U.S. ELECTION ASSISTANCE COMMISSION
1225 New York Ave. NW – Suite 1100
Washington, DC 20005

OFFICE OF THE CHAIRMAN

Chairman Soaries' Remarks about Electronic Voting Security Strategy for the November 2004 Presidential Election

The increased use of electronic voting devices has created security concerns that the U.S. Election Assistance Commission must address. A priority of the EAC is to address security needs related to the use of electronic voting devices.

The EAC has been in discussion with election administrators, computer scientists, advocates, voters, scholars and other government and law enforcement officials about electronic voting security. On May 5, 2004 the EAC held a public hearing on the use, reliability and security of electronic voting devices. As Chairman, I will recommend that the EAC initiate the following strategy to insure election integrity and promote voter confidence in the administration of the 2004 federal election:

1. EAC should request that all voting software vendors allow election officials with whom they have contracted to analyze the proprietary source codes of their software and to protect that process by using appropriate nondisclosure and confidentiality agreements. EAC should assist in the analysis when needed.

2. EAC should ask every election jurisdiction that uses electronic voting devices to identify and implement enhanced security measures in November. Options include paper verification, voice verification, cryptography, parallel monitoring, chain of custody, testing practices, intergovernmental agreements for enhanced management, etc. EAC will offer best practices and guidance on specific methods and will assist in the identification and execution of security methods when needed.

3. EAC should invite every voting software vendor to submit their certified software to the National Software Reference Library (NSRL) at the National Institute of Standards and Technology (NIST). This would facilitate the tracking of software version usage. NSRL is designed to collect software from various sources and incorporate file profiles computed from this software into a Reference Data Set (RDS) of information. The RDS can be used by law enforcement, government, and industry organizations to review files on a computer by matching file profiles in the RDS. The NSRL was built to meet the needs of the law enforcement community for rigorously verified data that can meet the exacting requirement of the criminal justice system.

4. EAC should solicit information about suspicious electronic voting system activity including software programming and should request aggressive investigative and prosecutorial responses from the U. S. Department of Justice Elections Crimes Branch in the Criminal Division.

5. EAC should document incidents and record data concerning electronic voting equipment malfunctions in November. This information can be submitted to the EAC Technical Guidelines Development Committee that will be creating the new voluntary voting systems standards.