U.S. ELECTION ASSISTANCE COMMISSION
Office of Inspector General

Independent Audit of U. S. Election Assistance Commission's 2012 Information Security Program

Executive Summary

In accordance with the Federal Information Security Management Act (FISMA), the Office of Inspector General (OIG) engaged Leon Snead & Co. P.C. (LSC), an independent certified public accounting firm, to conduct an audit of the U.S. Election Assistance Commission's (EAC) compliance with the OMB Circular A-130 and FISMA requirements. FISMA requires federal agencies, including EAC, to perform annual independent evaluations of their information security programs and practices and report the results to the Office of Management and Budget (OMB). FISMA states that annual evaluations shall be performed by the agency Inspector General or by an independent external auditor, as determined by the Inspector General. The objective of this audit was to assess whether the EAC had developed, documented, and implemented an agency-wide information security program, as required by OMB Circular A-130 and FISMA.

Background – The E-Government Act (Public Law 107-347) was signed into law in December 2002. Title III of the E-Government Act entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement agency-wide 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 other agencies, contractors, or other sources.

The National Institute of Standards and Technology (NIST) is directed by FISMA to develop risk-based standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of the agency or other national security systems. OMB establishes policy for management of federal information resources and annual requirements under FISMA.

Summary of Audit - LSC concluded that EAC was in substantial compliance with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines for the security control areas that were evaluated. LSC determined that EAC had developed an agency-wide internet technology security program based upon assessed risk, and the security program provided reasonable assurance that the agency's information and information systems were appropriately protected. However, LSC did note one area relating to the vulnerability scans of EAC's internal network where EAC's controls and processes could be further strengthened. EAC officials took action to address the vulnerabilities identified. LSC tested the actions taken by EAC officials and confirmed corrective actions had been taken.

Recommendations and Management Comments – On September 17, 2012 EAC officials provided a written response to the draft report. In the response, EAC officials concurred with the findings and recommendations, and provided a detailed plan that was responsive.

This report contains sensitive information concerning the EAC's information security program. Accordingly, we do not plan to release the report publicly.