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

September 28, 2007

Memorandum

To: Thomas Wilkey
Executive Director

From: Curtis Crider
Inspector General

Subject: Non Compliance with the Federal Information Security Management Act by the U.S. Election Assistance Commission (Assignment No. I-EV-EAC-03-07)

The EAC has made improvements in the information security area, but additional actions are needed to bring the EAC into compliance with the Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) guidelines.

FISMA (Section 3544) requires the Head of each Federal agency to provide "information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of --

(i) information collected or maintained by or on behalf of the agency; and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency."

EAC is a small Federal agency; it has an annual operating budget of approximately $16 million and has 38 employees and contractors. More importantly, it does not own or operate any information technology (IT) systems. The EAC uses a Federal service provider, the General Services Administration (GSA) for its information technology needs. Thus, we believe, the impact of its non compliance is minor. Nonetheless, the Office of Management and Budget (OMB) advised[1] in its fiscal year 2007 reporting requirements that the EAC and GSA have a shared responsibility for FISMA compliance.

[1] See OMB Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act*, dated July 25, 2007.

DISCUSSION

Congress authorized the EAC with the passage of the Help America Vote Act (HAVA) in October 2002. According to HAVA, the duties of EAC are to "serve as a national clearinghouse and resource for the compilation of information and review of procedures with respect to the administration of Federal Elections . . . ." EAC's first full year of operation was fiscal year 2004.

The General Services Administration (GSA) provides administrative support and related IT services for personnel management, payroll, and financial management to EAC under three reimbursable agreements. GSA also furnishes IT support by maintaining EAC's Local Area Network and electronic mail. EAC's website is operated by an independent contractor.

EAC has not yet established policies and procedures for information security or privacy management.

RECOMMENDATIONS

We recommend that the Executive Director:

1. Establish and implement policies and procedures for information security and privacy management.

2. Comply with the applicable provisions of FISMA and OMB implementing guidance.

AGENCY COMMENTS

The EAC recently entered into two key contracts with third parties to comply with procedural requirements. First, the EAC contracted with firm to create a Continuity of Operations Plan (COOP), which is required by National Security Presidential Directive 51. The EAC anticipates receiving a COOP from the contractor on or before December 31, 2007. In addition to the COOP, the EAC entered into a contract with another firm to assist in (1) creating policies and procedures for processing Freedom of Information requests, (2) giving public notice of meetings pursuant to the Government in the Sunshine Act, (3) publishing a policy concerning records under the Privacy Act, (4) creating a common rule for grants, and (5) creating Touhy regulations. The EAC anticipates receiving a completed project from the firm on or before April 30, 2008. EAC has worked with the Office of Personnel and Management to identify an individual to assist in the development of agency policies and procedures including those identified in the recommendations of this report. It is anticipated that the contractor will begin work shortly after the beginning of the fiscal year.

RESPONSE TO MEMORANDUM

Please provide a response to this memorandum by November 3, 2007. Your reply should indicate whether you agree or disagree with the recommendations and, if applicable, include a plan of action for implementing the recommendations. The plan should include target dates and the name of the official responsible for implementing the recommendations

The legislation creating the Office of Inspector General requires that we report to the Congress semiannually on all reports issued, actions taken to implement our recommendations, and recommendations that have not been implemented. Therefore, this report will be included in the next semiannual report.