U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL

FINAL REPORT:

U.S. ELECTION ASSISTANCE COMMISSION

EVALUATION OF COMPLIANCE WITH THE REQUIREMENTS OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT

FISCAL YEAR 2011

No. I-PA-EAC-02-11
OCTOBER 2011

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

MEMORANDUM

October 5, 2011

To: 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-02-11)

In accordance with the Federal Information Security Management Act (FISMA), the Office of Inspector General (OIG) engaged Leon Snead & Co. P.C., an independent certified public accounting firm, to conduct an audit of the U.S. Election Assistance Commission's (EAC) compliance with the OMB Circular A-130 and FISMA requirements. 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.

Leon Snead & Co. found that the EAC was in substantial compliance with FISMA requirements. EAC implemented actions to address prior year's findings regarding Privacy Act requirements and established sufficient policies and procedures relative to its IT security program.

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 2011

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

September 23, 2011

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 2011.

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

Leon Snead & Company, P.C.

TABLE OF CONTENTS

Page

Introduction

Leon Snead & Company, P.C. has completed an audit of EAC's Information Technology (IT) security program for fiscal year 2011. 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.
- 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.

- developed, documented and tested comprehensive contingency plans for the agency's information systems.
- provided security awareness training to all employees and contractors, and provided sufficient specialized training to key IT security personnel.
- established a continuous monitoring program, including whether the agency monitored scanning results and corrected vulnerabilities, as necessary.
- designed and implemented access controls effectively.
- met OMB requirements for securing sensitive personal identifying information and Privacy Act requirements.

We conducted this audit 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. Other criteria used in the audit included the National Institute of Standards and Technology (NIST) guidance, and OMB Memoranda. The audit was performed during the period April and September 2011.

Summary of Audit

Our audit found that the EAC was in substantial compliance with FISMA requirements. Specifically, we noted that the EAC had established sufficient policies and procedures relating to its IT security program to address identified risks; implemented actions to address prior concerns relating to meeting Privacy Act requirements; established a continuous monitoring program that substantially addressed all NIST requirements; provided annual security awareness training and specialized training to its IT specialists; developed and tested a contingency plan; and had established required access controls sufficient to meet identified risks.

Status of Prior Year Findings

Prior Year Condition	Current Status
Contingency planning for EAC was not in full compliance with FISMA because the recently completed plan had not yet undergone testing.	EAC officials took action to correct this problem.
Develop and publish a "routine use" policy dealing with breach of security relating to personnel identifiable information data, including actions taken for individuals affected by the breach.	EAC officials took action to correct this problem.
Conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available.	EAC analyzed its systems that contain personnel identifiable information and published System of Record Notices in 2011, and determined that none of the agency's systems required a privacy impact assessment to be issued. We concurred in this determination.

U.S. Election Assistance Commission
Office of the Executive Director
1201 New York Ave. NW – Suite 300
Washington, DC 2005

Memorandum

September 21, 2011

To: Arnie Garza
Assistant Inspector General for Audits

From: Tom Wilkey
Executive Director

Subject: Draft Audit Report – U.S. Election Assistance Commission Audit of Compliance with the requirement of the Federal Information Security Management Act (FISMA) Fiscal year 2011 (Assignment No.I—PA-EAC-02-11)

After reviewing the attached audit report and summary of the audit results of the FISMA Audit, management agrees with the audit result submitted by the auditors.

As the audit report indicates, management took the necessary actions to address the findings that were found on the previous year audit report and we are now substantially in compliance with the FISMA requirements.

We thank you and the auditors for courtesies and assistance that was extended to our staff during the audit.

If you have any questions regarding our response, please do not hesitate to contact me at (202) 566-3109

Copy to: Alice Miller, COO
Mohammed Maeruf, CIO

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