

U.S. ELECTION ASSISTANCE COMMISSION OFFICE OF INSPECTOR GENERAL



FINAL REPORT:

AUDIT OF U.S. ELECTION ASSISTANCE COMMISSION'S COMPLIANCE WITH SECTION 522 OF THE 2005 CONSOLIDATED APPROPRIATIONS ACT

**No. I-PA-EAC-02-08
MARCH 2009**



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

March 4, 2009

Memorandum

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

From: Curtis W. Crider *Curtis W. Crider*
Inspector General

Subject: Final Audit Report – Audit of U.S. Election Assistance Commission’s Compliance with Section 522 of the 2005 Consolidated Appropriations Act (Assignment No. I-PA-EAC 02-08)

We contracted with the independent certified public accounting firm of Clifton Gunderson LLP (Clifton Gunderson) to conduct the subject audit. The objective of the audit was to determine whether: (1) the necessity of using personally identifiable information for processing was properly evaluated; (2) the EAC had established adequate procedures governing the collection, use and security of personally identifiable information; and (3) EAC had properly complied with the prescribed procedures to prevent unauthorized access to and the unintended use of personally identifiable information.

The review found that the EAC was not fully compliant with several Privacy Act Requirements:

- 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 as required by the Office of Management and Budget Memorandum 06-16, Requirements for Protecting Personally Identifiable Information.
- No formalized policies and procedures are in place for Personally Identifiable Information which: (1) explicitly identify the rules for determining whether physical removal is allowed; (2) require the information be encrypted and that appropriate procedures, training and accountability measures are in place to ensure that remote use of this encrypted information does not result in bypassing the protections provided by the encryption; (3) explicitly identify the rules for determining whether remote access is allowed for personally identifiable information that can be removed; (4) require that the remote access be accomplished via a virtual private network connection established using agency issued authentication certificate (s) or hardware token, when remote access is allowed; (5) identify the rules for determining whether download or remote storage of the information is allowed, when remote access is allowed.

Based on the Executive Director's response to the draft report, dated February 20, 2009, we consider Recommendation No. 4 resolved and implemented. The remaining recommendations are considered resolved but not implemented. Please notify the Office of Inspector General when the proposed corrective actions have been completed.

The Inspector General Act of 1978, as amended, requires semiannual reporting to Congress on all reports issued, actions taken to implement recommendations, and recommendations that have not been implemented. Therefore, we will include the information in the attachment in our next semiannual report to Congress. The distribution of this report is not restricted, and copies are available for public inspection.

We appreciate the cooperation and assistance of EAC personnel during the audit. If you or your staff has any questions, please contact me at (202) 566-3125.

Attachments

Cc: Commissioners Hillman, Davidson
Executive Director
Chief Operating Officer
Director of Administration

ELECTION ASSISTANCE COMMISSION (EAC)

Report on the 2008 Review of EAC's Compliance
with Section 522 of the Consolidated Appropriations
Act, 2005.

(Policies, Procedures & Practices for Protection of
Personally Identifiable Information)

Clifton Gunderson LLP
September 30, 2008

TABLE OF CONTENTS

	PAGE
TRANSMITTAL LETTER.....	1
EXECUTIVE SUMMARY	2
BACKGROUND.....	2
SCOPE AND METHODOLOGY	5
DETAILED RESULTS OF REVIEW.....	7
APPENDIX	13



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 present our report on the Election Assistance Commission's (EAC) compliance with protection of personal data in an identifiable form. This review included assessing compliance with applicable federal security and privacy laws and regulations as well as assessing the privacy and data protection procedures used by EAC as they relate to the guidelines set forth in Section 522-d of the Omnibus Spending Bill for Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005. The objective of our review was to determine whether: (1) the necessity of using personally identifiable information for processing was properly evaluated; (2) EAC had established adequate procedures governing the collection, use and security of personally identifiable information; and (3) EAC had properly complied with the prescribed procedures to prevent unauthorized access to and unintended use of personally identifiable information.

We interviewed key personnel involved in identifying and protecting personally identifiable information and reviewed documentation supporting EAC's efforts to comply with federal privacy and security laws and regulations.

This performance audit was conducted from August 2008 to September 2008 at the EAC office in Washington, District of Columbia in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We appreciate the opportunity to have served you once more and are grateful for the courtesy and hospitality extended to us by EAC personnel. Please do not hesitate to call me at (301) 931-2050 or email at george.fallon@cliftoncpa.com if you have questions.

Sincerely,

CLIFTON GUNDERSON LLP

A handwritten signature in cursive script that reads "Clifton Gunderson LLP".

Calverton, Maryland
September 30, 2008

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

www.cliftoncpa.com

EXECUTIVE SUMMARY

Based on our review, EAC has (a) developed and implemented a privacy training course for employees and contractors; and (b) assigned privacy oversight responsibilities. However, more work remains to be accomplished. Specifically, we noted the following:

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 the Office of Management and Budget (OMB) Memorandum 06-16, Requirements for Protecting Personally Identifiable Information.
- No formalized policies and procedures are in place for Personally Identifiable Information which: (1) explicitly identify the rules for determining whether physical removal is allowed; (2) require the information be encrypted and that appropriate procedures, training and accountability measures are in place to ensure that remote use of this encrypted information does not result in bypassing the protections provided by the encryption; (3) explicitly identify the rules for determining whether remote access is allowed for personally identifiable information that can be removed; (4) require that the remote access be accomplished via a virtual private network (VPN) connection established using agency issued authentication certificate (s) or hardware token, when remote access is allowed; (5) identify the rules for determining whether download or remote storage of the information is allowed, when remote access is allowed.

BACKGROUND

On December 8, 2004, the President signed into law H.R. 4818, Consolidated Appropriations Act, 2005 (Public Law 108-447). Title V, Section 522 of this act mandates the designation of a senior privacy official, establishment of privacy and data protection procedures, a written report of the agency's use of information in an identifiable form,¹ an independent third party review of the agency's use of information in an identifiable form, and a report by the Inspector General to the agency head on the independent review and resulting recommendations. Section 522 (d) (3) requires the Inspector General to contract with an independent third party privacy professional to evaluate the agency's use of information in an identifiable form, and the privacy and data protection procedures of the agency. The independent review is to include (a) an evaluation of the agency's use of information in identifiable form, (b) an evaluation of the agency's privacy and data protection procedures, and (c) recommendations on strategies and specific steps to improve privacy and data protection management. Section 522 requires the agency to have an independent third party review at least every 2 years and requires the Inspector General to submit a detailed report on the review to the head of the agency. The third party report and related Inspector General report are to be made available to the public, i.e. internet availability.

In addition to Section 522, Federal agencies are subject to a number of other legislative requirements aimed at protecting the privacy rights of individuals and agency held sensitive information. Further, recent high-profile incidences surrounding actual or potential privacy

¹ Identifiable form is any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Personally identifiable information (PII) has a similar meaning and will be the term used throughout this document.

breaches or loss of sensitive information has led to increased direction from OMB to agencies in the form of a memorandum. A listing of key privacy related statutes, policies and guidelines follows.

- The Privacy Act of 1974, as amended
- The E-Government Act of 2002, section 208
- Federal Information Processing Standard Publication (FIPS PUB) 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST Special Publications 800-60, volume I: Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST 800-60, Volume II: Guide for Mapping Types of Information and Information Systems to Security Categories
- OMB Circular No. A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for maintaining Records about Individuals
- OMB Memorandum M-03-18, Implementation of E-government Act of 2002
- OMB Memorandum M-03-22, OMB guide for Implementation of the E-Government Act of 2002
- OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information
- OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- OMB Memorandum M-07-16, Safeguarding Against and Responding to Breach of Personally Identifiable Information
- OMB Memorandum M-07-18, Ensuring New Acquisitions Include Common Security Configurations
- OMB Memorandum M-07-19, Reporting Instructions for Federal Information Security Management Act and Agency Privacy Management
- EAC Information System Security Policy (Draft)
- EAC Privacy Protection Policies (Draft)

EAC's use of personally identifiable information and related policies and procedures

Congress established EAC with the passage of the Help America Vote Act (HAVA) in October 2002. EAC became operational in fiscal year 2004. The EAC is an independent, bipartisan agency created by HAVA. It assists and guides State and local election administrators in improving the administration of elections for Federal office. The EAC provides assistance by dispersing Federal funds to States to implement HAVA requirements, auditing the use of HAVA funds, adopting the voluntary voting system guidelines, and serving as a national clearinghouse and resource of information regarding election administration. The EAC also accredits testing laboratories and certifies, decertifies, and recertifies voting systems.

EAC's principle responsibilities are to:

- Administer funds that HAVA authorized for states to improve the administration of Federal elections, to replace-punch card and lever-action voting machines, and to meet the election technology and other administrative requirements of HAVA. To date, states have received Federal payments of approximately \$3 billion.

- Serve as a national clearinghouse on matters concerning the administration of elections under Federal law; and provide outreach to state and local election officials.
- Develop and update standards on voting systems and provide guidance on subjects such as statewide voter registrations systems and provisional ballots critical to the implementation of HAVA.
- Implement a system to accredit laboratories that test voting systems and to certify, decertify, and recertify voting system software and hardware against standards.

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.
- Otherwise 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.
- Submit an annual report to Congress describing EAC activities for the previous fiscal year.

The EAC has an operating budget of approximately \$26 million and has 38 employees and contractors. The EAC is headed by four Commissioners who are nominated by the President and confirmed by the U.S. Senate. Commissioners may serve only two consecutive terms. Commissioners serve staggered terms. No more than two Commissioners may belong to the same political party. The Commissioner Chairmanship rotates every year.

The EAC privacy function is temporarily assigned to the human resources specialist. However, responsibilities for privacy policy development, leadership, monitoring or enforcement have not been formally designated within a position description. A Privacy training course has been developed which is required to be completed by all EAC employees and contractors. EAC privacy policies and procedures are presently undergoing development, and in the interim, employees and contractors are referred to respective policies existing at their external service provider, General Services Administration (GSA). Privacy data is not stored, accessed or transmitted electronically at EAC. All personnel documents (i.e. Personally Identifiable Information (PII) data) are sent via fax, FedEx or United Postal Service (UPS) to the GSA Agency Liaison's office. This office uploads all EAC information (includes PII data) to the appropriate applications or databases. EAC employees or contractors do not have access to the GSA human resources system (i.e. CHRIS) which is utilized to store this data.

SCOPE AND METHODOLOGY

EAC's Office of the Inspector General (OIG) contracted with Clifton Gunderson LLP to conduct an audit of EAC's privacy and data protection policies and procedures in compliance with Section 522. The objective of this review was to assess the progress of EAC's Privacy Office in carrying out its responsibilities under federal law, more specifically, to determine whether: (1) the necessity of using personally identifiable information for processing was properly evaluated; (2) EAC had established adequate procedures governing the collection, use and security of personally identifiable information; and (3) EAC properly complied with the prescribed procedures to prevent unauthorized access to and unintended use of personally identifiable information.

To address this objective, we reviewed federal statutes including the Privacy Act of 1974 and Section 208 of the E-Government Act, to identify responsibilities of EAC's Privacy Office. We reviewed and analyzed privacy policies, guidance, and reports, and interviewed with officials from the Privacy Office. The personnel interviewed included the acting Privacy Officer for EAC to identify privacy office's plans, priorities, and processes for implementing its responsibilities using available resources.

We further evaluated the Privacy Office policies, guidance, and processes for ensuring compliance with the Privacy Act, and the E-Government Act. We analyzed the System of Records Notice (SORN)s and PIA development processes and assessed the progress of the office in implementing these processes. This analysis included analyzing the Privacy Office's overview of PIAs developed and assessing the overall quality of published PIAs.

Perform an assessment of EAC's privacy policies

We reviewed EAC information management practices for protection of PII, as they relate to the guidelines set forth in Section 522-d of the 2005 Government Appropriations Act. Public Law 107-347, the E-Government Act of 2002, defines "identifiable form" as any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. We performed procedures to assist the OIG in evaluating EAC's information management practices in order to:

- A. Determine the accuracy of the descriptions of the use of information in identifiable form² while accounting for current technologies and processing methods;
- B. Determine the effectiveness of privacy and data protection procedures by measuring actual practices against established procedural guidelines;
- C. Determine compliance with the stated privacy and data protection policies of EAC and applicable laws and regulations;
- D. Determine whether all technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in operation of the program, and

²information in identifiable form is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

- E. Provide EAC with recommendations, strategies, and specific steps, to improve privacy and data protection management.
- F. Evaluate EAC's use of information in identifiable form.

We examined EAC's PII policies, practices and data protection procedures and mechanisms in operation. Specifically, the tasks focused on:

- A review of the agency's technology, practices and procedures with regard to the collection, use, sharing, disclosure, transfer, and storage of information in an identifiable form;
- A review of the agency's stated privacy and data protection policies and procedures for personal information of employees and the public;
- A detailed analysis of agency intranet, network and Websites for privacy vulnerabilities;
- A review of agency compliance with the Section 522 of the Appropriations Act of 2005;
- An analysis of the extent to which the Privacy Report filed with the EAC Inspector General (IG) is accurate, accounts for the EAC's current technologies, information processing, and whether all areas are consistent with the section 522 of the Appropriations Act 2005;
- A follow-up review of findings identified in any previous EAC OIG reports; and

Given that the overall privacy control environment of the EAC is based on the Privacy Act, incremental compliance directives from OMB, and internal policies and procedures, the contractor should consider, and include where appropriate, assessment of OMB privacy and security memorandums as well as EAC policies and procedures in determining compliance with Section 522.

The E-Government Act of 2002 requires agencies to conduct a PIA either (1) before developing or procuring information technology systems or projects that collect, maintain or disseminate information in identifiable form or (2) when initiating a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government). In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks, for example, when converting paper-based records to electronic systems. On the other hand, no PIA is required where (1) information relates to internal government operations, (2) has been previously assessed under an evaluation similar to a PIA, or (3) where privacy issues are unchanged.

To accomplish the above-mentioned objectives, we:

- Verified that EAC had identified and maintained an inventory of information systems containing PII and systems requiring PIAs and had conducted PIAs for electronic information systems.
- Reviewed a sample of PIAs for the systems selected under review and noted the following:
 - What information was collected (e.g., nature and source).
 - Why the information was collected (e.g., to determine eligibility).
 - Intended use of the information (e.g., to verify existing data).
 - With whom the information was shared (e.g., another agency for a specified programmatic purpose).

- What opportunities individuals had to decline to provide information or to consent to particular uses of the information (other than required or authorized uses), and how individuals communicated consent.
- How the information was secured from abusive use (e.g., administrative and technological controls).
- Selected a representative sample of systems and tested technical controls to achieve the PII protection objectives.
- Reviewed the nature and use of PII, to determine whether a SORN was required and if required, whether one was published. We further reviewed EAC's publication of SORNs in the Federal Register and verified that they contained only information about individuals that was "relevant and necessary" to accomplish EAC's purpose. We verified that this information was updated as necessary.

For the Fiscal Year 2008 Privacy Assessment, we were not engaged to and did not perform procedures to determine if the inventory of systems containing PII data was exhaustive and if EAC had performed procedures to ensure all EAC IT systems had been reviewed for existence of PII information.

DETAILED RESULTS OF REVIEW

1. *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 2007 and noted EAC 's level of compliance. The following questions were extracted from the Data Collection Instrument issued by the President's Council on Integrity and Efficiency (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	<p>Although EAC has not received an inventory of all systems used by GSA to support EAC's activities, EAC has 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 indeed encrypted and noted no exception.</p> <p>EAC has identified that Pegasys and Comprehensive Human Resources Integrated System (CHRIS) are the GSA owned systems that contain EAC's personally identifiable information.</p>
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 not identified security policies and procedures.
Step 3	Has EAC implemented protections for personally identifiable information being transported and/or stored	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 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

	offsite? If so, to what level.		<p>encrypted and noted no exception.</p> <p>We noted that EAC issued blackberries are not currently encrypted with the Credent encryption software.</p>
Step 4	Has EAC implemented protections for remote access to personally identifiable information? If so to what level.	Partial	<p>The IG's office has signed the GSA's Rules 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.</p> <p>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.</p> <p>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.</p> <p>EAC does not have Plan of Actions and Milestones (POA & M) for developing and implementing protection of sensitive information.</p>
Sect 2.1	Has the Agency encrypted all data on mobile computers/devices which carry agency data unless the data determined to be non-sensitive, in writing by Agency Deputy Secretary or an individual he/she may designate in writing?	Partial	<p>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 and noted no exception.</p> <p>We noted that EAC issued blackberries or portable memory sticks are not currently encrypted with the Credent encryption software.</p>
Sect 2.2	Does the agency use remote access with two-factor authentication where one of the factors is	No	<p>We were not provided evidence of major steps and milestones directed to implement two-factor authentication.</p>

	provided by a device separate from the computer gaining access?		
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	Although EAC has implemented a "time-out" function for EAC desktops, laptops and VPN access requiring user re-authentication after 30 minutes of inactivity, formalized EAC policies and procedures requiring this configuration have not been developed to date.
Sect 2.4	Does the Agency log all computer-readable data extracts from databases holding sensitive information and verifies each extract including sensitive data has been erased within 90 days or its use is still required?	No Not Applicable	EAC does not own or operate any information systems that hold sensitive information. All identified systems, Pegasys, FMIS and CHRIS are owned and managed by GSA. EAC on the other hand, has not defined which systems have to be logged and the nature of activity to be logged and reported by its service provider.
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 on the reporting of PII breaches within the first hour of occurrence. EAC is also required to fill out the GSA incident report to describe the event and 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 to include:
 - a) references to applicable information technology security policies and procedures
 - b) EAC specific procedures for responding to breaches of PII
 - c) identification of which PII systems are to be logged and the nature of activity to be logged and reported by the respective service provider(s)
 - d) requirements to utilize a time out function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity.
- 4) Complete the encryption of blackberry devices and laptops with Credent Encryption software as well as implement two-factor authentication.
- 5) Develop and maintain a plan of actions and milestones (POA&M) to address weaknesses identified in developing and implementing protections of PII.
- 6) Conduct a risk assessment which addresses the risks associated with the download, remote access, or other removal of PII from each system containing PII.

Management's Response:

- 1) The Human Resources Director will be assigned as the Chief Privacy Officer and will modify the PD to include the necessary functions. In addition she will be taking necessary training towards certification. This will be effective March 16, 2009. Alice Miller, the COO will be responsible for implementation.
- 2) EAC has an inventory of GSA systems that we use. These GSA systems are covered by GSA's FISMA review. With this, EAC has an understanding for the rotation schedule for these systems. GSA provides EAC with the required documents for FISMA compliance. EAC will request the documentation for these systems to include the POA&M to identify what vulnerabilities these systems have and what GSA is doing to remediate them in the off-years. The request will be completed by March 16 and will be the responsibility of the IT Specialist.
- 3) EAC has begun to evaluate the necessary steps to implement formal policies and procedures that address the information protection needs and have concluded that it will be necessary to procure outside help to fully implement the recommendation. Once the Continuing Resolution is lifted and budgetary resources are identified, EAC will consider releasing an RFP for the services. Anticipated date for release is within 45 days of the removal of the CR and approval of a budget. The Contracting Officer and IT Specialist will be responsible for this task. In addition, EAC has taken some steps to implement the recommendations. For instance there is currently a 30 minute time out function for both RAS and VPN remote connections. Also, there is a maximum 15 minute time out function on all Blackberry mobile devices.
- 4) With the assistance of GSA, EAC has encrypted all Blackberry devices. The Credent

encryption software has been installed on all laptops. The EAC has begun the process of identifying appropriate software to encrypt thumb drives which will be encrypted prior to distribution to staff.

- 5) EAC is in the process of drafting a formal plan of actions and milestones to address weaknesses identified in the developing and implementing the protections of PII. Estimated date of the first release is June 30, 2009. Responsible party is Diana Scott, Director of Administration.
- 6) EAC intends to conduct a risk assessment which addresses the risks associated with the download, remote access or other removal of PII from each system containing PII. Once the Continuing Resolution is lifted and budgetary resources are identified, EAC will consider releasing an RFP for the services. Anticipated date for release is within 45 days of the removal of the CR and approval of a budget. The Contracting Officer, Chief Privacy Officer and IT Specialist will be responsible for this task.




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

February 20, 2009

MEMORANDUM

TO: Curtis Crider, Inspector General

FROM: Thomas R. Wilkey, Executive Director 

RE: Responses to Draft Audit Report - Review of U.S. Election Assistance Commission's Compliance with Section 522 of the Consolidated Appropriations Act, 2005 (Assignment No. 1-EV-EAC 02-08)

Recommendation #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.

Response # 1

The Human Resources Director will be assigned as the Chief Privacy Officer and will modify the PD to include the necessary functions. In addition she will be taking necessary training towards certification. This will be effective March 16, 2009. Alice Miller, the COO will be responsible for implementation.

Recommendation #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.

Response #2

EAC has an inventory of GSA systems that we use. These GSA systems are covered by GSA's FISMA review. With this, EAC has an understanding for the rotation schedule for these systems. GSA provides EAC with the required documents for FISMA compliance. EAC will request the documentation for these systems to include the POA&M to identify what vulnerabilities these systems have and what GSA is doing to remediate them in the off-years. The request will be completed by March 16 and will be the responsibility of the IT Specialist.

Recommendation #3

Develop and implement formal policies that address the information protection needs associated with PII to include:

- a) references to applicable information technology security policies and procedures,
- b) EAC specific procedures for responding to breaches of PII,
- c) identification of which PII systems are to be logged and the nature of activity to be logged and reported by the respective service provider(s).
- d) requirements to utilize a time out function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity.

Response #3

EAC has begun to evaluate the necessary steps to implement formal policies and procedures that address the information protection needs and have concluded that it will be necessary to procure outside help to fully implement the recommendation. Once the Continuing Resolution is lifted and budgetary resources are identified, EAC will consider releasing an RFP for the services. Anticipated date for release is within 45 days of the removal of the CR and approval of a budget. The Contracting Officer and IT Specialist will be responsible for this task. In addition, EAC has taken some steps to implement the recommendations. For instance there is currently a 30 minute time out function for both RAS and VPN remote connections. Also, there is a maximum 15 minute time out function on all Blackberry mobile devices.

Recommendation #4

Complete the encryption of blackberry devices and laptops with Credent Encryption software as well as implement two factor authentication

Response #4

With the assistance of GSA, EAC has encrypted all Blackberry devices. The Credent encryption software has been installed on all laptops. The EAC has begun the process of

identifying appropriate software to encrypt thumb drives which will be encrypted prior to distribution to staff.

Recommendation #5

Develop and maintain a plan of actions and milestones (POA&M) to address weaknesses identified in developing and implementing protections of PII.

Response #5

EAC is in the process of drafting a formal plan of actions and milestones to address weaknesses identified in the developing and implementing the protections of PII. Estimated date of the first release is June 30, 2009. Responsible party is Diana Scott, Director of Administration.

Recommendation #6

Conduct a risk assessment which addresses the risk associated with the download, remote access, or other removal of PII from each system containing PII.

Response #6

EAC intends to conduct a risk assessment which addresses the risks associated with the download, remote access or other removal of PII from each system containing PII. Once the Continuing Resolution is lifted and budgetary resources are identified, EAC will consider releasing an RFP for the services. Anticipated date for release is within 45 days of the removal of the CR and approval of a budget. The Contracting Officer, Chief Privacy Officer and IT Specialist will be responsible for this task.

ccs: Chair Beach
Commissioners Hillman, Davidson, Rodriguez
Alice Miller, Chief Operating Officer
Diana Scott, Director of Administration

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

