

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 2010

**No. I-PA-EAC-02-10
OCTOBER 2010**




U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL
1201 New York Ave. NW - Suite 300
Washington, DC 20005

October 27, 2010

Memorandum

To: Donetta Davidson
Chair, U.S. Election Assistance Commission

From: Curtis W. Crider 
Inspector General

Subject: Final Report –U.S. Election Assistance Commission’s Compliance with the Requirements of the Federal Information Security Management Act (Assignment No. I-PA-EAC-02-10)

We contracted with the independent certified public accounting firm of Leon Snead & Co. (LSC) to conduct the audit of the U.S. Election Assistance Commission’s (EAC) compliance with the requirements of the Federal Information Security Management Act (FISMA). LSC found that EAC information technology security program is in substantial compliance with FISMA. The audit noted that EAC took actions to address control weaknesses identified in the 2009 FISMA audit. However, EAC still needs to complete corrective action in two areas: (1) The agency’s contingency planning and testing, and (2) compliance with Personal Identification Information and Privacy Act requirements.

In its October 8, 2010 response to the draft report (Attachment 2) the EAC generally concurred with the recommendations and provided the actions planned to address the issues identified in the report. Based on the response we consider the recommendations in the report resolved but not implemented. The OIG will monitor the implementation of the recommendations.

The legislation, as amended, creating the Office of Inspector General (5 U.S.C. § App.3) requires semiannual reporting to Congress on all reports issued, actions taken to implement recommendations, and recommendations that have not been implemented. Therefore, this report will be included in our next semiannual report to Congress.

If you have any questions regarding this report, please call me at (202) 566-3125.

U.S. Election Assistance Commission

Compliance with the Requirements of
the Federal Information Security Management Act

Fiscal Year 2010

Submitted By

Leon Snead & Company, P.C.
Certified Public Accountants & Management Consultants



**LEON SNEAD
& COMPANY, P.C.**

*Certified Public Accountants
& Management Consultants*

416 Hungerford Drive, Suite 400
Rockville, Maryland 20850
301-738-8190
fax: 301-738-8210
leonsnead.companypc@erols.com

October 12, 2010

Mr. Curtis W. Crider
Inspector General
U.S. Election Assistance Commission
1440 New York Ave, N.W., Suite 203
Washington, DC 20005

Dear Mr. Crider:

Enclosed is the final report on our audit of U.S. Election Assistance Commission's compliance with the Federal Information Security Management Act for fiscal year 2010.

We appreciate the courtesies and cooperation provided by EAC personnel during the audit.

Leon Snead & Company PC

Leon Snead & Company, P.C.

TABLE OF CONTENTS

	<u>Page</u>
Introduction.....	1
Objective, Scope and Methodology.....	1
Summary of Audit.....	2
Findings and Recommendations.....	3
Attachment 1 – Status of Prior Year Findings.....	6
Attachment 2 – Response to Audit.....	7

Introduction

Leon Snead & Company, P.C. has completed its audit of EAC's Information Technology (IT) security program for fiscal year 2010.

Title III of the E-Government Act, entitled the *Federal Information Security Management Act* (FISMA) requires each Federal agency to develop, document, and implement an agency-wide program to provide security for information and information systems that support the operations and assets of the agency, including those systems managed by another agency or contractor. FISMA, along with the *Paperwork Reduction Act of 1995* and the *Information Technology Management Reform Act of 1996*, emphasize a risk-based policy for cost-effective security. In support of and reinforcing this legislation, the Office of Management and Budget (OMB) through Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, requires executive agencies within the Federal government to:

- Plan for security;
- Ensure that appropriate officials are assigned security responsibility;
- Periodically review the security controls in their information systems; and
- Authorize system processing prior to operations and, periodically, thereafter.

The EAC is an independent, bipartisan agency created by the Help America Vote Act (HAVA) to assist in the effective administration of Federal elections. In October 2002, Congress passed HAVA to invest in election infrastructure and set forth a comprehensive program of funding, guidance, and ongoing research. To foster those programs and to promote and enhance voting for United States Citizens, HAVA established the EAC.

EAC'S mission is to assist in the effective administration of Federal elections. The agency is charged with developing guidance to meet HAVA requirements, adopting voluntary voting systems guidelines, and serving as a national clearinghouse of information about election administration. EAC also accredits testing laboratories and certifies voting systems and audits the use of HAVA funds.

Objective

The objective of our audit was to evaluate EAC's compliance with OMB Circular A-130 and FISMA requirements.

Scope and Methodology

To accomplish the objective, we reviewed EAC policies and procedures, and performed tests to determine whether:

- EAC policies and procedures were adequate to establish an agency-wide IT security program in accordance with OMB requirements.

- EAC personnel assessed the risk to operations and assets under their control, assigned a level of risk to the systems, tested and evaluated security controls and techniques, implemented an up-to-date security plan for each major application and general support system, and performed certification and accreditation of the agency's systems.
- EAC developed, documented, and tested comprehensive contingency plans for the agency's information systems.
- EAC provided security awareness training to all employees and contractors, and provided sufficient specialized training to key IT security personnel.
- EAC established a continuous monitoring program, including whether the agency monitored scanning results and corrected vulnerabilities, as necessary.
- EAC designed and implemented access controls effectively.
- EAC met OMB requirements for securing sensitive personal identifying information and Privacy Act requirements.

The audit was performed in accordance with *Government Auditing Standards*, and included appropriate tests necessary to achieve the audit objective. Other criteria used in the audit included the National Institute of Standards and Technology (NIST) guidance, and OMB Memorandum *M-10-15, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated April 21, 2010.

Summary of Audit

While the EAC IT security program is now in substantial compliance with FISMA, the agency remained at risk for a substantial portion of 2010. Our audit found that EAC had implemented actions to address control weaknesses identified in our 2009 report except for: (1) the testing and exercise of the recently completed contingency plan; and (2) compliance with required OMB PII and Privacy Act controls. EAC delayed implementation of planned corrective actions until it hired a Chief Information Officer (CIO) about June 2010. As a result, many of the weaknesses identified in 2009 continued for a significant portion of the 2010 fiscal year.

EAC officials in a response to the draft report advised that the agency is committed to establishing and maintaining an agency-wide program to provide security for information and information systems that support the operations and assets of the agency, including those systems managed by another agency or contractor. EAC officials advised that as part of this effort, EAC hired a Chief Information Officer (CIO) and developed, documented, and implemented its agency-wide Information Security Program. EAC officials agreed with the recommendations to complete the EAC contingency plan by the end of the calendar year, and update the contingency plan based on the results of testing, and to bring the EAC into full compliance with OMB PII regulations and Privacy Act requirements. The agency plans to be in full compliance by the end of the calendar year 2010.

FINDINGS AND RECOMMENDATIONS

1. IT Security Program Improved but Additional Controls are Necessary

EAC has corrected most of the significant control weaknesses identified during our audit in 2009 that impacted the agency's IT security program. While the EAC IT security program is now in substantial compliance with FISMA, the agency was at risk for a substantial portion of fiscal year 2010. The agency delayed completion of corrective actions until the CIO was hired in about June 2010. Also, EAC has not yet completed required actions to test the newly completed contingency plan, or implemented controls for compliance with PII and Privacy Act requirements.

As part of our audit, we assessed whether EAC had taken action to address the problems we identified in 2009 with the agency's agency-wide IT security program. For each of the security control areas established by Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information System*, we determined if actions taken by EAC brought the agency into substantial compliance with the control requirements contained in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*. The table below shows our determinations for 2010.

CONTROL REQUIREMENT	Compliance Determination
Access Control	Substantial Compliance
Awareness and Training	Substantial Compliance
Audit and Accountability	Substantial Compliance
Certification, Accreditation, and Security Assessments	Substantial Compliance
Configuration Management	Substantial Compliance
Contingency Planning	Partial Compliance
Identification and Authentication	Substantial Compliance
Incident Response	Substantial Compliance
Maintenance	Substantial Compliance
Media Protection	Substantial Compliance
Physical and Environmental Protection	Substantial Compliance
Planning	Substantial Compliance
Personnel Security	Substantial Compliance
Risk Assessment	Substantial Compliance
System and Services Acquisition	Substantial Compliance
System and Communications Protection	Substantial Compliance
System and Information Integrity	Substantial Compliance

As noted above, we rated the contingency planning as partial compliance because the plan was only recently completed and has not yet undergone testing. EAC has developed testing and exercise plans, and once these tests are completed, analyzed, and any necessary adjustments made to the plan, EAC will be in compliance with this control area.

In our 2009 audit, we reported that EAC was not in compliance with OMB requirements dealing with securing PII data and certain requirements of the Privacy Act. We performed audit tests to determine whether EAC had taken actions to come into substantial compliance with these requirements. EAC's privacy officer advised us that the agency was moving to come into full compliance with OMB and Privacy Act requirements, but all actions are not yet completed. The following table shows the 2009 problem areas, the actions EAC has taken, and those areas where additional corrective actions are necessary.

OMB Guidance	Requirement	EAC Actions in 2010	Auditor Comments
M-07-16, dated May 22, 2007	Requires agency to develop and implement a breach notification.	EAC has published a policy on this matter.	EAC meets requirement.
	Review current PII holdings and determine if holdings are accurate, relevant and reduce the PII holdings to minimum necessary.	EAC completed a review in 2010, and has taken actions to reduce holdings.	EAC meets requirement.
	Encrypt data on mobile computers.	EAC has purchased encrypted drives, and does not maintain PII data on Hard Drive.	EAC meets requirement.
	Require two-factor authentication.	EAC was required by GSA to implement this requirement.	EAC meets requirement.
	Require all personnel with access to PII to sign at least annually a document that describes rules of behavior on PII.	EAC has training and requires personnel to authenticate security awareness and privacy training.	EAC meets requirement.
	Develop and publish a "routine use" policy dealing with breach of security relating to PII data, including actions taken for individuals affected by the breach.	EAC has a internal policy but has not published a "routine use" policy in the federal register	EAC is not in full compliance with this area.
OMB Circular A-130	Publish and review biennially each system of records notice to ensure that it accurately describes the system of records.	EAC has not yet published its system of records.	EAC is not in full compliance with this area.
	Review every four years the routine use disclosures associated with each system of records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency collected the information.	EAC has not yet published its system of records.	EAC is not in full compliance with this area.

OMB Guidance	Requirement	EAC Actions in 2010	Auditor Comments
OMB Memorandum 03-22	Conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available.	EAC has not yet completed this assessment.	EAC is not in full compliance with this area.
	Post privacy policies on agency websites used by the public.	EAC has posted on website.	EAC meets requirement.

EAC has written policies and procedures, and developed and implemented necessary controls to bring its IT security program, as of the end of fiscal year 2010, into substantial compliance with FISMA requirements. As discussed above, EAC needs to continue to take actions to bring itself into compliance with OMB directives dealing with PII and Privacy Act requirements. At the end of 2010, EAC has developed a foundation for its IT security program that, as its IT operations mature, will enable EAC to sustain compliance with FISMA requirements.

Recommendations:

1. Assure that the testing and exercise of the recently completed EAC contingency plan is accomplished by the end of the calendar year. Update the plan based upon the results of this testing.
2. Emphasize the completion of actions necessary to bring the EAC into full compliance with OMB PII regulations and Privacy Act requirements.

Agency Response

The Executive Director, in a response to the draft report, advised that the agency is committed to establishing and maintaining an agency-wide program to provide security for information and information systems that support the operations and assets of the agency, including those systems managed by another agency or contractor. The Executive Director advised that as part of this effort, EAC hired a Chief Information Officer (CIO) and developed, documented, and implemented its agency-wide Information Security Program.

EAC officials agreed with the recommendations to complete the EAC contingency plan by the end of the calendar year, update the contingency plan based on the results of testing, and to bring the EAC into full compliance with OMB PII regulations and Privacy Act requirements. The agency plans to be in full compliance by the end of the calendar year 2010.

Status of Prior Year Findings

No.	Prior Year Condition	Current Status
1	IT Security Program Improved but Additional Controls are Necessary.	EAC officials took action to correct this problem.
2	An agency-wide information security program in compliance with FISMA has not been developed. A security management structure with adequate independence, authority, and expertise which is assigned in writing has not been implemented.	EAC officials took action to correct this problem.
3	Policies or procedures for information security or privacy management have not been developed. Per the terms of the MOU, the GSA procedures will prevail where there are not guiding policies provided by the user organization.	EAC officials took action to correct this problem.
4	A Continuity of Operations Plan, Disaster Recovery Plan, or Business Impact Assessment has not been developed.	EAC has completed a contingency plan, but has not yet tested the plan.
5	FDCC requirements were not met.	EAC officials took action to correct this problem.
6	Access Controls and Remote Access Need Strengthening	EAC officials took action to correct this problem.
7	Security Risk Assessments Need to be Finalized and Used to Develop Controls	EAC officials took action to correct this problem.
8	<p>EAC is not fully compliant with several Privacy Act Requirements including:</p> <ul style="list-style-type: none"> • A Chief Privacy Officer with the responsibility for monitoring and enforcing privacy related policies and procedures have not been designated. • EAC has not identified systems housing personally identifiable information or conducted related Privacy Impact Assessments required by OMB Memorandum 06-16. • EAC has not developed formal policies that address the information protection needs associated with personally identifiable information that is accessed remotely or physically removed. 	EAC officials took action to correct some but not all of these problems. Issue remains open.
9	Establish Controls to Ensure Audit and Accountability	EAC officials took action to correct this problem.
10	Restrict Access to Network Devices	EAC officials took action to correct this problem.



U. S. ELECTION ASSISTANCE COMMISSION
OFFICE OF THE EXECUTIVE DIRECTOR
1201 New York Avenue, NW, Suite 300
Washington, DC. 20005

October 8, 2010

Memorandum

To: Arnie G. Garza
Assistant Inspector General for Audits

From: Thomas R. Wilkey
Executive Director

A handwritten signature in black ink, appearing to read "TRW", is positioned to the right of the "From:" line.

Subject: Management Response to: Draft Audit Report – U.S. Election Assistance Commission Audit of Compliance with the Requirement of the Federal Information Security Management Act (FISMA) Fiscal Year 2010 (Assignment No.I – PA-EAC-02-10).

The U.S. Election Assistance Commission (EAC) appreciates the opportunity to review the draft report on the audit of the Federal Information Security Management Act (FISMA) for FY 2010. We have reviewed the draft report. Responses to the recommendations are provided below.

As part of the audit, the auditor assessed whether EAC had taken action to address the issues identified in fiscal year (FY) 2009 with EAC's agency-wide IT security program. The review indicated that EAC has corrected most of the significant issues but needs to implement corrective actions in two major areas. The first area deals with the agency's contingency planning and testing. The second area involves the agency's compliance with Personal Identification Information (PII) and Privacy Act requirements.

The auditor rated contingency planning as in partial compliance since the plan was only recently completed and has not yet undergone testing. EAC has developed its testing criteria for the plan and will be in compliance with the control requirements once the tests are completed, results analyzed, and necessary adjustments made to the plan.

The auditor also determined that PII regulations and Privacy Act requirements are in partial compliance since additional actions are needed to bring the agency into full

compliance with Office of Management and Budget (OMB) requirements dealing with securing PII data and certain requirements of the Privacy Act.

Auditor's Recommendations:

1. Assure that the testing and exercise of the recently completed EAC contingency plan is accomplished by the end of the calendar year. Update the plan based upon the results of the testing.
2. Emphasize the completion of actions necessary to bring the EAC into full compliance with OMB PII regulations and Privacy Act requirements.

Management's Response:

EAC is committed to establishing and maintaining an agency-wide program to provide security for information and information systems that support the operations and assets of the agency, including those systems managed by another agency or contractor. As part of this effort, EAC hired an experienced Chief Information Officer (CIO) and developed, documented, and implemented its agency-wide Information Security Program. We appreciate the auditor's acknowledging the significant progress made by EAC to resolve FY 2009 FISMA audit findings. Below is our response to FY 2010 FISMA audit recommendations.

1. Management agrees with the recommendations to complete the EAC contingency plan by the end of the calendar year, and update the contingency plan based on the results of testing.
2. Management agrees with the recommendation to bring the EAC into full compliance with OMB PII regulations and Privacy Act requirements. The agency plans to be in full compliance by the end of the calendar year 2010.

ccs: Tom Heideman (via e-mail)
Curtis Crider (via e-mail)
Alice Miller (via e-mail)
Mohammed Maeruf (via e-mail)

OIG's 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.

Obtaining 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
1201 New York Ave. NW - Suite 300
Washington, DC 20005

To order by phone: Voice: (202) 566-3100
Fax: (202) 566-0957

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
1201 New York Ave. NW - Suite 300
Washington, DC 20005

E-mail: eacoig@eac.gov

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

FAX: 202-566-0957

