Supplementary Exhibit 2

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 Consolidated Appropriations Act 2005

Report No.
I-PA-EAC-04-12
May 2013

U.S. ELECTION ASSISTANCE COMMISSION
Office of Inspector General

May 7, 2013

TO: Alice Miller,
Acting Executive Director and Chief Operating Officer

FROM: Curtis W. Crider
Inspector General

SUBJECT: Review of the U.S. Election Assistance Commission Compliance with Section 522 of the Consolidated Appropriations Act 2005

We contracted with the independent certified public accounting firm of CliftonLarsonAllen, LLP to perform an audit of EAC's compliance with protection of personal data in an identifiable form. The audit 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 Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005. The contract required that the audit be performed in accordance with generally accepted government auditing standards. Attached is a copy of the final report.

In response to the draft report dated February 27, 2013, the EAC generally agreed with the report which included providing expected completion dates for each of the recommendations.

The legislation as amended, creating the Office of Inspector General (5 U.S.C. § App. 3) requires semiannual reporting to Congress on all inspection and evaluation reports issued, actions taken to implement recommendations, and recommendations that have been implemented. Therefore, a summary of 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.

Copy to: Mohammed Maeruf, CIO
Annette Lafferty, CFO
Sheila Banks, PO

U.S. ELECTION ASSISTANCE COMMISSION (EAC)

Report on the 2012 Review of EAC's Compliance with Section 522 of the Consolidated Appropriations Act 2005

(Policies, Procedures & Practices of Personally Identifiable Information)

April 25, 2013

CliftonLarsonAllen LLP
www.cliftonlarsonallen.com

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 U.S. 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 Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005. The objective of our review was to determine whether EAC's stated privacy and data protection policies and procedures for personal information of employees and the public are adequate and effective and in compliance with Section 522 of the Appropriations Act of 2005.

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

This audit was performed between November 2012 to January 2013 at the EAC office in Washington, District of Columbia. We conducted this performance audit 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@cliftonlarsonallen.com if you have questions.

Sincerely,

CLIFTONLARSONALLEN LLP

CliftonLarsonAllen LLP

Calverton, Maryland
April 25, 2013

Table of Contents

Executive Summary

Based upon our review, EAC has made improvements to strengthen controls over the security of Personally Identifiable Information (PII) including conducting Privacy Impact Assessments (PIA), appointed a senior agency official for privacy and privacy officer, and developed formalized policies and procedures for PII, however more work remains to be accomplished.

Specifically, EAC was not fully compliant with Section 522 of the Consolidated Appropriations Act 2005 requirements, including:

- Effective encryption mechanisms to appropriately protect agency information, including PII were not implemented;
- Formalized PII usage reports were not submitted to the Office of Inspector General (OIG); and
- EAC Records Management Processes and Procedures Standard Operating Procedures were not formally documented.

Introduction

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 the related Inspector General report are to be made available to the public, i.e. internet availability.

[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.

Scope and Methodology

Our audit objectives were to evaluate and report on whether the EAC had established adequate privacy and data protection policies and procedures governing the collection, use, disclosure, transfer, storage and security of information relating to agency employees and the public in accordance with Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005.

Our audit scope included the review of EAC documents, and a walkthrough of how PII data is received, processed and stored in electronic and manual form at EAC headquarters in Washington, DC. The following specific procedures were performed to complete the survey assessment:

- Issued a document request list detailing the initial information needed for the audit.
- Reviewed any baseline documentation prepared by EAC to gain a preliminary high level understanding of information in an identifiable form and its use throughout EAC.
- Identified key individuals with responsibility or control over privacy data collected, maintained or processed throughout EAC.
- Evaluated existing work performed by the EAC, the OIG or third parties.
- Reviewed all available documentation related to audits regarding the EAC's implementation and compliance with privacy policy, and practices.
- Coordinated administrative, technical and key logistical aspects of the audit with OIG.
- Obtained permission from the OIG and management to review working papers, documentation, and reports at agreed-upon dates, times and locations; and perform interviews as needed to establish an understanding of missing or incomplete support for the purposes of conducting the privacy audit.
- Obtained an understanding of EAC's privacy and data protection policies and procedures for personal information of EAC employees, contractors and the public.
- Identified and documented risks in EAC's operations for effectively identifying securing and protecting privacy data.
- Analyzed EAC's internal controls related to processes to safeguard privacy data, related policies and procedures, and records management.
- Tested significant controls to determine whether those controls are operating effectively to mitigate any identified risk.
- Issued Notice of Findings and Recommendations (NFRs) to EAC and discussed results with EAC and OIG.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Findings and Recommendations

1. ***EAC had not implemented effective encryption mechanisms to appropriately protect agency information, including PII.***

   We noted that EAC had not implemented effective encryption to appropriately protect agency information, including PII. Specifically, the following was noted:

   - EAC did not employ encryption of all data stored on employee desktops or laptops. Additionally, we noted several instances where PII, including names, addresses, phone numbers and social security numbers, were located on the network and not password protected or encrypted.
   - Backup tapes were not encrypted prior to being sent off-site.

   We understand that EAC issued encrypted flash drives to staff, who are required to save sensitive or PII data on these flash drives before removal from the office. Also, EAC employees are required to utilize a designated encryption tool to store the data on their laptops.

   Although all data stored on EAC laptops were not encrypted, we understand that all laptops are protected and monitored by a third party vendor responsible for monitoring the use of each laptop. In the event the laptop is lost or stolen, this vendor is capable of wiping the drive remotely as soon as they identify the computer online. EAC personnel could remotely access their shared drives via VPN and their email by means of a secured web site (SSL) using an Online Web Application.

   EAC's Office of the Chief Information Officer (OCIO), backs up data using a password protected tool that requires using the same password to restore any data. In support of EAC's Disaster Recovery effort, PII data is encrypted by data owners prior to backing up the data to a tape drive and sending it to an offsite location for storage.

   EAC management is presently developing a plan to upgrade workstations and laptops to an operating system platform, which has full-disk encryption capabilities. To address our recommendations, the OCIO and Privacy Officer have indicated they will perform a full scale review of the agency's shared drive to detect unprotected PII and ensure that files and folders are properly protected. At the same time, the SAOP will evaluate the backup device encryption capability of all backup tapes transported offsite for storage.

   Section 1.2 of the *EAC Encryption Key Management* policy states, "all agency data on laptop and portable storage devices (e.g., USB flash drives, external hard drives) must be encrypted with a FIPS 140-2 certified encryption module." Additionally, section 1.3 states "if it is a business requirement to store PII on EAC user workstations or mobile devices including, but not limited to notebook computers, USB drives, CD-ROMs/DVDs, person digital assistants and Black berries, PII must be encrypted using a FIPS 140-2 certified encryption module."

   National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, security control MP-5, states the following regarding media transport:

The organization:

a. Protects and controls [*Assignment: organization-defined types of digital and non-digital media*] during transport outside of controlled areas using [*Assignment: organization-defined security measures*]; Control Enhancement:

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

EAC employees are encouraged by management to utilize the zipping tool, as an encryption mechanism for storing PII on laptops and other mobile devices; however, files must be stored on the EAC network prior to being compressed and encrypted. EAC is planning to move to the Windows 7 operating system which has built encryption. Additionally, the ability to encrypt backup tapes is available; however, it is a manual feature which EAC can turn on and off. The EAC encryption key was created during the audit period and use was unable to be verified. By not encrypting data, EAC is at an increased risk of data loss or theft.

Recommendations

We recommend EAC management:

1) Develop and implement a plan to implement encryption to all data stored on agency laptops and workstations.
2) Perform a review for unprotected PII stored on the network share drives to ensure files are adequately protected.
3) Implement a validation process to ensure encryption of all backup tapes being transported off-site for storage.

2. Formalized PII usage reports were not submitted to the OIG in accordance with Section 522 of the Consolidated Appropriations Act of 2005.

We noted that EAC management did not provide written PII usage reports to the OIG.

Section 522 of the *Consolidate Appropriations Act of 2005* states, "each agency shall prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency. Each report shall be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report. By signing the report the privacy officer also verifies that the agency is only using information in identifiable form as detailed in the report." (5 U.S.C. § 552a(c))

EAC completes the annual FISMA review which requires the agency to report on information privacy; although the FY 2012 FISMA audit and report did not address the agency's controls surrounding the protection of privacy data. Furthermore, management was unaware of the requirement to complete reports to provide to the OIG of their use and collection of PII, and their adherence of agency policy and regulations.

Without periodic reviews of agency use of PII, EAC may be unaware of the information that is being collected, used, and stored by the agency; therefore, the agency may inadvertently apply insufficient security controls to adequately protect that information.

Recommendation

We recommend EAC management 1) perform an inventory of EAC's PII data and how it is used within the agency and 2) document and implement a process for the Privacy Officer to periodically report to the Office of Inspector General on the Agency's use of information in an identifiable form, and verify compliance with privacy and data protection policies and procedures.

3. The EAC Records Management Processes and Procedures Standard Operating Procedure was not formally documented

We noted that EAC had not finalized the Records Management Processes and Procedures Standard Operating Procedure as they were in the process of coordinating completion with National Archives and Records Administration (NARA). However, if procedures are not formally documented related to records management, documents may not be adequately encrypted or secured, additionally EAC is at an increased risk of data loss or theft of these records.

We understand that the draft of EAC's Records Management Processes and Procedures Standard Operating Procedures is currently being reviewed by the agency's Acting Executive Director and Chief Operating Officer, Senior Agency Official for Privacy, Privacy Officer, and outside counsel. Once comments have been agreed upon, they will be incorporated into the document and the SOP will be finalized.

Section 522 of Public Law 108-447 states as part of bullet (b)(1), "Within 12 months of enactment of this Act, each agency shall establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public. Such procedures shall be consistent with legal and regulatory guidance, including OMB regulations, the Privacy Act of 1974, and section 208 of the E-Government Act of 2002.

Recommendation

We recommend EAC finalize and implement the Records Management Processes and Procedures Standard Operating Procedure.

Conclusions and Recommendations

Based upon our review, EAC has made improvements since the last Privacy audit to strengthen controls over the security of PII including conducting PIA, appointing a senior agency official for privacy and privacy officer, and developing formalized policies and procedures for PII, however more work remains to be accomplished. To become fully compliant with Section 522 of the Consolidated Appropriations Act 2005, EAC needs to ensure privacy role based training is performed, encryption controls to secure PII data stored on desktops, laptops and backup tapes are strengthened, and an ongoing review of and reporting to the OIG of PII usage within the agency and the finalization of records management policies. We recommend EAC management:

- Develop and implement a plan to apply data encryption to all agency laptops and workstations.
- Perform a review for unprotected PII stored on the network share drives to ensure files are adequately protected.
- Implement a validation process to ensure encryption of all backup tapes being transported off-site for storage.
- Perform an inventory of EAC's PII and how it is used within the agency.
- Document and implement a process for the Privacy Officer to periodically report to the Office of Inspector General on the Agency's use of information in an identifiable form, and verify compliance with privacy and data protection policies and procedures.
- Finalize and implement the Records Management Processes and Procedures Standard Operating Procedure.

Agency Response and OIG Comments

1. **EAC had not implemented effective encryption mechanism to appropriately protect agency information, including PII.**

   Management Response
   Management initially disagreed with this finding related to the recommendation for full disk encryption, however also indicated the current use of encrypted flash drives and planned projects including operating system upgrades, data encryption implementation, review of all shared drives for unsecured PII and a reconfiguration project to mitigate the risks identified.

   OIG Comments
   Revisions were made to the finding and recommendation within this report to address management's concerns related to full disk encryption. Management subsequently concurred with revised wording to data encruption.

2. **Formalized PII usage reports were not submitted to the OIG in accordance with Section 522 of the Consolidated Appropriations Act of 2005.**

   Management Response
   Management agreed with the finding and recommendation and plans to conduct an inventory of EAC's PII and submit a PII usage report to the IG by the first week of July 2013.

   OIG Comments
   Management concurred with our finding and recommendation.

3. **The EAC Records Management Processes and Procedures Standard Operating Procedure (SOP) was not formally documented.**

   Management Response
   Management agreed with the finding and recommendation and indicated EAC's Records Management Standard Operating Processes and Procedures was signed and approved on April 4, 2013.

   OIG Comments
   Management concurred with our finding and recommendation.

U.S. ELECTION ASSISTANCE COMMISSION
1201 New York Avenue, NW, Suite 300
Washington, DC 20005

Memorandum April 9, 2013

To: Arnie Garza
Assistant Inspector General for Audits

From: Alice Miller
Acting Executive Director & Chief Operating Officer

Subject: 2012 Review of the U.S. Elections Assistance Commission Compliance with Section 522 of the Consolidated Appropriations Act 2005

This memorandum transmits the U.S. Election Assistance Commission's (EAC) responses to the recommendations resulting from the audit performed by CliftonLarsonAllen (CLA) between November 2012 and January 2013. As stated in the draft report, the purpose of the audit was to review EAC's compliance with Section 522 of the Consolidated Appropriations Act 2005.

We are pleased that CLA notes the proactive and significant progress that EAC's Privacy Act Program has made in addressing our statutory responsibilities. We consider privacy to be a matter of great importance and have undertaken significant efforts to ensure compliance.

This memorandum: (1) identifies management's agreement and disagreement with the recommendations; and (2) identifies actions that EAC will take to address the recommendations.

EAC's response to each CLA recommendation follows:

1. ENCRYPTION MECHANISMS

Recommendation: Develop and implement a plan to apply full-disk encryption to agency laptops and workstations. Perform a review for unprotected PII stored on the network share drives to ensure files are adequately protected. Implement a validation process to ensure encryption of all backup tapes being transported off-site for storage.

Management Response: We disagree. To administer internal security controls to protect sensitive and PII data, EAC issued encrypted flash drives to staff. Sensitive and PII data must be encrypted and saved on the hard drives on the server and the flash drives by the information owner.

As indicated in the audit report, efforts are being made by management to safeguard PII data. Current projects include:

- Developing a plan to upgrade workstations and laptops to Windows 7 and utilizing an encryption software application for the partitioned full-disk encryption of EAC workstations and laptops. Sample testing is currently underway.

- Partitioning the disk, thereby, separating the operating system (OS) from the data section. Since the OS does not have to be encrypted, the section containing data will be encrypted on all EAC laptops and workstations.

The Senior Agency Officer of Privacy (SAOP) and the Privacy Officer (PO) will perform a full scale review of the agency's shared drive to ensure that files and folders are properly protected and security access permissions are updated. During this process, active and inactive files will be identified to facilitate the reconfiguration of the shared drive. Active files that can be viewed by all EAC staff will be placed in an Access Central folder; whereas, active files containing PII and sensitive data will be placed in Division folders and accessible via security access permissions. Inactive files will be archived, by division, and will also require security access permissions. To that end, the reconfiguration project will (1) provide increased space on the shared drive, (2) decrease the amount of time it takes to back up the t-drive, and (3) facilitate encryption of all backup tapes being transported off-site for storage.

2. PII USAGE REPORTS

Recommendation: We agree. Perform an inventory of EAC's PII data and how it is used within the agency and document and implement a process for the Privacy Officer to periodically report to the Office of Inspector General on the Agency's use of information in an identifiable form, and verify compliance with privacy and data protection policies and procedures.

Management Response: An inventory of EAC's PII and how it is used in the agency will take place during the current Records Management project, which is expected to be completed by the third quarter in FY 2013. The PO will submit a PII usage report to the IG by the first week in July.

3. RECORDS MANAGEMENT STANDARD OPERATING PROCEDURE (SOP)

Recommendation: Finalize and implement the Records Management Processes and Procedures Standard Operating Procedure.

Management Response: We agree. The final draft of EAC's Records Management Standard Operating Processes & Procedures was signed and approved by executive staff on April 4, 2013 and is currently on EAC's t-drive.

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

If you have any questions regarding our responses, please do not hesitate to contact me at (202) 566-3110.

Copy to: Mohammed Maeruf, CIO
Annette Lafferty, CFO
Sheila Banks, PO

MANAGEMENT RESPONSES TO RECOMMENDATIONS

This table presents management's responses to the recommendations in the draft audit report and the status of the recommendations as of the date of report issuance.

Rec. Number	Corrective Action: Taken or Planned/Status	Measure	Expected Completion Date	Responsible Party(ies)	Resolved:* Yes/ No	Open or Closed**
1	EAC workstations and laptops will be upgraded to Windows 7. IT is currently testing the several encryption software applications to support this task Review, restructure, and update security access to agency's shared drive.	Encryption of data contained on partitioned disk. Full-disk encryption is not necessary.	December 31, 2013	Office of Chief Information Officer Privacy Officer	No	Open
2	PII inventory and usage information will be collected along with information for the Records Management project.	Annual PII Usage Reports submitted to the Office of Inspector General (OIG)	July 5, 2013	Records Management Officer Privacy Officer	Yes	Open
3	Implement the Records Management Standard Operating Processes and Procedures	Finalized Records Management Standard Operating Procedure	April 3, 2013	Acting Executive Director, Inspector General, Chief Financial Officer, Chief Information Officer, Privacy Officer	Yes	Closed

* Resolved – (1) Management concurs with the recommendation, and the planned corrective action is **consistent** with the recommendation.
(2) Management does not concur with the recommendation, but planned alternative action is **acceptable** to the OIG.

** Once the OIG determines that the agreed-upon corrective actions have been completed and are effective, the recommendation can be closed.

OIG's Mission	The OIG audit mission is to provide timely, high-quality professional products and services that are useful to OIG's clients. OIG seeks to provide value through its work, which is designed to enhance the economy, efficiency, and effectiveness in EAC operations so they work better and cost less in the context of today's declining resources. OIG also seeks to detect and prevent fraud, waste, abuse, and mismanagement in these programs and operations. Products and services include traditional financial and performance audits, contract and grant audits, information systems audits, and evaluations.
Obtaining Copies of OIG Reports	Copies of OIG reports can be requested by e-mail. (eacoig@eac.gov). Mail orders should be sent to: U.S. Election Assistance Commission Office of Inspector General 1201 New York Ave. NW - Suite 300 Washington, DC 20005 To order by phone: Voice: (202) 566-3100 Fax: (202) 566-0957
To Report Fraud, Waste and Abuse Involving the U.S. Election Assistance Commission or Help America Vote Act Funds	By Mail: U.S. Election Assistance Commission Office of Inspector General 1201 New York Ave. NW - Suite 300 Washington, DC 20005 E-mail: eacoig@eac.gov OIG Hotline: 866-552-0004 (toll free) FAX: 202-566-0957