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 2009

No. I-PA-EAC-02-09
OCTOBER 2009

U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL
1225 New York Ave. NW - Suite 1100
Washington, DC 20005

October 15, 2009

Memorandum

To: Gineen Beach
Chair, U.S. Election Assistance Commission

From: Curtis W. Crider
Inspector General

Subject: Final Report –Evaluation of U.S. Election Assistance Commission's Compliance with the Requirements of the Federal Information Security Management Act (Assignment No. I-PA-EAC-02-09)

We contracted with the independent certified public accounting firm of Leon Snead & Co. (Leon Snead) to conduct the evaluation of the U.S. Election Assistance Commission's (EAC) compliance with the requirements of the Federal Information Security Management Act. Leon Snead found that the EAC has taken significant actions to address many of the serious problems noted in prior FISMA reports. However, the EAC still needs to make improvements in its agency-wide security program to bring it into full compliance with Federal Information Security Management Act and Office of Management and Budget requirements.

In its September 30, 2009 response to the draft report (Appendix A) 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

Evaluation of Compliance with the Requirements of
the Federal Information Security Management Act

Fiscal Year 2009

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 1, 2009

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:

Leon Snead & Company, P.C., has completed its evaluation of U.S. Election Assistance Commission's compliance with the Federal Information Security Management Act for fiscal year 2009. We have incorporated and attached the agency's response into the report.

Leon Snead & Company appreciates the courtesies and cooperation provided by EAC personnel during the evaluation.

Sincerely,

Leon Snead & Company, P.C.

Leon Snead and Company, P.C.

TABLE OF CONTENTS

Page

Introduction

Leon Snead & Company, P.C. has completed its evaluation of EAC's Information Technology (IT) security program for fiscal year 2009.

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 Unites 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.

Objectives

The evaluation's objectives were to (1) assess the agency's information security program and practices and related compliance with FISMA requirements and (2) follow up on whether the agency implemented appropriate actions to address recommendations made in the previous OIG report.

Scope and Methodology

To accomplish the objectives stated above, we evaluated the following control and compliance requirements.

- Determined if EAC's policies and procedures met FISMA and OMB requirements, and whether EAC maintained an adequate agency-wide IT security program in accordance with FISMA requirements.

- Determined if 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, as appropriate.
- Ascertained if comprehensive contingency plans have been developed, documented, and tested.
- Determined if EAC has provided security awareness training to all employees and contractors.
- Determined if access controls were developed and effectively implemented.
- Ascertained whether the agency met OMB requirements for securing sensitive personnel privacy information.
- Determined, for the areas tested, if EAC's IT security program met the minimum security requirements identified in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations.*

The evaluation was performed in accordance with *Government Auditing Standards*, and included appropriate tests necessary to achieve the evaluation objectives. Other criteria used in the evaluation included the National Institute of Standards and Technology (NIST) guidance, and OMB Memorandum M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated August 20, 2009.

Summary of Evaluation

Our 2009 evaluation found that EAC had taken actions to address many of the serious problems noted in the 2008 FISMA evaluation report. In addition, EAC had plans to address other issues noted in the report. However, EAC has not yet taken sufficient actions to establish an agency-wide IT security program that is in full compliance with FISMA and OMB requirements. The following table describes our conclusions on whether EAC was in substantial compliance (SC), partial compliance (PC), or not in substantial compliance (NSC) with IT security control areas indentified in FIPS 200.

CONTROL REQUIREMENT	Compliance Determination (SC, PC, NSC)
Access Control	NSC
Awareness and Training	SC
Audit and Accountability	PC
Certification, Accreditation, and Security Assessments	PC
Configuration Management	SC
Contingency Planning	NSC
Identification and Authentication	PC
Incident Response	SC
Maintenance	SC

Media Protection	SC
Physical and Environmental Protection	SC
Planning	PC
Personnel Security	SC
Risk Assessment	PC
System and Services Acquisition	SC
System and Communications Protection	PC
System and Information Integrity	SC

We identified the following problems that support our determinations shown above.

- IT security policies and procedures, which form the basis for a risk-based IT security program, have not been fully developed. During our evaluation, EAC issued a draft IT security handbook; however, the document needs to be finalized and detailed operational procedures need to be developed to fully meet this key FISMA control requirement. As a result, EAC incurs unnecessary risk until security policies and procedures are developed (or finalized) and implemented.

- EAC has not completed the required contingency planning for its information systems, which are part of an overall organizational program for achieving continuity of operations for mission/business operations during an emergency. We attributed this issue to the need for a security officer with expertise in managing an agency-wide IT security program. As a result, until EAC completes necessary contingency planning, COOP development, and implements actions to mitigate the identified risks, EAC incurs unnecessary risk of disruption of its operations.

- EAC has not fully implemented Federal Desktop Computer Configuration (FDCC) for workstations that OMB first mandated in 2007. As required by OMB, NIST has issued guidance that provides mandatory configuration requirements for desktops that run a windows operating system. These configurations eliminate known computer security vulnerabilities.

- EAC's access controls, including remote access to EAC's network, do not fully meet FISMA requirements. As a result, EAC incurs an unnecessary risk of unauthorized access to its information systems and data.

- EAC has not finalized required assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. As a result, EAC is not yet able to develop risk-based controls that take into account vulnerabilities and threat sources.

- Although EAC has actions underway to meet many of the OMB directives related to personally identifiable information (PII), additional actions are necessary before the agency fully meets these requirements.

- EAC's system produces audit records that contain sufficient information to establish what events occurred, and tracks sufficient elements to enable EAC to monitor network events. However, EAC has not established a continuous monitoring program which requires the organization to regularly review and analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, and take necessary actions based upon the results of these reviews.

- The EAC needs to extend its access security controls to include network devices attached to the agency's internal network. EAC relies on external access controls and physical access controls to its workplace, and has not implemented additional required controls to prohibit access to network devices without required identification and authentication controls in place.

EAC officials provided a written response to the draft report dated September 30, 2009. In that response, EAC officials generally agreed with the issues in the report and advised that they have established a high-level POA&M which, when implemented over FY 2010, will enable compliance in every FISMA control area.

FINDINGS AND RECOMMENDATIONS

1. IT Security Program Improved but Additional Controls are Necessary

The U.S. Election Assistance Commission (EAC) has begun to take actions to address the IT security deficiencies that were reported in the 2008 FISMA report. While many corrective actions are underway or planned, EAC has not fully corrected all weaknesses that impact its IT security program. We attributed this condition, in part, to the absence of management officials with IT security program expertise. As a result, EAC is not in full compliance with the requirements of the Financial Information Systems Management Act (FISMA).

As part of our evaluation, we assessed whether EAC's agency-wide IT security program was in substantial compliance with each of the security control areas established by Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information System*. For each control area, we determined whether the EAC was either in substantial compliance (SC), partial compliance (PC), or not in substantial compliance (NSC). The table below shows our determinations.

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

FIPS 199, *Standards for Security Categorization of Federal Information and Information System,* provides that policies and procedures play an important role in the effective implementation of an enterprise-wide information security program, and the success of the resulting security measures employed to protect an agency's information and information systems. FIPS 199 provides that organizations must develop and promulgate formal, documented policies and procedures governing the minimum security requirements set forth in this standard, and must ensure their effective implementation.

NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, provides that agencies must categorize their information and information systems under the requirements of FIPS 199. Security categorization is accomplished as an organization-wide activity with the involvement of senior-level organizational officials. As required by FIPS 200, organizations use the security categorization results to designate information systems as low-impact, moderate-impact, or high-impact systems. For each information system, the agency must meet recommended minimum security controls, as applicable to their operations.

NIST SP 800-53 stresses that information obtained during the agency-wide risk assessment facilitates the selection of security controls including supplementing the minimum controls contained in this document. NIST SP 800-53 provides the minimum security requirements covering seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems.

We based our determination on EAC's compliance with each of the above security control areas by assessing the IT security policies and procedures EAC had drafted, testing selected minimum control requirements identified in NIST SP 800-53, and reviewing IT security documentation provided by EAC's service provider for most of the agency's general support system security and operational requirements.

EAC in response to the IT security weaknesses reported in the 2008 FISMA report developed a detailed Plan of Action and Milestone (POA&M) to address each of the report's findings and recommendations. We performed tests to determine whether EAC had corrected the weaknesses or had actions underway to correct them. As noted in a subsequent finding, we determined that EAC had addressed or was in the process of addressing many of the problems. However, due to the extent of the problems noted in the prior report, the EAC had not yet corrected several problem areas. Our tests noted additional control weaknesses that were not previously identified.

Recommendations

1. Establish an overall comprehensive plan of action and milestone (POA&M) document, with target dates for completion of corrective actions, to address the problems noted in this report. Assure that the plan is monitored on a monthly basis and updates provided to the commissioners.

2. Provide sufficient specialized training to EAC personnel to enable EAC to develop and maintain a risk-based IT security program that meets FISMA requirements, or hire an official that has experience managing an agency-wide IT security program.

3. Establish a continuous monitoring program to address the NIST 800-53 requirements.

Agency Response

EAC officials advised that the agency has already developed an overall POA&M which includes target dates for completion of key corrective actions. EAC officials also advised that the agency has appointed a Privacy Officer, and will initiate a search for a full-time CIO. Further, these officials indicated that procedures will be developed to ensure that a continuous monitoring program is developed within EAC.

Auditor Comments

The agency has agreed to take action to address each recommendation.

2. EAC has Taken Actions on Prior Deficiencies but Weaknesses Remain

As part of our evaluation, we tested the actions that EAC took to address the weaknesses identified in EAC's 2008 FISMA report. The 2008 evaluation report concluded that EAC had not established an IT security program, and had not been proactive in monitoring security controls in order to strengthen EAC's IT security program.

Our tests disclosed that, prior to the start of our 2009 evaluation; EAC began to develop an overall strategy to address the problems impacting the IT security program. EAC contracted with a firm to assist in developing an overall plan to address the IT security program weaknesses, and to assist in the development of specific corrective action plans. The actions taken by EAC included, among others:

- Drafting an IT security program handbook that provides outlines EAC's IT security program, and identifies selected specific control processes;
- Developing an IT management structure that includes hiring a full-time Chief Information Officer;
- Implementing actions to develop PII controls; and
- Conducting a comprehensive risk assessment.

The following table summarizes the problems noted in the 2008 FISMA report, and our determination of whether the actions taken by EAC were sufficient to substantially correct the problems. For those problems that continue, we have noted what corrective actions EAC has taken or planned to address them.

Issue	Auditor Conclusions	Actions Taken by EAC
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.	**Partially Addressed.** EAC has drafted an IT security handbook, but has not yet started to develop the detailed operational policies required to implement the controls required by FISMA, or identified in the draft handbook. EAC needs to implement additional actions before this issue is fully addressed. EAC is developing a management structure, but has not yet fully implemented the plan.	EAC is developing an agency-wide IT security program, and has taken some actions to address program weaknesses, and has other actions planned. EAC is developing an IT management structure, and is planning to hire a full-time Chief Information Officer. Other management structure changes are on hold until this position is filled.
A Certification & Accreditation (C&A) and formal Risk assessment, security plan or Security Test and Evaluation of EAC's local area network and website general support system has not been completed or developed.	**Resolved.**	

EAC is not fully compliant with several Privacy Act Requirements including: 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.	**Partially Addressed.** Until EAC completes actions underway, and implements controls required by OMB directives on PII and the Privacy Act, EAC remain s not in full compliance with several OMB directives dealing PII, and the Privacy Act.	EAC has appointed a privacy officer, and has identified those systems, both manual and automated, that house PII data. EAC has several actions underway that will address many of the remaining issues.
Weaknesses noted in review of the independent third party information security examinations and inspections, are not monitored by EAC within the GSA POA&M.	**Resolved.**	
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.	**Partially Addressed.** EAC has made progress in this area, however, EAC needs to finalize its IT security handbook, and develop operational directives before it fully addresses this problem area fully.	EAC will issue a handbook on EAC IT security controls in the near future. EAC also plans to develop additional operational directives to implement established IT security controls.
A formal incident response capability has not been established.	**Resolved.**	
A Continuity of Operations Plan, Disaster Recovery Plan, or Business Impact Assessment has not been developed.	**Problem Continues.**	EAC has not yet addressed this issue.
EAC does not have an inventory of all the systems or applications used by GSA to support the operations of EAC, or formally identified major applications and general support systems.	**Resolved.**	

Since recommendations are made in other findings, we are not making any recommendations for this issue.

3. IT Security Policies and Procedures Should be Finalized

IT security policies and procedures, which form the basis for a risk-based IT security program, have not yet been completed. EAC issued a draft IT security handbook; however, the document needs to be finalized and detailed operational procedures need to be developed in order to fully meet this key FISMA control requirement. As a result, EAC incurs unnecessary risk until security policies and procedures are developed and implemented.

NIST SP 800-53 requires organizations to develop, disseminate, and periodically review and update a formal control policy that addresses purpose, responsibilities, coordination among organizational entities, and criteria for achieving compliance in each of seventeen IT control areas identified in FIPS 200. NIST SP 800-53 also provides that policies and procedures that are based on risk assessments cost-effectively reduce information security risks to an acceptable level and address information security throughout the life cycle of each organizational information system.

As noted above, EAC developed an "Information Security Policy Handbook". The handbook outlines EAC's agency-wide IT security program, and identifies selected controls that EAC will follow in its security program. The handbook provides guidance, among others, in the following areas:

- Scope. The handbook provides that policies apply to every individual, organization, and information system that processes or handles EAC-owned information.
- Management Controls. The handbook provides guidance on risk management, required monitoring requirements, and other management control areas identified in NIST SP 800-53.
- Operational Controls. The handbook provides guidance on personnel security requirements, contingency planning requirements, and other operational control areas identified in NIST SP 800-53.
- Technical Controls. The handbook identifies the technical control security policy statements for EAC systems. Areas addressed include policies on access controls, including remote access, and other technical control areas indentified in NIST SP 800-53.

We reviewed the draft handbook to determine whether it substantially met the requirements contained in NIST SP 800-53. We found that the handbook provides a high level overview of EAC's IT security program objectives, and provides specific IT security control requirements. Overall, we concluded that the handbook met the requirements, except for the need to develop specific operational details that are needed to implement the policy directives.

Recommendation

Finalize the EAC IT security handbook, and establish a process to identify and document necessary operational processes to enable personnel to meet the control requirements contained in the handbook, and applicable NIST control requirements.

Agency Response

EAC officials advised that they will finalize the handbook, and will develop written operational procedures.

Auditor Comments

The agency proposed actions that when implemented should address the audit recommendation.

4. Completion of Contingency Planning and COOP Development Should be a High Priority

EAC has not completed the required contingency planning for its information systems, which are part of an overall organizational program for achieving continuity of operations for mission/business operations during an emergency. We attributed this issue to the need for a security officer with expertise in managing an agency-wide IT security program. As a result, until EAC completes necessary contingency planning, COOP development, and implements actions to mitigate the identified risks, EAC incurs an unnecessary risk of disruption to its operations.

NIST SP 800-53 requires that an organization should develop a contingency plan for the information system that:

- Identifies essential missions and business functions and associated contingency requirements, and provides recovery objectives, restoration priorities, and metrics.
- Addresses contingency roles, responsibilities, assigned individuals with contact information, and addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure.
- Establishes timeframes for periodic review of the contingency plan, revises the contingency plan to address changes to the organization, information system, or environment; and any problems encountered during contingency plan implementation, execution, or testing.
- Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions.

Our tests of this critical control area found that EAC backs up its general support system records daily and maintains copies of these records indefinitely. We also determined that EAC contracts with the General Services Administration (GSA) as a service provider for its core network operations. Therefore, EAC does obtain contingency operational controls for aspects of its network provided by the service provider. However, our evaluation noted that EAC has not sufficiently addressed other critical operational processes that are necessary to meet its contingency of operations objectives, as required by NIST SP 800-53 and related NIST documents. In addition, we were not provided any documentation to support that the EAC had completed critical functions required by Continuity of Operations planning to ensure it can continue to accomplish critical mission functions during an event that requires use of contingency or COOP plan.

Recommendation

Assign a high priority to the completion of required contingency plans and COOP documents.

Agency Response

EAC officials advised that the agency will develop required contingency plans and COOP documents once the risk assessment process has been completed.

Auditor Comments

The agency proposed actions that when implemented should address the audit recommendation.

5. FDCC Requirements Need to be Implemented

EAC has not fully implemented Federal Desktop Computer Configuration (FDCC) that OMB first mandated in 2007. As required by OMB, NIST has issued guidance that provides mandatory configuration requirements for desktops that run a windows operating system. These configurations eliminate known computer security vulnerabilities.

The FDCC configuration contains numerous settings and configuration requirements. In order to determine whether EAC had implemented the FDCC requirements, we selected several requirements dealing with password configuration, and compared them to the current EAC settings. Details of our review follow:

FDCC Requirement	LSC Comments
Account lockout - 15 minutes	EAC meets or exceeds requirement.
Account lockout threshold - 5 invalid attempts	EAC meets or exceeds requirement.
Reset at 15 minutes	EAC meets or exceeds requirement.
Passwords remembered - 24	EAC does not meet requirement.
Maximum password age - 60 days	EAC does not meet requirement.
Minimum password age - 1 day	EAC meets or exceeds requirement.
Password length - 12 characters	EAC does not meet requirement.
Password complexity enabled	EAC meets or exceeds requirement.
Store password using reversible encryption disabled	EAC meets or exceeds requirement.

As discussed above, the FDCC contains substantial numbers of other required configuration requirements that are mandated to be followed by agencies. We discussed FDCC implementation with EAC IT personnel, and were advised that the service provider has provided a new "image" that meets FDCC requirements. However, implementation is being delayed until further testing, and other administrative actions are completed. EAC officials advised us that changes to the password requirements have been revised to meet FDCC requirements.

Recommendation

Implement the minimum password settings for the network. Ensure that other FDCC mandatory configuration settings are established as soon as possible.

Agency Response

EAC officials advised that the agency has already changed the minimum password settings, and agreed to implement FDCC settings once an on-going legal issue is resolved.

Auditor Comments

The agency proposed actions that when implemented should address the audit recommendation.

6. Access Controls and Remote Access Need Strengthening

EAC's access controls, including remote access to EAC's network do not fully meet FISMA requirements. As a result, EAC's information and information systems incur unnecessary risk of unauthorized access.

NIST SP 800-53 requires that agencies implement the following minimum control requirements:

- The organization uses cryptography to protect the confidentiality and integrity of remote access sessions, and the encryption strength of mechanism is selected based on the security categorization of the information.
- The information system routes all remote accesses through a limited number of managed access control points.
- The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.
- The organization ensures that remote sessions for accessing critical security functions and security-relevant information employ additional security

We tested selected control requirements for access controls including remote access through dial-up methods. In addition, we performed tests to determine whether EAC met requirements established by OMB over remote access for devices that contain or access sensitive Personal Identifying Information (PII).

Our tests identified that the EAC had not yet established a policy to require that system administrator's periodically change their passwords. Since administrators have significant authorities in a system, individuals should be required to change these passwords at required intervals. In addition, EAC needs to maintain documentation of specific user access authorities granted, along with the supervisory concurrence that this access is necessary for the individual to accomplish his/her job. We also found that the EAC was not able to perform the required minimum control requirement to review and recertify the user's access authorities at least annually.

In addition, we found that EAC has not yet implemented the security control mandated by OMB that remote devices that will access or store PII data must have two-factor authentication, and one of the factors must be a device separate from the computer gaining access. In addition, OMB requires that agencies encrypt on all data on mobile computers if storing or accessing PII data.

Recommendation

Implement access controls required by FISMA, including controls over all remote access methods, and OMB guidance on securing PII data.

Agency Response

EAC officials advised that the agency will work to address security over dial-up access, and will work to implement two-factor authentication.

Auditor Comments

The agency proposed actions that when implemented should address the audit recommendation.

7. Security Risk Assessments Need to be Finalized and Used to Develop Controls

EAC has not finalized required assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. As a result, EAC is not yet able to develop risk-based controls that take into account vulnerabilities, and threat sources.

NIST SP 800-53 provides that an effective information security program should include periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization. Risk assessments also include periodic vulnerability scanning of information systems.

During our evaluation, EAC provided a draft risk assessment to us. However, we did not perform detailed tests of this document to determine if it met NIST requirements because we received it after completion of our testing. We also performed tests to determine whether EAC performed periodic vulnerability scanning of its information systems, including workstations attached to its network. We found that EAC's service provider performed periodic vulnerability scans of the network and workstations. We also found that the service provider updates and applies security patches to existing software periodically.

Recommendation

Finalize the risk assessment, and ensure it is used to develop risk-based controls, and as a starting point for development of contingency plans and COOP documents.

Agency Response

EAC officials advised that the agency will work to finalize the risk assessment, and will include a comprehensive review of threats and vulnerabilities to EAC systems.

Auditor Comments

The agency proposed actions that when implemented should address the audit recommendation.

8. EAC Has Made Progress Towards Compliance with PII and Privacy Act Requirements

Although EAC has actions underway to meet many of the OMB PII directives, additional actions are necessary to comply with Federal privacy requirements. As a result, EAC is not in full compliance with regulations and requirements in these areas.

We tested EAC's adherence to PII directives issued by OMB, and other privacy requirements. The details of our tests follow:

OMB Guidance	Requirement	EAC Actions	Comments
M-07-16, dated May 22, 2007	Requires agency to develop and implement a breach notification policy by November 2007. Includes all systems and paper documents.	EAC has a draft document and expects to publish it in the next few months.	EAC is not in full compliance with this area.
	Requires agency to review existing requirements to ensure meet all security and privacy requirements.	EAC has completed this review.	EAC provided us with documentation, and we determined that EAC meets this requirement.
	Review current PII holdings and determine if holdings are accurate, relevant and reduce the PII holdings to minimum necessary. Agency specific review plans and progress reports were to be included in FISMA reports.	EAC has compiled a listing of systems with PII information. EAC is developing plans to address what PII holdings it can eliminate.	EAC is not in full compliance with this area.
	Following initial review, publish a schedule for which the agency will periodically review holdings.	EAC has notice ready, but has not yet issued the document. EAC advised that the document is undergoing legal review.	EAC is not in full compliance with this area.
	Review agency use of social security numbers in agency systems to identify any unnecessary collection and use of social security numbers. Establish plan, based upon this review, within 120 days of memo to eliminate collection or use of social security numbers. Elimination of unnecessary collection or use within 18 months.	The EAC is looking at ways to reduce any unnecessary collection of social security numbers.	EAC is not in full compliance with this area.

	Encrypt on all data on mobile computers.	Not yet implemented	EAC is not in full compliance with this area.
	Require two-factor authentication.	Not yet implemented	EAC is not in full compliance with this area.
	Require time out function for remote computing.	EAC has implemented this control.	Our tests support that this control implemented.
	Require all personnel with access to PII to sign at least annually a document that describes rules of behavior on PII and clearly describes the person's responsibilities. This rule must include the consequences and corrective actions for failure to follow rules on PII.	A draft letter has been prepared, but has not yet been issued.	EAC is not in full compliance with this area.
	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.	A draft letter has been prepared, but has not yet been issued.	EAC is not in full compliance with this area.
	Develop a breach notification plan addressing the elements in the OMB guidance.	Not yet published, but have a draft that is being cleared.	EAC is not in full compliance with this area.
OMB Circular A-130	Review biennially each system of records notice to ensure that it accurately describes the system of records.	Not yet accomplished.	EAC is not in full compliance with this area.

Recommendation

Monitor ongoing actions to ensure that compliance with OMB PII guidance and Privacy Act requirements are completed expeditiously.

Agency Response

EAC officials advised that the agency has drafted several policies related to the protection of PII data, and will continue to work to ensure full compliance with requirements.

Auditor Comment

The agency proposed actions that when implemented should address the audit recommendation.

9. Establish Controls to Ensure Audit and Accountability

EAC's system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, the outcomes of the events, and tracks sufficient elements to enable EAC to monitor network events. However, EAC has not yet established a continuous monitoring program which requires the organization to regularly review and analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions based upon the results of these reviews.

NIST SP 800-53 requires that the agency establish a control that the information system alerts appropriate organizational officials in the event of an audit processing failure and takes appropriate actions to address the problem. In addition, the agency should regularly review and analyze information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Our tests found that EAC has not yet implemented the required minimum controls that the information system alert appropriate organizational officials in the event of an audit processing failure and implements the organization-defined actions to be taken, such as shutting down the information system. In addition, EAC does not employ automated mechanisms to alert security personnel of the inappropriate or unusual activities with security implications defined by EAC, as required by NIST requirements.

Recommendation

Establish controls over the audit logs maintained to ensure that the system is capable of providing required alerts. Ensure that periodic reviews are made of the logs to identify any unusual activity, other concerns or problems.

Agency Response

EAC officials advised that the agency will develop a procedure relating to audit logs, and will strengthen actions in this area.

Auditor Comments

The agency proposed actions that when implemented should address the audit recommendation.

10. Restrict Access to Network Devices

EAC needs to extend its access security controls to include network devices attached to the agency's internal network. EAC relies on external access controls and physical access controls to its workplace, and has not yet implemented additional required controls to prohibit access to network devices without required identification and authentication controls in place. As a result, EAC allows anyone within its physical office boundaries to access network devices (printers, copiers and other devices attached to the network) without identification and authorization controls being employed.

NIST SP 800-53 provides that access control policies and associated access enforcement are employed by organizations to control access between users and objects (e.g., devices) in the information system.

The FEC has external risk-based protection to its information and information systems through its service provider's (GSA) security controls, and our tests of several key IT security controls have found that the service provider's controls met FISMA requirements. Although EAC has implemented external IT controls and physical security controls, the U.S. CERT and other entities have reported that vulnerabilities in network printers have allowed malicious computer hackers to attack networks. If EAC implemented required access controls over these devices, EAC would further decrease the risk to its information and information systems.

Recommendation

Ensure that access controls are implemented for all EAC network devices.

Agency Response

EAC officials advised that the agency intends to implement controls to address this problem.

Auditor Comments

The agency proposed actions that when implemented should address the audit recommendation.

U. S. ELECTION ASSISTANCE COMMISSION
OFFICE OF THE EXECUTIVE DIRECTOR
1225 New York Avenue, NW, Suite 1100
Washington, DC. 20005

September 30, 2009

Memorandum

To: Curtis W. Crider
Inspector General

From: Thomas R. Wilkey
Executive Director

Subject: Management Response to Draft Evaluation Report-U.S. Election Assistance Commission Evaluation of Compliance with the Requirements of the Federal Information Security Management Act Fiscal Year 2009 (Assignment No. 1-EV-EAC-02-09)

This is in response to your Memorandum dated September 17, 2009 wherein you requested a written response to the findings associated with the above mentioned Draft Evaluation Report. As you have requested, the attached PDF document indicates Management's support for agreement or disagreement with the results of the evaluation.

Further attached is a 2009 FISMA High-level POA&M.

If you have any questions please feel free to contact me.

Attachment

SERIAL#	2009 FISMA Auditor Recommendation	EAC Management Response
1.1	Establish an overall comprehensive plan of action and milestone (POA&M) document, with target dates for completion of corrective actions, to address the problems noted in this report. Assure that the plan is monitored on a monthly basis and updates provided to the commissioners.	EAC has already developed an overall POA&M, which includes target dates for completion of key corrective actions. EAC is already working with a contractor to implement several corrective actions, and the contractor is required to keep EAC management closely informed of all progress.
1.2	Provide sufficient specialized training to EAC personnel to enable EAC to develop and maintain a risk-based IT security program that meets FISMA requirements, or hire an official that has experience managing an agency-wide IT security program.	EAC will initiate a search for a full-time CIO, who may also serve as SAISO, Chief Privacy Officer, and information security evangelist. EAC has appointed a Privacy Officer, who will work with the CIO to ensure that PII risk is properly addressed by the EAC information security program. EAC will finalize information security roles and responsibilities across the organization once the CIO position has been filled.
1.3	Establish a continuous monitoring program to address the NIST 800-53 requirements.	All operational procedures developed for information security at EAC will facilitate continuous monitoring of EAC information systems and security controls. In particular, procedures for change management, configuration management, audit log monitoring, network monitoring, patch management, risk management, and vulnerability scanning will facilitate continuous monitoring.
3	Finalize the EAC IT security handbook, and establish a process to identify and document necessary operational processes to enable personnel to meet the control requirements contained in the handbook, and applicable NIST control requirements.	EAC will finalize and disseminate the information security policies handbook through the organization. EAC information owners and IT staff will develop, implement, and periodically review written operational procedures that specify how to implement the controls required to satisfy EAC's information security policy objectives in every FISMA control area.
4	Assign a high priority to the completion of required contingency plans and COOP documents.	EAC will develop a BIA and DRP, and develop and test a COOP, once the current risk assessment has been reviewed by information owners, and major policies, procedures, and controls have been finalized and implemented.
5	Implement the minimum password settings for the network. Ensure that other FDCC mandatory configuration settings are established as soon as possible.	Minimum password settings for the network have already been implemented. Due to an ongoing legal matter, EAC is unable to re-image any computers at any time. Once this matter has been resolved, EAC will develop a reimaging schedule, present this schedule to appropriate supervisors, and then reimage computers as per this schedule.

6	Implement access controls required by FISMA, including controls over all remote access methods, and OMB guidance on securing PII data.	EAC will work with GSA to disable dialup remote access or, at a minimum, grant dialup access only on an as-required and/or contingency basis. EAC will re-initiate conversations with GSA and develop a timeline for the implementation of two-factor authentication for securing remote access to PII, possibly using HSPD-12 Employee ID badges for all portable computers.
7	Finalize the risk assessment, and ensure it is used to develop risk-based controls, and as a starting point for development of contingency plans and COOP documents.	EAC's FISMA contractor will work with EAC information owners to review, refine, and finalize the provisional risk assessment. This will include a comprehensive review of threats and vulnerabilities, a review of the SP 800-53 security controls baseline already developed by the contractor, and separation of controls into common and system-specific controls.
8	Monitor ongoing actions to ensure that compliance with OMB PII guidance and Privacy Act requirements are completed expeditously.	The EAC Privacy Officer has already taken inventory of PII systems and developed several draft policies and procedures related to protection of PII and privacy-related incident response. The 2009 EAC FISMA evaluation provides detailed guidance on areas in which EAC is still only partially compliant with PII and Privacy Act requirements, and EAC will formally adopt the PII recommendations from the FISMA evaluation as a guide to complete compliance.
9	Establish controls over the audit logs maintained to ensure that the system is capable of providing required alerts. Ensure that periodic reviews are made of the logs to identify any unusual activity, other concerns or problems.	EAC IT staff will create a written itemization of every audit log type in use, will work with GSA to both identify and implement appropriate action on audit failures, and will develop a procedure to review these log files monthly and report errors to appropriate supervisors.
10	Ensure that access controls are implemented for all EAC network devices.	EAC intends to implement either a separate, limited-access "visitor" VLAN segment on the EAC network, or else create a completely isolated wireless network for visitor access. In either case, there will be no visitor access to any shared resources on the EAC network, including network devices such as printers, scanners, and copiers.

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
1225 New York Ave. NW - Suite 1100
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
1225 New York Ave. NW - Suite 1100
Washington, DC 20005

E-mail: eacoig@eac.gov

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

FAX: 202-566-0957