U.S. ELECTION ASSISTANCE COMMISSION
1225 NEW YORK AVENUE, N.W., SUITE 1100
WASHINGTON, D.C. 20005

November 9, 2009

Memorandum

To: Curtis W. Crider
Inspector General

From: Gineen Bresso Beach Gineen B. Beach
Chair, U.S. Election Assistance Commission

Subject: Election Assistance Commission Response to the Inspector General's Statement Summarizing the Major Management and Performance Challenges

The Election Assistance Commission (EAC) over the past year pursued its mission to assist the effective administration of Federal elections. This response to the Inspector General's Statement Summarizing the Major Management and Performance Challenges highlights efforts to strengthen the management of its programs and operations. Specifics associated with each of the identified major management challenges are discussed below.

Performance Management and Accountability

During FY 2009, to address issues in the FY 2008 financial statement audit, EAC:

- Adopted its first Strategic Plan in March 2009, covering 2009 through 2014, which identified the reporting relationships beyond the Executive Director and Commissioners in an organization chart, and which allows the agency to begin the process of reporting on formal performance metrics contained in the Plan;
- Reorganized overall structure and established its first Chief Financial Officer department consisting of experienced grants, budget, accounting and procurement staff;
- Finalized financial management policies and procedures;
- Submitted a FY 2010 Congressional Budget Justification and FY 2011 OMB Budget Justification in a performance based format; and
- Closed out many outstanding recommendations from operational audits and the FY 2008 financial statement audit.

The agency has made tremendous progress in the program areas during FY 2009. EAC:

- Made strides in certifying voting systems: between February and August, three voting systems were certified;

- Improved communications with stakeholders by instituting a Testing and Certification Voting System Reports Clearinghouse on its website;
- Issued best practices for voter information web sites, Quick Start Management guides on administering Federal elections, and a report on the Impact of the National Voter Registration Act on Federal Elections, 2007-2008
- Held working groups on UOCAVA, Elections, Technology & Accessibility, and Election Office Management.
- Awarded 13 Poll Worker grants totaling $750,000, and seven Mock Election grants totaling $300,000.

EAC's plans for FY 2010 are in line with actions identified by the Inspector General for completing the process of "developing and implementing strategic planning tools for each of its divisions or programs." Part of this process has been an independent review of EAC performance measures, how well the measures capture information useful to accomplishing agency goals, and how well the data collection systems produce reliable results. EAC will implement a robust internal control program and reliable and useful performance measurement systems, based on independent recommendations. Internal control training for staff is planned for the first quarter of FY 2010. The training will emphasize the importance of identifying risk.

EAC will work to finalize and implement remaining policies and procedures, Communications, Clearinghouse, Research and updated administrative in FY 2010.

Financial Management and Performance

Policies and procedures for Grants Management, Testing and Certification, and Financial Management have been finalized. Financial management policies and procedures, developed during the second half of the fiscal year upon set up of the CFO department, are currently being implemented.

As mentioned above, an independent assessment of EAC's risks was conducted, using the reliability of performance measures in the Strategic Plan as a guide.

Information Technology Management and Security

As noted by the Federal Information Security Management Act (FISMA) of 2002 independent evaluation in FY 2009, EAC made significant efforts to improve information security. Nevertheless, there is still work to be done to bring EAC in full compliance with FISMA requirements. To facilitate this effort, EAC has developed an overall security Plan of Action and Milestones (POA&M) which included target dates for completion of key corrective actions. EAC is working with a contractor to implement several corrective actions. The contractor will be required to keep EAC management closely informed of all progress on these actions.

Once the items in the POA&M are implemented, the agency will be in full compliance with requirements in every FISMA control area.

The key areas of effort are summarized below, and more detail is available in both the management response to the FISMA evaluation and the overall EAC POA&M. The numbers below match the Finding Numbers in the OIG report; i.e., item 3 below matches item FY-09-03 in the OIG report, and so on. Key FISMA efforts scheduled for FY 2010 include:

1. EAC management will monitor progress on implementation of the EAC FISMA POA&M.

2. EAC will initiate a search for a full-time Chief Information Officer (CIO), who may also serve as Senior Agency Information Security Officer (SAISO), Chief Privacy Officer, and information security proponent. EAC will finalize information security roles and responsibilities across the organization once the CIO position has been filled.

3. All operational procedures developed for information security at EAC will facilitate continuous monitoring of EAC information systems and security controls. This process will use automatic monitoring procedures such as automated system alerts using periodic review by qualified staff to ensure that procedures remain appropriate and relevant. In particular, procedures for change management, configuration management, audit log monitoring, network monitoring, patch management, risk management, and vulnerability scanning will facilitate continuous monitoring.

4. EAC will finalize and disseminate the provisional information security policies handbook to agency staff. In particular, key policies concerning privacy will be included in the 2010 employee information security awareness training. EAC information owners and information technology (IT) staff will develop, implement, and periodically review written operational procedures that specify how to implement the required controls to satisfy EAC's information security policy objectives in every FISMA control area.

5. EAC will develop a Business Impact Analysis (BIA), Disaster Recovery Plan (DRP), and a Continuity of Operations Plan (COOP), once the information owners review the current risk assessment, and major policies, procedures, and controls have been finalized and implemented.

6. Minimum password settings for the network have already been implemented and are now fully compliant with Federal Desktop Core Configuration standards (FDCC). At the appropriate time, EAC will develop a re-imaging schedule, present this schedule to appropriate supervisors, and then re-image computers as per this schedule.

7. EAC will work with the General Services Administration (GSA) to disable dialup remote access or, at a minimum, grant dialup access only on an as-required and/or contingency basis. EAC will re-initiate conversations with GSA and develop a timeline for the implementation of two-factor authentication for securing remote

access to Personally Identifiable Information (PII), possibly using Homeland Security Presidential Directive 12 (HSPD-12) Employee identification badges for all portable computers.

8. EAC's FISMA contractor will work with EAC information owners to review, refine, and finalize the provisional risk assessment. This will include a comprehensive review of threats and vulnerabilities, and a review of the National Institute of Standards and Technology (NIST) Special Publication 800-53 *Recommended Security Controls for Federal information Systems* security controls baseline already developed. Finally, a separation of controls into common and system-specific controls will be completed.

9. The EAC Privacy Officer has taken inventory of the PII systems and developed several draft policies and procedures related to protection of PII and privacy-related incident response. The FY 2009 EAC FISMA evaluation provides detailed guidance on areas in which EAC is still only partially compliant with PII and Privacy Act requirements, and EAC will formally adopt the PII recommendations from the FISMA evaluation as a guide to complete compliance. In particular, key PII policies will be included in the 2010 employee Privacy Act awareness training.

10. EAC IT staff will create a written itemization of every audit log type in use, will work with GSA to both identify and implement appropriate action on audit failures, and will develop a procedure to review these log files monthly and report errors to appropriate supervisors.

11. EAC will implement either a separate, limited-access "visitor" virtual local area network (VLAN) segment on the EAC network, or create a completely isolated wireless network for visitor access. In either case, there will be no visitor access to any resources on the EAC network, including network devices such as printers, scanners, and copiers.

Human Capital Management

In the management area, EAC provided a process for independent assessment and analysis of Human Capital Management in line with the Inspector General's management challenge. Management is addressing issues identified in the agency's second employee survey, through staff teambuilding efforts, staff focus groups, and employee retreats. A professional facilitating team was retained to provide guidance, assistance and evaluation of the overall issues identified in the Human Capital Survey.

EAC committed resources and time to move from a disclaimer opinion on our financial statements to an unqualified (clean) opinion in the second half of FY 2009. EAC continues to improve it programs and operations, strengthening internal controls, financial management, and information technology across the agency.