



ELECTION TECHNOLOGY COUNCIL

Working Together for Secure and Accurate Elections

Election Technology Council Issues Test Guidelines for System Reviews

The Election Technology Council (ETC) member companies fully support comprehensive testing and reviews of all election systems. We share the goal of voters, election officials, and policy makers that every vote cast is safe, secure, and accurate. The ETC also wants the voting public to have confidence in the election systems by knowing that each system must pass stringent testing before being used in an election.

Recently, in addition to standard state certification programs, several states have indicated they will conduct supplementary comprehensive reviews on the election systems used within their jurisdictions. Any review of an election system should accurately reflect the procedures, processes and protocols that election officials, poll workers, political party representatives and technical support staff use on Election Day and throughout the year to ensure the safety and security of their election systems. All election systems used in a jurisdiction should be subject to the same level of scrutiny, whether they are Direct Record Electronic (DRE) systems or paper-based systems.

A proper review of a voting system should begin with a set of objective criteria against which a voting system may be measured. Accordingly, a complete set of requirements should be well documented prior to the review process so that an examiner(s) may clearly understand what constitutes acceptable performance/design. It should be commonly agreed that a vendor will be judged solely upon conformance to requirements. To achieve these goals, the Election Technology Council encourages states to adopt the following guidelines for any such review of an election system.

- Experienced election officials with an extensive knowledge of the election process must be part of the election system testing team. Testing teams should review their findings with election officials to ensure that test results adequately reflect operational security protocols pursuant to state law and established best practices as applied by each jurisdiction. Election system review professionals such as members of EAC independent testing authority organizations should be considered as test team members.
- Accepted and commonly applied physical security procedures and protocols, such as locks and tamper-evident security seals which provide a monitored barrier from tampering, must be included in the tests.
- Industry standard electronic security measures such as passwords of appropriate length and difficulty should be in place throughout the systems as security barriers during the testing process. Also, standard network access control and security roles in the election management system must be employed.
- All review and test criteria should include normal public oversight of equipment staging, equipment delivery and tabulation processes on Election Day. This would include the public, county officials, and political parties.

- A manual, vote simulation or combination logic and accuracy testing regime should be part of any realistic system examination.
- State audit procedures, conducted following each election, should be included in the examination process. These procedures provide an audit of several facets of the system, including the comparison of electronic and paper based results.
- Paper based election results reports should be used in addition to redundant electronic results storage and voter verifiable paper audit trails (where applicable) to verify system accuracy.
- All software that will be tested should be verified through a digital comparison with the identical software version qualified by the federal government and stored in the National Software Reference Library (NSRL).
- Election system manufacturers should be provided adequate time to review the results of the test report for their respective system prior to public release. This will allow vendors to formally comment on and discuss these results with the assessment team and correct any factual errors before the results are delivered to the sponsoring office or agency and released to the public. In the interests of protecting the security of a voting system when in use, vendors should likewise be asked to comment on the advisability of disclosing not only certain software/firmware/hardware features, but also use procedures for the purpose of preventing the inadvertent release of information that could be used to subvert the voting process.
- States deploying system attack team scenarios should ensure the proper assembly of red team (assessment team), blue team (responsible for systems to be tested) and white team (managerial control) members are included in the testing process. Since attack team members will have access to sensitive materials, background security checks need to be conducted and proper safeguards need to be put in place around sensitive materials.
- Rather than initiating multiple testing events, states should consider combining their efforts or requesting any desired testing efforts be added to the federal testing process to gain efficiencies.
- Recommendations based on results of any testing need to consider the length of time necessary to make and certify any system changes. If there is not enough time to effect and certify a system change, alternative procedural recommendations, that can also mitigate any identified vulnerabilities, need to be articulated by the study and attack team members.

For more information contact:

David Beirne
Executive Director
Election Technology Council
14173 NW Freeway, #239
Houston, TX 77040
713.896.9292
dbeirne@electiontech.org