

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 2015

**No. I-PA-EAC-02-15
NOVEMBER 2015**



U.S. ELECTION ASSISTANCE COMMISSION

OFFICE OF INSPECTOR GENERAL


1335 East West Highway - Suite 4300

Silver Spring, MD 20910

Memorandum

November 13, 2015

To: Alice Miller
Acting Executive Director

From: Roger La Rouché 
Deputy Inspector General

Subject: Final Report - U.S. Election Assistance Commission's Compliance with the Requirements of the Federal Information Security Management Act Fiscal Year 2015 (Assignment No. I-PA-EAC-02-15)

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) compliance with the Federal Information Security Management 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 had a properly designed and effective information security program except for patch and vulnerability management. As a result of these weaknesses, CLA said that EAC's operations and assets were not fully protected from the risk of unauthorized access, misuse, and disruption. CLA also reported that although EAC "management acknowledged that some of EAC managed devices were affected, CLA "determined that since other (e.g. General Services Administration [GSA]) devices were visible during our internal scanning, all these identified weaknesses could potentially affect EAC systems and data, due to an inadequate segmentation of the GSA and EAC networks." Finally, CLA stated that EAC initiated appropriate corrective action.

EAC's response to the draft report stated that its review of the scanning results noted that all "except one of the IP [Internet Protocol] addresses devices on the findings belongs to GSA's network." In that regard, EAC also responded that all its devices are separated and isolated from inbound traffic from GSA's network "by VLAN in line with the internal Firewall to prohibit any internal access to the EAC's network." Finally, EAC said that: "Due to inbound traffic restrictions to the EAC network, the risk

associated with the identified vulnerabilities would not be able to be exploited by external users. . . .The record shows no security incident was reported for the FY2015.”

In commenting on the EAC response, CLA said that while a firewall would provide some measure of protection, the fact that it was “able to view GSA during scanning indicates that inbound and outbound traffic to and from GSA systems was permitted. This pathway could be utilized to exploit vulnerabilities on GSA devices and potentially compromise EAC data and systems.”

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) 734-3106.

Attachment

**Audit of the Election Assistance Commission's
Compliance with the
Federal Information Security Management Act of 2002, as Amended
Fiscal Year 2015**



CliftonLarsonAllen LLP
www.claconnect.com

November 11, 2015

Mr. Roger LaRouche
Deputy Inspector General
U.S. Election Assistance Commission
1335 East West Highway
Suite # 4300
Silver Spring, MD. 20910

Dear Mr. LaRouche:

Enclosed is the draft version of the *Audit of the Election Assistance Commission's Fiscal Year 2015 Compliance with the Federal Information Security Management Act of 2002, as Amended*. The Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to conduct the audit.

The audit objective was to determine whether the Election Assistance Commission (EAC) implemented selected security and privacy controls for selected information systems in support of the Federal Information Security Management Act (FISMA) of 2002¹, as amended². To answer the audit objective, we tested EAC's implementation of selected 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*. The audit reviewed EAC's General Support System. Fieldwork was conducted at EAC's headquarters in Silver Spring, MD, from July 07, 2015, to October 8, 2015.

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 had sound controls for its information security program except for patch and vulnerability management. As a result, EAC's operations and assets were not fully protected from the risk of unauthorized access, misuse, and disruption. The weaknesses discussed in this report related to missing or outdated software patches and the

¹ Enacted as Title III of the E-Government Act of 2002, Public Law 107-347 (2002). Section 301 of the Act added a new subchapter on information security to the United States Code at 44 U.S.C. 3541-3549.

² The Federal Information Security Modernization Act of 2014 – Amends the FISMA 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 Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

use of unsupported software which resulted from an ineffective patch and vulnerability management program. The failure to appropriately and timely patch vulnerabilities may enable an attacker to exploit these weaknesses to read, modify, and/or delete financial or sensitive information, disrupt operations, or launch attacks against other systems at EAC.

To help EAC strengthen its information security program, we recommend that EAC management implement corrective actions to resolve critical and high risk weaknesses identified related to patching and software upgrades for those systems identified within the detailed scanning results provided by CLA.

We very much appreciate the opportunity to serve you and will be pleased to discuss any questions you may have.

Very truly yours,

CLIFTONLARSONALLEN LLP

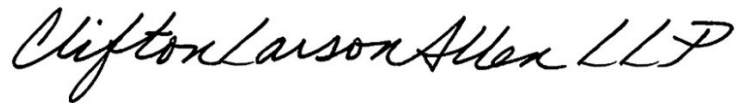
A handwritten signature in black ink that reads "CliftonLarsonAllen LLP". The signature is written in a cursive, flowing style with a large, stylized 'C' at the beginning.

Table of Contents

Executive Summary	1
Audit Findings	2
Background	3
<i>Federal Information Security Management Act</i>	3
<i>NIST Security Standards and Guidelines</i>	4
Appendix I - Scope and Methodology	5
Appendix II - Management Comments	7
Appendix III - Evaluation of Management Comments	9
Appendix IV - Status of Prior Year Findings.....	10
Appendix V - Summary of Results of each Control Reviewed	11

Executive Summary

The Federal Information Security Management Act of 2002 (FISMA), as amended³ requires 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) 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 and privacy controls for selected information systems⁴ in support of FISMA and related information security policies, procedures, standards, and guidelines.

These objectives included evaluating and reporting on whether a) security programs, plans, policies, and procedures in place were in compliance with applicable federal laws and regulations, b) controls provide reasonable assurance to adequately safeguard and protect EAC sensitive data and ensure that financial data are reliable and complete and provided timely, and c) controls were adequate to prevent or detect unauthorized activities, including external intrusion, theft, or misuse of EAC data, and destruction of EAC hardware, software, and data. 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.

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.

The audit concluded that EAC generally had sound controls for its information security program; however, however we did note weaknesses in the area of patch and vulnerability management controls. Thus, although EAC effectively implemented 64 of 66 selected security controls, they had not effectively implemented the remaining two control areas.

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

³ Enacted as Title III of the E-Government Act of 2002, Public Law 107-347 (2002). Section 301 of the Act added a new subchapter on information security to the United States Code at 44 U.S.C. 3541-3549.

The Federal Information Security Modernization Act of 2014 – Amends the FISMA 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 Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

⁴ For FY2015, CLA selected the EAC network (general support system), which is utilized for email, Internet, voice over Internet Protocol (VoIP) and provides access to EAC application.

Audit Findings

1. EAC needs to improve controls over patch management and maintenance of software upgrades.

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

- 9 instances of unsupported software (comprised of Open SSL [Secure Socket Layer], Windows Server 2003, McAfee, UNIX, and web servers) representing 7 critical and 2 high risk vulnerabilities.
- 2 critical instances and 9 high risk instances of missing or outdated software patches related to missing Microsoft 2012 patches and Open SSL.

Although management acknowledged that some EAC managed devices were affected, we determined that since other (e.g. General Services Administration [GSA]) devices were visible during our internal scanning, all these identified weaknesses could potentially affect EAC systems and data, due to an inadequate segmentation of the GSA and EAC networks. Management also stated that they would work with GSA to update the server version of the McAfee Orchestrator product.

According to NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, security control 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.

Failing to appropriately 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 (we identified unapplied patches or unsupported software going back to the year 2008).

Recommendation 1: We recommend that EAC management implement corrective actions to resolve critical and high risk weaknesses identified related to patching and software upgrades for those systems identified within the detailed scanning results provided by CLA.

Recommendation 2: We recommend that EAC management work with GSA to ensure EAC's internal network is properly segmented from GSA.

Background

Federal Information Security Management Act

The Federal Information Security Management Act of 2002 (FISMA), as amended was enacted into law as Title III of the E-Government Act of 2002, Public Law No. 107-347. Key requirements of FISMA include:

- The establishment of an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source;
- An annual independent evaluation of the agency's information security programs and practices; and
- An assessment of compliance with the requirements of the Act.

In addition, FISMA requires Federal agencies to implement the following:

- Periodic risk assessments;
- Information security policies, procedures, standards, and guidelines;
- Delegation of authority to the Chief Information Officer to ensure compliance with policy;
- Security awareness training programs;
- Periodic (annual and more frequent) testing and evaluation of the effectiveness of security policies, procedures, and practices;
- Processes to manage remedial actions for addressing deficiencies;
- Procedures for detecting, reporting, and responding to security incidents;
- Plans to ensure continuity of operations; and
- Annual reporting on the adequacy and effectiveness of the information security program.

The Office of Management and Budget (OMB) has issued executive branch policy for implementing FISMA: Circular No. A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources* (OMB Circular A-130, Appendix III), dated November 28, 2000. This circular establishes a minimum set of controls to be included in Federal agency automated information security programs. In particular Appendix III of OMB Circular A-130 defines adequate security as security commensurate with the risk and magnitude of the harm resulting from loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

Additionally, OMB has issued guidance related to information security with regard to plans of action and milestones (POA&Ms) for addressing findings from security control assessments, security impact analyses, and continuous monitoring activities. Per OMB Memoranda M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, POA&Ms provide a roadmap for continuous agency security improvement and assisting agency officials with prioritizing corrective action and resource allocation.

Further, OMB is responsible for reporting to Congress a summary of the results of Federal agencies' compliance with FISMA requirements.

NIST Security Standards and Guidelines

FISMA requires the National Institute of Standards and Technology (NIST) to provide standards and guidelines pertaining to federal information systems. Standards prescribed are to include information security standards that provide minimum information security requirements and are otherwise necessary to improve the security of federal information and information systems. FISMA also requires that federal agencies comply with Federal Information Processing Standards (FIPS) issued by NIST. In addition, NIST develops and issues Special Publications (SPs) as recommendations and guidance documents.

FIPS Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems* (FIPS PUB 200), mandates the use of NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

The purpose of NIST SP 800-53 is to provide guidelines for selecting and specifying security controls for information systems supporting an agency to meet the requirements of FIPS PUB 200. The security controls described in NIST SP 800-53 are organized into 18 families. Each security control family includes security controls associated with the security functionality of the family. In addition, there are three general classes of security controls: management, operational, and technical.

The NIST SP 800-53, Revision 4, security control families are as follows:

Table 1: Security Control Families

Control Class	Security Control Family
Management Controls	Risk Assessment
	Planning
	System and Services Acquisition
	Security Assessment and Authorization
Operational Controls	Personnel Security
	Physical and Environmental Protection
	Contingency Planning
	Configuration Management
	Maintenance
	System and Information Integrity
	Media Protection
	Incident Response
	Awareness and Training
Technical Controls	Identification and Authentication
	Access Control
	Audit and Accountability
	System and Communications Protection

Appendix I - 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 Management Act of 2002, as amended.

The audit included the testing of selected management, technical, and operational controls outlined in 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. In addition, the audit included a follow up on prior year audit recommendations⁵ to determine if EAC had made progress in implementing any recommended improvements.

The audit was conducted at EAC's headquarters in Silver Spring, MD, from July 07, 2015 to October 8, 2015.

Methodology

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

To accomplish our audit objective we:

⁵ *Audit of the Election Assistance Commission's Fiscal Year 2014 Compliance with the Federal Information Security Management Act of 2002*, October 31, 2014.

- 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 security control assessments.
- Tested system processes to determine the adequacy and effectiveness of selected controls (listed in Appendix V).

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 - Management Comments



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

Memorandum

November 3, 2015

To: Roger LaRouche
Deputy Inspector General

From: Alice P. Miller
Chief Operating Officer / Acting Executive Director

Subject: Response to Draft Audit Report - U.S. Election Assistance Commission
Compliance with the Requirements of the Federal Information Security
Management Act Fiscal Year 2015 (Assignment No. I-PA-EAC-01-15)

CLA FISMA Auditors performed a vulnerability scan of selected agency's devices on the IP address ranges provided including EAC's internal network during the week of September 28th.

After further reviewing the scanning result of the FISMA audit report, management concurs with the second part of the audit result submitted by the auditors with the following explanation and recommendations.

On the summary audit report, the auditors evaluated the effectiveness of EAC's information security program and practices, compliance with FISMA and related information security policies, procedures, standards and guidelines. As the draft report reflects EAC generally has sound controls for its information security program in place, except for patch and vulnerability management where EAC needs to further strengthen its patch management operations.

After reviewing the excel spreadsheet scanning result from the Auditors, we have noted all, except one of the IP addresses devices on the findings belongs to GSA's Network. The four machines that were reported on the findings which belong to GSA have been identified and analyzed. One of the devices attributed to the vulnerabilities was a Dell Remote Access controller (DRAC) card that helps in managing and troubleshooting a server. The other devices were a CISCO appliance and two windows 2003 servers. Even though, the scope of IP address range scanned were part of the IP address we provided to the FISMA auditors, and we have been informed these IP addresses should not have been assigned to EAC. All our devices are separated and isolated from inbound traffic from GSA's network by VLAN in line with the internal Firewall to prohibit any internal

access to the EAC's internal network. As you know, GSA is our Internet Service Provider (ISP) and we use their Network infrastructure, and we are partitioned by the internal Firewall.

EAC – OCIO has initiated actions to address the vulnerabilities identified. OCIO has reached out to GSA to start working with security and Firewall team to tighten rules and address the segment issues. We have requested GSA to re-segment EAC's IP address to include the 5 devices we have on the COOP site and reconfigure the internal Firewall to tighten the and restrict access from EAC to GSA and vice versa which we believe resolves the concern.

EAC- OCIO has requested GSA to isolate the affected devices from EAC's network by November 10, 2105 to address the concern on the notice of finding and recommendation.

The scanned report also indicates that one of EAC's devices showed unsupported McAfee Orchestra agent version 4.6 that expired on March 2105, which its function is to report the status of antivirus on the device to the enterprise antivirus server. Upon review the status of the server, the antivirus definition on the server is up to date, which reduces the risk of virus infection. EAC OCIO took action and has updated the Orchestra McAfee agent to the latest version 5.0

Due to inbound traffic restriction to EAC network, the risk associated with the identified vulnerabilities would not be able to be exploited by external users. Therefore, the EAC controls and mechanisms in place will keep external users from exploiting the CLA-indentified weaknesses. The record shows, no security incident was reported for the FY2015.

Copy to: Mohammed Maeruf, CIO
Annette Lafferty, CFO

Appendix III - Evaluation of Management Comments

CLA acknowledges that EAC has initiated improvements to controls to address weaknesses identified in our report. Furthermore, while we agree that the firewall between the EAC and GSA networks as described in the EAC response would provide some measure of protection, more needs to be done. In that regard, during our audit tests we were able to scan GSA devices indicating that inbound and outbound traffic to and from GSA systems was permitted. This pathway could be utilized by an attacker to exploit vulnerabilities on GSA devices visible during our scans and potentially compromise EAC data and systems.

Appendix IV - Status of Prior Year Findings

The following table provides the status of the FY 2014 FISMA audit recommendations.⁶

No.	FY 2014 Audit Recommendation	EAC Status	Auditor's Position on Status
1	None	Not Applicable	Not Applicable

⁶ *Audit of the Election Assistance Commission's Fiscal Year 2014 Compliance with the Federal Information Security Management Act of 2002, October 31, 2014.*

Appendix V - 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	Yes
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	Yes
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
MP-1	Media Protection Policy and Procedures	Yes

Appendix V

Control	Control Name	Is Control Effective?
MP-2	Media Access	Yes
MP-3	Media Marking	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-1	System and Services Acquisition Policy and Procedures	Yes
SA-5	Information System Documentation	Yes
SA-9	External Information Systems	Yes
SC-7	Boundary Protection	Yes
SC-8	Transmission Integrity	Yes
SC-19	VOIP	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-6	Information Security Measures of Performance	Yes
PM-9	Risk Management Strategy	Yes
PM-10	Security Authorization Process	Yes

OIG's Mission

Help to ensure efficient, effective, and transparent EAC operations and programs

Obtaining Copies of OIG Reports

Copies of OIG reports are available on the OIG website, www.eac.gov/inspector_general/

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

To order by phone: Voice: (301) 734-3104
Fax: (301) 734-3115

To Report Fraud, Waste and 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)

On-Line Complaint Form: www.eac.gov/inspector_general/

FAX: (301)-734-3115

