U.S. ELECTION ASSISTANCE COMMISSION
OFFICE OF INSPECTOR GENERAL

FINAL EVALUATION REPORT:

United States Election Assistance Commission Federal Information Security Management Act 2008 Independent Evaluation Report

No. I-EV-EAC-01-08
OCTOBER 2008

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

October 31, 2008

Memorandum

To: Chair, U.S. Election Assistance Commission

From: Curtis W. Crider
Inspector General

Subject: Final Evaluation Report – United States Election Assistance Commission Federal Information Security Management Act 2008 Independent Evaluation Report (Assignment No. I-EV-EAC-01-08)

We contracted with the independent certified public accounting firm of Clifton Gunderson LLP (Clifton Gunderson) to conduct the subject evaluation. Clifton Gunderson found that the U.S. Election Assistance Commission (EAC) has made progress in educating users through security and privacy awareness training, and has initiated discussions to develop EAC specific policies related to information system security and privacy. However, additional improvements are needed. The evaluation found that the EAC has not established an information security program and has not been proactive in reviewing security controls and identifying areas to strengthen this program. In addition, the evaluation found that the EAC was not fully compliant with several provisions of the Privacy Act.

Please provide us with your written response to the recommendations included in this report by December 1, 2008. Your response should contain information on actions taken or planned, including target dates and titles of EAC officials responsible for implementing 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.

UNITED STATES ELECTION ASSISTANCE COMMISSION FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

2008 INDEPENDENT EVALUATION REPORT

October 2, 2008

Clifton Gunderson LLP
Certified Public Accountants & Consultants

October 2, 2008

Mr. Curtis Crider
Office of the Inspector General
U.S. Election Assistance Commission
1225 New York Avenue NW, Suite 1100
Washington, DC 20005

Dear Mr. Crider,

We are pleased to provide the fiscal year (FY) 2008 Office of Inspector General (OIG) response to Office of Management and Budget (OMB) Memorandum M-08-21, "FY 2008 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management" and FY 2008 FISMA Independent Evaluation Report, detailing the results of our review of Election Assistance Commission's (EAC) information security program.

FISMA requires Inspectors General to conduct annual evaluations of their agency's security programs and practices, and to report to OMB on the results of their evaluations. OMB Memorandum M-08-21 provides instructions for meeting the FISMA reporting requirements.

We completed our response to M-08-21 based on our independent evaluation as of September 12, 2008, subsequent review through the date of this report of documentation supporting the security program performance statistics reported by EAC management, and review of Plans of Action and Milestones. In preparing our responses, we collaborated with EAC management and appreciate their cooperation in this effort.

EAC management has provided Clifton Gunderson LLP with a response (dated September 30, 2008) to this FISMA 2008 Independent Evaluation Report. Management accepts our findings and recommendations and intends to develop an action plan to address these findings.

We appreciate the opportunity to assist your office with these reports. Should you have any questions please call George Fallon at (301) 931-2050.

Very truly yours,

CLIFTON GUNDERSON LLP

Clifton Gunderson LLP

GFF:sgd

11710 Beltsville Drive
Suite 300
Calverton, MD 20705-3106
tel: 301-931-2050
fax: 301-931-1710

www.cliftoncpa.com

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Title III of the E-Government Act (Public Law No. 104-347), also called FISMA, requires agencies to adopt a risk-based, life cycle approach to improving computer security that includes annual security program reviews, independent evaluations by the Inspector General (IG), and reporting to the OMB and the Congress. It also codifies existing policies and security responsibilities outlined in the Computer Security Act of 1987 and the Clinger Cohen Act of 1996.

Based on the results of our fiscal year (FY) 2008 independent evaluation, we determined that the EAC has not established an information security program and has not been proactive in reviewing security controls and identifying areas to strengthen this program.

The FY 2007 Pre-FISMA Independent Evaluation Report included six findings, two of which were closed in the current year. The four findings that remain open relate to EAC's information system and privacy policies and procedures, agreements with, and oversight of external service providers. EAC has made progress in educating users through security and privacy awareness training, and has initiated discussions to develop EAC specific policies and procedures relating to information system security and privacy.

We are reporting nine findings for FY 2008.

II. BACKGROUND

The EAC was established by the Help America Vote Act of 2002 (HAVA). Central to its role, EAC serves as a national clearinghouse and resource for information and review of procedures with respect to the administration of Federal elections. According to the text of HAVA, the law was enacted to:

> " ... establish a program to provide funds to states to replace punch card voting systems, to establish the Election Assistance Commission in the administration of Federal elections and to otherwise provide assistance with the administration of certain Federal election laws and programs, to establish minimum election administration standards for states and units of local government with responsibility for the administration of Federal elections, and for other purposes."

HAVA requires the EAC to:

- Generate technical guidance on the administration of federal elections.
- Produce voluntary voting systems guidelines.
- Research and report on matters that affect the administration of federal elections.
- Provide information and guidance with respect to laws, procedures, and technologies affecting the administration of Federal elections.
- Administer payments to states to meet HAVA requirements.
- Provide grants for election technology development and for pilot programs to test election technology.
- Manage funds targeted to certain programs designed to encourage youth participation in elections.
- Develop a national program for the testing, certification, and decertification of voting systems. Maintain the national mail voter registration form that was developed in

accordance with the National Voter Registration Act of 1993 (NVRA), report to Congress every two years on the impact of the NVRA on the administration of Federal elections, and provide information to states on their responsibilities under that law.
- Audit persons who received federal funds authorized by HAVA from the General Services Administration (GSA) or the EAC.
- Submit an annual report to Congress describing EAC activities for the previous fiscal year (FY).

Through FISMA, the U.S. Congress showed its intention to enhance the management and promotion of electronic government services and processes. Its goals are to achieve more efficient government performance, increase access to government information, and increase citizen participation in government. FISMA also provides a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. It also codifies existing policies and security responsibilities outlined in the Computer Security Act of 1987 and the Clinger Cohen Act of 1996.

The EAC Office of the Inspector General (OIG) contracted with Clifton Gunderson LLP to conduct EAC's FY 2008 FISMA Independent Evaluation. We performed this evaluation in conjunction with our review of information security controls required as part of the annual financial statement audit.

III. OBJECTIVES

The purpose of this evaluation was to assess the effectiveness of EAC's information security program and practices and to determine compliance with the requirements of FISMA and related information security policies, procedures, standards, and guidelines.

IV. SCOPE & METHODOLOGY

To perform our review of EAC's security program, we followed a work plan based on the National Institute of Standards and Technology (NIST)'s Recommended Security Controls for Federal Information Systems – Special Publication (SP) 800-53 for specification of security controls and NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems and 800-53A Guide for Assessing the Security Controls in Federal Information Systems for the assessment of security control effectiveness, and the Government Accountability Office (GAO)'s Federal Information System Controls Audit Manual (FISCAM: GAO/AIMD-12.19.6), and our general controls review methodology. The combination of these methodologies allowed Clifton Gunderson LLP to meet the requirements of both FISMA and the Chief Financial Officer (CFO)'s Act. In addition, our evaluation was conducted in accordance with the January 2005, *Quality Standards for Inspections*, issued by the President's Council on Integrity and Efficiency.

Our procedures included following-up on recommendations made in the FY 2007 Pre-FISMA Independent Evaluation Report; performing internal and external security reviews of EAC's information technology (IT) infrastructure; reviewing agency Plans of Action and Milestones (POA&Ms); and evaluating EAC's major systems.

We performed procedures to test (1) EAC's implementation of an entity-wide security plan, and (2) operational and technical controls specific to each application such as service continuity, logical access, and change controls. We also performed targeted

tests of controls over financial processing applications and processes. We performed our review from August 1, 2008 to September 12, 2008 at EAC's headquarters in Washington, District of Columbia.

EAC management and staff were very helpful and accommodating throughout this review and assisted us in refining the recommendations. This independent evaluation was prepared based on information available as of September 12, 2008.

V. DETAILS OF RESULTS

A. Prior Year Results

The FY 2007 Pre-FISMA Independent Evaluation Report identified six findings, reported as other weaknesses (i.e., not significant to be reported as a significant deficiency in accordance with OMB classification guidelines). The following table summarizes the findings reported in FY 2007 and their current status.

#	Title	Current Status
FY07-01	EAC does not have an inventory of all the systems/applications used by GSA to support the operations of EAC. GSA utilizes a suite of applications for the various services it provides EAC, like CHRIS for HR management and Pegasys®, a commercial-off-the-shelf product for financial management and reporting.	Open
FY07-02	The Memorandum of Understanding (MOU) does not provide guidance on EAC's responsibilities with respect to data integrity and completeness. EAC prepares manual vouchers and transmits these to GSA for input. The responsibilities of each party are not spelled out in the MOUs. We did not see evidence of the existence of an Interconnection Security Agreement (ISA) or evidence that the EAC concerns were addressed in a timely manner by the service provider.	Closed
FY07-03	EAC has not developed any policies or procedures for information security or privacy management. Per the terms of the MOU, the GSA procedures will prevail where there are no guiding policies provided by the user organization.	Open
FY07-04	There is no evidence that employees and contractors of EAC have received Security Awareness Training.	Closed
FY07-05	Only the OIG and its contractors have signed the Rules of Behavior Governing Acceptable Use of Federal Information System Resources policy.	Closed

#	Title	Current Status
FY07-06	Inadequacies were noted related to personnel security practices at EAC's service provider (GSA). The GSA OIG has reported several cases of non-compliance with background investigations for GSA's contract personnel supporting GSA systems. This weakness may potentially impact the integrity of EAC systems.	Open

B. Current Year Results

In FY 2008, EAC addressed our recommendation related to security awareness training by rolling out a separate privacy and information security training course which includes a test of the user's knowledge of key concepts, a minimum passing score and mandate to complete the course and provide the completion certificate to management.

We identified six new findings during the FY 2008 review within the following table summary.

Finding Number	Title	Comments
FY08-01	An agency-wide information security program in compliance with FISMA, has not been developed.	None
FY08-02	A security management structure with adequate independence, authority, and expertise which is assigned in writing has not been implemented.	None
FY08-03	A Certification and Accreditation (C&A), formal Risk Assessment, security plan or Security Test and Evaluation (ST&E) of its local area network and website general support systems has not been completed/developed.	None
FY08-04	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 has not been designated - EAC has not identified systems housing personally identifiable information or conducted related Privacy Impact Assessments (PIA's) as required by OMB Memorandum 06-16, Requirements for Protecting Personally Identifiable Information. - EAC has not developed formal policies that address the information protection needs associated with personally identifiable	None

Finding Number	Title	Comments
	information (PII) that is accessed remotely or physically removed.	
FY08-05	Weaknesses noted in our review of the independent third party information security examinations and inspections, are not monitored by EAC within the GSA POA&M.	Repeat of prior year finding FY07-06
FY08-06	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 no guiding policies provided by the user organization.	Repeat of prior year finding FY07-03
FY08-07	A formal incident response capability has not been established.	None
FY08-08	A Continuity of Operations Plan (COOP), Disaster Recovery Plan (DRP) or Business Impact Assessment (BIA) has not been developed.	None
FY08-09	EAC does not have an inventory of all the systems/ applications used by GSA to support the operations of EAC, or formally identified major applications and general support systems.	Repeat of prior year finding FY07-01

The details of our findings and recommendations follow.

VI. FINDINGS AND RECOMMENDATIONS

FY08-01 An agency-wide information security program in compliance with FISMA, has not been developed.

Based upon discussions with EAC management and review of provided documentation we determined that EAC has not developed, documented or implemented the following in accordance with FISMA:

- 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 agency;

- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system;

- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;

- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;

- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency;

- Procedures for detecting, reporting, and responding to security incidents; and,

- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. We determined a disaster recovery plan is in development.

The E-Government Act (Public Law 107-347) Title III, entitled FISMA, requires each federal agency to develop, document, and implement 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. The information security program must 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 agency;

- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system;

- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;

- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the agency) of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks;

- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;

- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency;

- Procedures for detecting, reporting, and responding to security incidents; and,

- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

OMB Circular No A-130 Appendix III states: 'Agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications'.

NIST Special Publication 800-18 states:' All information systems must be covered by a system security plan and labeled as a major application or general support system'.

Recommendation
We recommend EAC management continue ongoing efforts and implement a formal agency-wide security program plan in line with OMB A-130 Appendix III, NIST Special Publication 800-18 and FISMA.

EAC Management's Response
Currently, EAC has procured a contractor to assist with the agency's strategies to become compliant with OMB A-130, NIST special Publication 800-18 and FISMA. These measures include completion of a certification and accreditation of support systems, System Security Plans and practices and procedural guides and documentation that will address the following issues noted in the condition above:

- Periodic assessments of risks
- Policies and procedures that are based on risk assessments
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency
- Procedures for detecting, reporting, and responding to security incidents
- Plans and procedures to ensure continuity of operations
- Subordinate plans for providing adequate information security for Support systems

Though EAC's process is informal considering the lack of documentation and procedural guides, a contingency plan exists for GSA systems which include EAC. As a result, EAC would be effectively operational in the event of a minor or major disaster. EAC currently has a draft of recommendations for a COOP plan which will be addressed during the agencies efforts to be in compliance with OMB Circular A-130, NIST special Publication 800-18 and FISMA.

In the event of a security incident, EAC follows GSA's CIO-IT Security-01-02 in the Handling IT Security Incidents Procedural Guide.

FY08-02 A security management structure with adequate independence, authority, and expertise has not been implemented.

OMB Circular No A-130 Appendix III states: 'Assign responsibility for security in each system to an individual knowledgeable in the information technology used in the system and in providing security for such technology'.

'For each system, an individual should be a focal point for assuring there is adequate security within the system, including ways to prevent, detect, and recover from security problems. That responsibility should be assigned in writing to an individual trained in the technology used in the system and in providing security for such technology, including the management of security controls such as user identification and authentication.'.

Recommendation
We recommend EAC management assign responsibility for the security management function to an individual with the oversight responsibility over the security management structure. The individual should have the expertise and independence to enforce security policies.

EAC Management's Response
GSA provides IT infrastructure support systems and services to the EAC. Within this support provided, EAC adheres to all rules, laws, policies, regulations, guidelines and plans set forth by GSA. EAC has not documented nor has formally implemented a security management structure or assigned any security roles. EAC operates within GSA's security controls. In the lack thereof, EAC has authorized an on site IT specialist to work with GSA to address security issues. Due to limited human resources, we have not been able to monitor GSA's security structure and plan. To address staffing and role assignment issues, EAC has strategically engaged in the process of having a contractor recommend and assist with the delegation and designation of security roles. EAC has also interviewed for a position in the IT division.

Currently, EAC is in the process of having a contractor assist with the Agency's strategies to become compliant with OMB A-130, NIST special Publication 800-18 and FISMA. This will include completion of a C&A of support systems, System Security Plans and Practices and procedural guides and documentation.

FY08-03 A Certification and Accreditation (C&A), formal Risk Assessment, security plan or Security Test and Evaluation (ST&E) of its local area network and website general support systems has not been completed/developed.

NIST Special Publication 800-37 requires agencies to perform certification and accreditation of its major applications or general support system at least once every three years or when there is a significant change in the IT operating environment.

A C&A is required for all Federal information systems as indicated within Section 3544(b)(3) of FISMA. This section refers to "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems" and does not distinguish between major or other applications.

Supplementing the above considerations, mandatory *NIST Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems*, defines security categories for information systems based on potential impact on organizations or individuals should there be a breach of security—that is, a loss of confidentiality, integrity (including authenticity and non-repudiation), or availability. FIPS 199 security categories can play an important part in defining accreditation boundaries by partitioning the agency's information systems according to the criticality or sensitivity of the systems and the importance of those systems in accomplishing the agency's mission. The partitioning process facilitates the cost-effective application of security controls to achieve adequate security commensurate with the mission/business functions being supported by the respective information systems.

NIST Special Publication 800-53 Rev 2 (RA-3) states: 'The organization conducts 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 (including information and information systems managed/operated by external parties)'.

Recommendations
We recommend EAC management:

- Continue with ongoing efforts and conduct certification and accreditation of its general support system.
- Implement a risk assessment policy to require risk assessments to be performed periodically or when there is a significant change in the IT operating environment.

EAC Management's Response
In agreement, EAC has not performed the following on its local area network and website general support:

1. Certification and Accreditation (C&A)
2. Formal risk assessment

3. Security plan
4. System Testing & Evaluation

The website and local area network are supported by two different parties. The LAN is supported by GSA and the website is supported by Humanitas, a contracted company.

GSA provides IT infrastructure support services to the EAC. Within this support provided, EAC adheres to all rules, laws, regulations and plans set forth by GSA.

Currently, EAC is in the process of procuring a contractor to assist with the completion of a C&A that addresses all four issues mentioned above. Documentation was provided to CG on this.

In section 10 of GSA Responsibilities in the MOU between GSA and EAC, it indicates that EAC will fall under the FY08 System Security Plan (SSP) for GSA. Though EAC currently does not have an SSP of it's own, it informally has one via GSA's SSP.

FY08-04 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 has not been designated.**
- **EAC has not identified systems housing personally identifiable information or conducted related PIA's.**
- **EAC has not developed formal policies that address the information protection needs associated with PII that is accessed remotely or physically removed.**

We reviewed EAC's compliance with privacy protection of PII and determined that EAC has temporarily assigned Privacy Officer duties to the Human Resource Specialist.

We noted the 2008 FISMA Review performed for the GSA does not specify which systems were covered by this review. The FISMA template lists GSA systems by region and bureau [rather than by the system name] making it difficult to determine if EAC supported systems were part of this review. EAC does not have an inventory of systems covered by the FISMA evaluation and in which bureau or region these systems are located, or performed a PIA on systems identified as containing EAC PII.

OMB M-06-16 states that: Verify information categorization to ensure identification of personally identifiable information requiring protection when accessed remotely or physically removed. The purpose is to review the Federal Information Processing Standards (FIPS) Publication No. 199 security categorization of organizational information with the focus on remote access and physical removal. The intent is to ensure all personally identifiable information through which a moderate or high impact might result has been explicitly

identified. For example, databases where the loss, corruption, or unauthorized access to personally identifiable information contained in the databases could result in a serious adverse effect, with widespread impact on individual privacy being one area of specific concern.

NIST Special Publication 800-53 Rev 2 (PL-5) states: 'The organization conducts a privacy impact assessment on the information system in accordance with OMB policy'.

OMB Circular M-06-16 'Protection of Sensitive Agency Information' requires agencies to implement organizational policy that addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed'.

We reviewed the critical elements required of government agencies and organizations in FY 2006 and noted EAC 's level of compliance. The following questions were extracted from the Data Collection Instrument issued by the PCIE. For purposes of this assessment, we extracted high-level questions only. Our results are documented in the following table.

Ref	Control Step	Yes, No, Partial, Not Applicable	Clifton Gunderson Comments
Step 1	Has EAC confirmed identification of personally identifiable information protection needs? If so to what level?	Partial	Although EAC has not received an inventory of all systems used by GSA to support he EAC's activities, it has however identified the need to protect all portable computers accessing EAC data. To achieve this goal, management has affirmed that EAC has procured "Credant" encryption software. We noted during the period of our audit that about 70% percent of all EAC computers have been encrypted with the Credent Encryption software. We randomly selected five (5) laptops to determine if they are encrypted. EAC has identified that Pegasys, FMIS and CHRIS are the GSA owned systems that contain EAC's personally identifiable information.
Step 2	Has EAC verified the adequacy of organizational policy? If so, to what level?	Partial	Administrative policies have been developed addressing employee conduct and hiring procedures. However, EAC has still not identified security policies and procedures.

Step 3	Has EAC implemented protections for personally identifiable information being transported and/or stored offsite? If so, to what level.	Partial	See Step 1 above. EAC has procured encryption software to protect information being transported and/or stored off-site; We noted during the period of our audit that approximately 70% percent of all EAC computers have been encrypted with the Credent Encryption software. We randomly selected five (5) laptops to determine if they are encrypted. We noted that EAC issued blackberries are not currently encrypted with the Credent encryption software.
Step 4	Has EAC implemented protections for remote access to personally identifiable information? If so to what level.	Partial	The IG's office has signed the GSA's Riles of Behavior policy establishing acceptable use of government information resources including downloading software, improper web access, etc. EAC's rules of behavior are currently incorporated into the EAC Security Awareness and Privacy Training programs. EAC has not conducted a risk assessment that address the risk associated with download, remote access, or other removal or PII from each system containing PII. Virtual Private Network (VPN) use has been granted to a selected few individuals. We selected a sample of five (5) VPN users to determine if their accesses are appropriately authorized without exception. EAC does not have Plan of Actions and Milestones (PO & M) for developing and implementing protection of sensitive information.
Sect 2.1	Has the Agency encrypted all data on mobile computers/devices which carry agency	Partial	We noted during the period of our audit that approximately 70% of all EAC computers have been encrypted with the Credent Encryption software. We randomly selected five (5) laptops to determine if they are encrypted.

	data unless the data determined to be non-sensitive, in writing by Agency Deputy Secretary or an individual he/she may designate in writing?		We noted that EAC issued blackberries or portable memory sticks are not currently encrypted with the Credent encryption software.
Sect 2.2	Does the agency use remote access with two-factor authentication where of the factors is provided by a device separate from the computer gaining access?	No	We did not see evidence of major steps and milestones directed at implementing two-factor authentication.
Sect 2.3	Does the Agency use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity?	Partial	EAC has implemented a "time-out" function for EAC desktops, laptops and VPN access requiring user re-authentication after 30 minutes of inactivity.
Sect 2.4	Does the Agency log all computer-readable data extracts from databases holding sensitive information and verifies each extract including sensitive data	No Not Applicable	EAC does not own or operate any information systems that contain sensitive information. All identified systems, Pegasys, FMIS and CHRIS are owned and managed by GSA. EAC has not defined which systems should be logged and the nature of activity to be logged and reported by its service provider.

	has been erased within 90 days or its use is still required?		
STEP 5	Has the Agency implemented provisions of OMB M07-16 of May 22, 2007, "Safeguarding Against and Responding to the Breach of PII"	Partial	EAC has not documented procedures to follow when responding to a breach of PII. However, EAC follows GSA policies which require the report of a breach within the first hour after the incident occurred. EAC is also required to fill out a GSA incident report to describe the event and provide any other details.

Recommendations
We recommend EAC management:

1) Designate a Chief Privacy Officer or formally appoint an individual with the responsibility of monitoring and enforcing privacy related policies and procedures. Privacy responsibilities should be added to the position description (PD) of this assigned individual.

2) Develop an understanding of which EAC systems are covered by GSA's FISMA review rotation plan. Consequently, EAC should request from the service provider their systems review rotation schedule and note which systems are covered in each year's rotation. For fiscal years where EAC systems are not covered GSA should grant EAC access to review these systems to comply with FISMA requirements.

3) Develop and implement formal policies that address the information protection needs associated with PII when it is either accessed remotely or physically removed from EAC controlled areas.

EAC Management's Response
1) EAC is currently researching this issue. Due to the fact that the EAC is a small agency with limited human resources and capital, EAC needs to verify that the current 'Acting Privacy Officer' can formally be appointed Chief Privacy Officer due to the multiple roles and assignments that the person formally has.

   Currently, EAC is in the process of formally identifying a Privacy Officer. In the interim, The Human Resources Division informally executes the roles and responsibilities of a Privacy Officer and daily ensures that PII is not compromised.

2) Currently, EAC has procured a contractor to assist with the Agency's strategies to meet compliancy for OMB A-130, NIST special Publication 800-18 and FISMA. This will include completion of a C&A of support systems,

System Security Plans and Practices and procedural guides and documentation. Also, EAC is currently waiting for a reply from GSA on which systems are identified in the FISMA 2008 review.

3) A Privacy Impact Assessment will be completed as EAC moves forward to become compliant with FISMA. This would address compliancy as required by OMB memorandum 06-16, requirements for protecting personally identifiable information (PII).

GSA provides IT infrastructure and some resource support that contains Personally Identifiable Information. EAC adheres to all rules, laws, policies and regulations in regards to the access, handling and protection of personally identifiable information set forth by GSA.

At present, EAC is in the process of procuring a contractor assist with the design construction and implementation of policies to address personally identifiable information.

In 2006, EAC purchased software and server licenses in a joint attempt with GSA to encrypt all workstations and mobile devices. Included in the plan was a pilot test group which EAC users and EAC OIG were to participate in. Before the software and encryption server were deployed, GSA put a stop to the program due to issues found during the testing phase. This issue was addressed when OMB/NIST made changes to the compliancy requirements for vulnerabilities in 2007. GSA was to follow a hardening guide that addressed the found vulnerabilities and apply the changes to their image before February of 2008. In January of 2008, GSA released an image addressing those vulnerabilities and it included encryption software. EAC has updated all but 3 workstations with the latest image provided by GSA which includes the encryption software. The name of the encryption software is credent v5. Currently, all but 3 workstations are encrypted with this software to address PII. The remaining 3 workstations will be completed by 12/15/2008.

FY08-05 Weaknesses noted in our review of the independent third party information security examinations and inspections, are not monitored by EAC within the GSA POA&M. (Re-Issued)

Based upon discussions with management, we determined that EAC does not monitor or follow up on weaknesses noted in third party security examinations within a POA&M.

Based upon a review of the Memorandum of Understanding (MOU) between GSA and EAC (signed 3/6/08), GSA is responsible for making available the FISMA report, FISMA audit action plan and POA&M. The POA&M will be made available on a quarterly basis.

GSA reviews its IT systems in a cyclical manner and systems used to service EAC and other agencies are subject to an annual SAS 70 review.

Based upon our review of the GSA SAS70 "Pegasys Financial Management

System" for the period 7/1/07 through 6/30/08, the following weaknesses were identified:

- Approval for user access was not consistently documented or evidence of the review of operating system failed logins was not available, and multiple exceptions in the effectiveness of logical access controls specifically within the UNIX and Windows server configurations existed.

- One individual had access to the source code as well as the ability to move program changes into the production environment.

Based upon our review of the GSA SAS70 "Payroll Accounting & Reporting System (PAR)" for the period 7/1/07 through 6/30/08, the following weaknesses were identified:

- Documentation of the testing and approval of emergency changes was not completed by the close of the next business day following the change, as required by GSA policy.

- Evidence of approval for specific roles granted to users of the operating system software was not consistently available, and that evidence of testing and approval for operating system software modifications was not consistently available.

In accordance with the provisions of the *OMB, Memorandum M-06-20 dated July 17, 2006,* GSA should perform a complete FISMA review of all systems used in supporting other agencies for these user agencies to meet their FISMA requirement. " ...FISMA requires annual reviews and reporting of all systems, including National Security Systems...". *FISMA Section 3544(b) (5)* " ... all information systems used or operated by the agency or by a contractor of an agency or other organization on behalf of an agency must be tested at least annually..."".

NIST Special Publication 800-53 Rev 2 (CA-5) states: 'The organization develops and updates [Assignment: organization-defined frequency], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system'.

Per FISMA M08-21 guidance, "The agency is responsible for ensuring the contractor corrects weaknesses discovered through self-assessments and independent assessments. Any weaknesses are to be reflected in the agency's POA&M."

"Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract. Agencies must ensure identical, not "equivalent," security procedures. For example, annual reviews, risk

assessments, security plans, control testing, contingency planning, and C&A must, at a minimum, explicitly meet guidance from NIST. "

Agencies and IGs should to the maximum extent practicable, consult with other agencies using the same service provider, share security review results, and avoid the unnecessary burden on the service provider and the agencies resulting from duplicative reviews and re-reviews. Additionally, provided they meet FISMA and policy requirements, agencies and IGs should accept all or part of the results of industry-specific security reviews performed by an independent auditor on the commercial service provider.

In the case of agency service providers, they must work with their customer agencies to develop suitable arrangements for meeting all of FISMA's requirements, including any special requirements for one or more particular customer agencies. Any arrangements should also provide for an annual evaluation by the IG of one agency. Thereafter, the results of that IG evaluation would be shared with all customer agencies and their respective IGs.

Per *FISMA M08-21* guidance, reporting instruction guidance, agency POA&Ms must:

1) Be tied to the agency's budget submission through the unique project identifier of a system. This links the security costs for a system with the security performance of a system.

2) Include all security weaknesses found during any other review done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments. These plans should be the authoritative agency-wide management tool, inclusive of all evaluations.

3) Be shared with the agency IG to ensure independent verification and validation of identified weaknesses and completed corrective actions.

4) Be submitted to OMB upon request.

Recommendations
We recommend EAC management:

- Request from GSA their systems review rotation plan and note which EAC support systems are covered by each rotation [by FY]. For FYs where EAC systems are not covered, GSA should grant EAC access to review these systems to comply with FISMA Section 3544.

- Obtain from GSA its POA&M to address security weaknesses identified in: (1) the SAS 70 review of the Heartland Finance Center; (2) the GSA OIG's 2008 FISMA Report and (3) any other security-related reviews it may have performed on EAC support systems.

EAC Management's Response
Currently, EAC has procured a contractor to assist with the agency's strategies to become compliant with OMB A-130, NIST special Publication 800-18 and

FISMA. These measures include completion of a certification and accreditation of support systems, System Security Plans and Practices and procedural guides and documentation that will address the following issues noted in the condition above:

- Periodic assessments of risks
- Policies and procedures that are based on risk assessments
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency
- Procedures for detecting, reporting, and responding to security incidents
- Plans and procedures to ensure continuity of operations
- Subordinate plans for providing adequate information security for Support systems

FY08-06 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 no guiding policies provided by the user organization. (Re-Issued)

Since the pre-FISMA assessment in 2007, EAC's information security awareness and privacy training programs and content make references to applicable GSA policies (in the absence of corresponding EAC policies and procedures).

The E-Government Act (Public Law 107-347) Title III, entitled the FISMA, requires each federal agency to develop, document, and implement 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. The information security program must 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 agency.

- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system.

Recommendation
We recommend EAC management develop and implement information security policies for EAC. Where GSA policies are used, distribute these policies so employees are aware of their responsibilities and obligations.

EAC Management's Response
Currently, EAC has procured a contractor to assist with the agency's strategies to become compliant with OMB A-130, NIST special Publication 800-18 and FISMA. These measures include completion of a certification and accreditation of support systems, System Security Plans and Practices and procedural guides and documentation that will address the following issues noted in the condition above:

- Periodic assessments of risks
- Policies and procedures that are based on risk assessments
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency
- Procedures for detecting, reporting, and responding to security incidents
- Plans and procedures to ensure continuity of operations
- Subordinate plans for providing adequate information security for Support systems

Though EAC's process is informal considering the lack of documentation and procedural guides, a contingency plan exists for GSA systems which include EAC. As a result, EAC would be effectively operational in the event of a minor or major disaster. EAC currently has a draft of recommendations for a COOP plan which will be addressed during the agencies efforts to be in compliance with OMB Circular A-130, NIST special Publication 800-18 and FISMA.

Additionally, EAC is in the process of having a contractor assist with the design construction and implementation of policies to address personally identifiable information.

In the event of a security incident, EAC follows GSA's CIO-IT Security-01-02 in the Handling IT Security Incidents Procedural Guide.

FY08-07 A formal incident response capability has not been established.

EAC has not established a formal incident response capability. Specifically,

- Formal incident response procedures that clearly define the roles and responsibilities of key parties and users have not been developed;
- A formal incident response team has not been established; and
- EAC does not provide incident response training to users.

We were informed that EAC currently reports all security incidents to GSA and has not developed its own incident response capability. Further, we inspected the EAC security awareness training documentation and noted that EAC system users are not provided training on their incident response responsibilities.

NIST Special Publication 800-61 Computer Security Incident Handling Guide requires agencies to establish an incident response capability to include among

other things, incident response procedures, incident response team and incident response training.

Recommendations
We recommend EAC management:

- Implement a formal incident response policy and procedures in line with NIST 800-61.
- Establish a formal incident response team with defined roles and responsibilities.
- Update the security awareness training documentation to include incident response training.

EAC Management's Response
Currently, EAC has procured a contractor to assist with the agency's strategies to meet compliancy for OMB A-130, NIST special Publication 800-18 and FISMA. This will include completion of a C&A of support systems, System Security Plans and Practices and procedural guides and documentation that will address the following issues noted in the condition above:

- Periodic assessments of risks
- Policies and procedures that are based on risk assessments
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency
- Procedures for detecting, reporting, and responding to security incidents
- Plans and procedures to ensure continuity of operations
- Subordinate plans for providing adequate information security for Support systems

Though EAC's process is informal by not having documentation and procedural guides, a contingency plan exists for GSA systems which include EAC. As a result, EAC would be effectively operational in the event of a minor or major disaster. EAC currently has a draft of recommendations for a COOP plan which will be addressed during the agencies efforts to be in compliance with OMB Circular A-130, NIST special Publication 800-18 and FISMA.

In the event of a security incident, EAC follows GSA's CIO-IT Security-01-02 in the Handling IT Security Incidents Procedural Guide.

FY08-08 A Continuity of Operations Plan (COOP), Disaster Recovery Plan (DRP) or Business Impact Assessment (BIA) has not been developed.

*NIST Special Publication 800-34 r*equires agencies to conduct business impact analysis to identify and prioritize critical IT systems and components prior to developing a contingency plan.

NIST Special Publication 800-53 Rev 2 Information Security (CP-2) states: "The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel".

Presidential Decision Directive 67 (PDD 67) among other things requires federal agencies to develop Continuity of Operations Plans for essential operations.

Recommendations
We recommend EAC management:

- Conduct and document a formal business impact analysis to identify and prioritize critical IT systems and components.
- Finalize and approve the draft contingency and continuity of operations plan and ensure that the plan is tested periodically.

EAC Management's Response
Currently, EAC has procured a contractor to assist with the agency's strategies to become compliant with OMB A-130, NIST special Publication 800-18 and FISMA. This will include completion of a C&A of support systems, System Security Plans and Practices and procedural guides and documentation that will address the following issues noted in the condition above:

- Periodic assessments of risks
- Policies and procedures that are based on risk assessments
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency
- Procedures for detecting, reporting, and responding to security incidents
- Plans and procedures to ensure continuity of operations
- Subordinate plans for providing adequate information security for Support systems

Though EAC's process is informal by not having documentation and procedural guides, a contingency plan exists for GSA systems which include EAC. As a result, EAC would be effectively operational in the event of a minor or major disaster. EAC currently has a draft of recommendations for a COOP plan which will be addressed during the agencies efforts to be in compliance with OMB Circular A-130, NIST special Publication 800-18 and FISMA.

In the event of a security incident, EAC follows GSA's CIO-IT Security-01-02 in the Handling IT Security Incidents Procedural Guide.

FY08-9 EAC does not have an inventory of all the systems/applications used by GSA to support the operations of EAC, or formally identified major applications and general support systems. (Re-Issued)

Federal Information Security guidelines recommend that each organization should develop, document and maintain a current, baseline configuration of the information system and an inventory of the system's constituent components even if these systems are not operated by the organization. We reviewed the EAC's organizational structure and held discussions with management to identify EAC's IT infrastructure as well as identify critical systems and platforms that support their operations. EAC does not own or operate any IT systems or platforms. They rely on GSA which provides administrative, financial management and IT related support services for EAC. GSA owns and operates the systems that support EAC.

United States Code (USC) Chapter 35 of title 44 Subchapter III § 3505 (c) states that:

(1) The head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of such agency.
(2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.
(3) Such inventory shall be:
    (a) Updated at least annually.
    (b) Made available to the Comptroller General.
    (c) Used to support information resources management, including:

1. Preparation and maintenance of the inventory of information resources under section 3506(b) (4). ii. IT planning, budgeting, acquisition and management.

Recommendation

Obtain from their service provider, GSA, an inventory of systems that support EAC's operations. They should further obtain from GSA, a list of systems covered by the 2008 FISMA review and reconcile this with the list of EAC support systems to ensure EAC systems are adequately covered by the service provider's FISMA review.

EAC Management's Response

Currently, EAC has procured a contractor to assist with the Agency's strategies to meet compliancy for OMB A-130, NIST special Publication 800-18 and FISMA. This will include completion of a C&A of support systems, System Security Plans and Practices and procedural guides and documentation.

EAC is currently waiting for a reply from GSA on which systems are identified in the FISMA 2008 review.

VII. ACRONYMS

CFO	Chief Financial Officer
FIPS	Federal Information Processing Standard
FISCAM	Federal Information System Control Audit Manual
FISMA	Federal Information Security Management Act of 2002
FY	Fiscal Year
GAO	Government Accountability Office
GSA	General Services Administration
IG	Inspector General
IT	Information Technology
CG	Clifton Gunderson LLP
LAN	Local Area Network
NIST	National Institute of Standards and Technology
EAC	Election Assistance Commission
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&Ms	Plans of Action and Milestones
SP	Special Publication

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