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

		Page
I.	EXECUTIVE SUMMARY	1
II.	BACKGROUND	1
III.	OBJECTIVES	2
IV.	SCOPE AND METHODOLOGY	2
V.	DETAILS OF RESULTS	3
	A. Prior Year Results	3
	B. Current Year Results	4
VI.	FINDINGS AND RECOMMENDATIONS	5
VII.	ACRONYMS	23

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.