 10, 2016

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

From: Patricia Layfield
Inspector General

Subject: Final Report - Fiscal Year 2016 U.S. Election Assistance Commission Compliance with the Requirements of the Federal Information Security Modernization Act (Assignment No. I-PA-EAC-02-16)

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 and related information security policies, procedures, standards, and guidelines (Attachment). 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.

CLA found that EAC generally complied with FISMA requirements by implementing 56 of 60 security controls selected for testing. 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. As a result, EAC's systems could be exposed to unauthorized access, use, disclosure, disruption, modification, or destruction.

CLA made two recommendations for improvement:

1. CLA recommended that 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 CLA's detailed scanning results and implement a process to scan on a regular basis and remediate weaknesses noted from those scans.

EAC responded that they agreed with the recommendation and had already begun implementing corrective actions to resolve critical and high risk weaknesses identified related to patching, software upgrades, and configuration weaknesses. The agency was also in the process of reimaging the workstations to GSA's gold image and had implemented automated vulnerability scanning and a remediation schedule that is discussed in a new draft procedure for patch management.

2. CLA recommended that EAC management document and implement a formalized standard operating procedure to review audit logs. EAC responded that they had already started documenting better the processes to scan on a regular basis as well as remediating weaknesses noted from the scans. The agency had also purchased new tools to automate the collection of log data and included information on reviewing and documenting all logs in its new draft standard operating procedure.

The audit was conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. CLA is responsible for the final audit report and the conclusions expressed in the report. The OIG performed the procedures necessary to obtain a reasonable assurance about CLA's independence, objectivity, qualifications, and technical approach.

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit reports issued, actions taken to implement our recommendations, and recommendations that have not been implemented. Therefore, we will include the information in the attached audit report in our next semiannual report to Congress.

If you have any questions regarding this report, please call me at (301) 734-3104.

cc: Commissioner Matthew Masterson, 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 2016

Final Report

CliftonLarsonAllen LLP
www.claconnect.com

November 9, 2016

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 final report of the *Audit of the Election Assistance Commission's Fiscal Year 2016 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, MD, from July 07, 2016 to October 5, 2016.

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 56 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,

[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.

disclosure, disruption, modification, or destruction. Consequently, the audit identified areas in EAC's information security program that need to be improved. We are making two 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 the staff of EAC and value the opportunity to serve you and will be pleased to discuss any questions you may have.

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 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 are mandatory for Federal agencies.

The EAC Office of Inspector General 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 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.

For this audit, we reviewed EAC's general support system (GSS). 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 56 of 60 selected security controls, for selected information systems, however we did note weaknesses in the following areas:

- Mitigating network vulnerabilities
- Implementing controls surrounding audit logging and monitoring

The report makes two recommendations 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 Improve Controls Over Vulnerability Management.

As a result of our internal non-credentialed vulnerability scanning of the EAC network, we identified 355 instances of critical and high risk vulnerabilities in the areas of configuration weaknesses, unsupported systems, and patch management. Specifically, we identified:

- 243 (68% of total critical and high risk vulnerabilities) instances of missing or outdated software patches.
- 63 (18% of total critical and high risk vulnerabilities) instances of configuration weaknesses.
- 49 (14% of total critical and high risk vulnerabilities) instances of unsupported software.
- United States Government Configuration Baseline (USGCB) compliance was 43% after failing an average of 150 out of 263 security checks. USGCB defines secure baselines for government furnished workstations. Deviances from recommended settings could affect controls over the confidentiality, integrity, and availability of data.

EAC's configuration management process was not effective in remediating system configuration vulnerabilities.

Management indicated the EAC has undergone several leadership changes in 2016, ranging from the introduction of a new Executive Director and General Counsel, to the departure of the agency's Chief Operating Officer (COO), and very importantly, its' Chief Information Officer (CIO). From the time the former CIO left (in July 2016), two months before the FISMA scanning took place (in September 2016), the remaining IT staff worked to identify and mitigate vulnerabilities. As part of the mitigation plan, the EAC obtained an individual detailed from GSA to assist with FISMA compliance, and procured professional services to assist with addressing flaws in remediating vulnerabilities. In addition, EAC has taken steps to implement network scanning and remediation of vulnerabilities.

According to the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4*, Security and Privacy Controls for Federal Information Systems and Organizations,* security controls:

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.

RA-5 “Vulnerability Management” states that the organization:

a) Scans for vulnerabilities in the information system and hosted applications [organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b) Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
   1. Enumerating platforms, software flaws, and improper configurations;
   2. Formatting checklists and test procedures; and
   3. Measuring vulnerability impact;
c) Analyzes vulnerability scan reports and results from security control assessments;
d) Remediates legitimate vulnerabilities [organization-defined response times] in accordance with an organizational assessment of risk; and
e) Shares information obtained from the vulnerability scanning process and security control assessments with [organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

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.

Office of Management and Budget (OMB) Memorandum A-130 - Appendix I to OMB Circular A-130 Responsibilities for Protecting and Managing Federal Information Resources states the following:

- i. Specific Safeguarding Measures to Reinforce the Protection of Federal Information and Information Systems, Agencies shall:

9) Implement and maintain current updates and patches for all software and firmware components of information systems;

- p. Unsupported Information System Components

  Unsupported information system components (e.g., when developers or vendors are no longer providing critical software patches) provide a substantial opportunity for adversaries to exploit weaknesses discovered in the currently installed components. Prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission or business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option. For such systems, agencies can establish in-house support, for example, by developing customized patches for critical software components or securing the services of external providers who through contractual relationships, provide ongoing support for the designated unsupported components. Such contractual relationships can include, for example, open source software value-added vendors.

Failing to appropriately configure security settings and timely patch vulnerabilities may 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 1: We recommend that 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.

2. The Process To Review Audit Logs Needs Strengthening.

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 document did not outline the frequency of audit log reviews or responsibilities around monitoring activities specific to EAC. There was also no formalized standard operating procedure or ongoing process in place to review audit logs.

In addition, although EAC logged user actions on the network upon login success and login failure, failure to access an object, and successful and unsuccessful policies changes, evidence of audit log reviews were not documented to demonstrate these reviews were occurring as indicated.

Without a formal process to review audit logs, there is an increased potential of security incidents and security breaches occurring undetected.

According to the NIST SP 800-53, Revision 4, security controls:

AU-6 “Audit Review, Analysis and Reporting” states that the organization:

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

Recommendation 2: We recommend that EAC management document and implement a formalized standard operating procedure to review audit logs

Scope and Methodology

Scope

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

The audit included the testing of selected 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 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 July 07, 2016, to October 5, 2016.

Methodology

Following the framework for minimum security controls in National Institute of Standards and Technology Special Publication (NIST) SP 800-53, Revision 4, certain controls (listed in Appendix V) were selected from the NIST security control families. We reviewed the selected controls over EAC's General Support System.

To accomplish our audit objective we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA.
- Reviewed documentation related to EAC's information security program, such as security policies and procedures, system security plans, and risk assessments.
- Tested system processes to determine the adequacy and effectiveness of selected controls (listed in Appendix V).
- Reviewed the status of recommendations in the fiscal year 2015 FISMA audit report.
- Completed a network vulnerability assessment of EAC's general support system.

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.

Management Comments

OFFICE OF THE EXECUTIVE DIRECTOR
1335 East West Highway – Suite 4300
Silver Spring, MD 20910

Memorandum

October 31, 2016

To: Patricia Layfield
Inspector General

From: Brian D. Newby
Executive Director

Re: Response to Draft Audit Report – U.S. Election Assistance Commission Compliance with the Requirements of the Federal Information Security Management Act Fiscal Year 2016 (Assignment No. I-PA-EAC-02-16)

The Election Assistance Commission (EAC) is pleased that the FY 2016 audit concluded that EAC has generally complied with FISMA requirements. On the summary audit report, the auditors evaluated the effectiveness of EAC's information security program and practices, as well as compliance with 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. Management generally agrees with the two recommendations provided by the auditors.

Regarding the recommendation to improve controls over vulnerability management, management agrees, but notes that the EAC is already implementing corrective actions to resolve critical and high risk weaknesses identified related to patching, software upgrades and configuration weaknesses. All EAC workstations are being reimaged with the General Services Administration's (GSA's) gold image. All software in the GSA gold image has been tested for the EAC's network and includes current versions of software. For software not found in the gold image, the EAC has purchased the latest versions. In addition, the EAC has already implemented an automated vulnerably scanning and remediation schedule that is in a new draft Standard Operating Procedure (SOP) for patch management.

Regarding strengthening the audit log process, the EAC is already better documenting processes to scan on a regular basis, as well as remediating weaknesses noted from those scans. The EAC has purchased new tools to automate the collection of log data. The new draft SOP includes information on how the EAC reviews and documents all logs.

The EAC is pleased to share that no security incidents were reported for FY 2016.

Thank you for giving me the opportunity to provide feedback on these recommendations.

Copy to: Henry Botchway, Acting Interim CIO
Annette Lafferty, CFO

Evaluation of Management Comments

In response to the draft report, EAC outlined its plans to address both recommendations. EAC's comments are included in their entirely in Appendix II.

Based upon our evaluation of management comments, we acknowledge that management agrees with both recommendations.

Status of Prior Year Findings

The following table provides the status of the FY 2015 FISMA audit recommendations.

No.	FY 2015 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 and software upgrades for those systems identified with the detailed scanning results provided by CLA.	In Progress	Open and repeated in FY2016
2	EAC management work with GSA to ensure EAC's internal network is properly segmented from GSA.	Closed	Closed

Summary of Results of each Control Reviewed

Control	Control Name	Is Control Effective?
EAC Network		
AC-1	Access Control Policy & Procedures	Yes
AC-2	Account Management	Yes
AC-3	Access Enforcement	Yes
AC-5	Separation of Duties	Yes
AC-6	Least Privilege	Yes
AC-7	Unsuccessful Logon Attempts	Yes
AC-11	Session Lock	Yes
AC-17	Remote Access	Yes
AC-18	Wireless Access	Yes
AC-19	Access Control for Mobile Devices	Yes
AC-20	Use of External Information Systems	Yes
AT-1	Security Awareness & Training Policy and Procedures	Yes
AT-2	Security Awareness	Yes
AT-3	Security Training	Yes
AT-4	Security Training Records	Yes
AU-6	Audit Review, Analysis, and Reporting	Not Effective, See Finding 2
CA-1	Security Assessment and Authorization Policy & Procedures	Yes
CA-2	Security Assessments	Yes
CA-3	Information System Connections	Yes
CA-5	Plan of Action and Milestones	Yes
CA-6	Security Authorization	Yes
CM-1	Configuration Management Policy and Procedures	Yes
CM-2	Baseline Configuration	Yes
CM-3	Configuration Change Control	Yes
CM-6	Configuration Settings	Not Effective, See Finding 1
CM-8	Information System Component Inventory	Yes
CP-1	Contingency Planning Policy & Procedures	Yes
CP-2	Contingency Plan	Yes
CP-4	Contingency Plan Testing and Exercises	Yes
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)	Yes
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

Control	Control Name	Is Control Effective?
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	Yes
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