



Working Together for Secure and Accurate Elections

For more information contact:
David Beirne
Executive Director
Election Technology Council
14173 NW Freeway, #239
Houston, TX 77040

Safeguarding the Vote: Applying Best Practices to Mitigate Perceived Threats for Voting Systems

Overview:

Over the last few years, a number of procedures have been adopted by local jurisdictions to respond to perceived and potential threats to electronic voting systems. Regardless of the platform, there are a number of procedures that may be put into place by a local jurisdiction to respond to public concerns and reflect a proactive approach. As part of the Election Technology Council's continuing objective to serve as a resource for election officials, this document is designed to outline the perceived threats, mitigation strategies for these threats and some key procedures for the benefit of your jurisdiction and voter confidence.

Key Steps for Pre-Election Setup:

Below are a few key steps that each jurisdiction may take to establish that your voting equipment is operating as it should, is properly certified, and documents each step of the election definition process (process/time period):

Acceptance Testing (conduct upon receipt of equipment/continuous): Upon acceptance of your voting equipment, verify that the components specified in both the software and hardware versions match those currently certified within your State. In addition, verify the basic functionality of the equipment by conducting a series of response tests so the all components are operating as they should. The United States Election Assistance Commission recently issued a "Quick Start Guide" on this very issue which can be found at www.eac.gov.

Establish Clear Custody Controls (continuous): Inventory tracking systems, ranging from the use of bar coding and a simple database to a more robust product provided by a service provider, can be a critical component to your success. These tracking systems provide documentation on the specific chain of events associated with your voting equipment and provide an efficient means of accounting for all of your voting units. The use of tracking systems should be incorporated into all facets of your voting system including the physical voting units, memory cards, and ballot activation devices.

Pre-Election Hash Code Testing (conduct upon receipt of equipment and/or prior to establishing your election definitions and your absentee ballot programming): Hash Code testing is a valuable tool for use during the period of acceptance as well as for just prior to establishing your election definitions. More information on hash code testing and its software application is available directly from the National Institute of Standards and Technology (NIST) and its National Software Resource Library (NSRL). Trusted copies of software applications and firmware are also available from the Independent Testing Authority (ITA) that tested the voting system or system component. Hash code testing is a software application which verifies that the software incorporated within your jurisdiction is exactly the same as submitted during the federal certification process; it provides an extremely high level of assurance that the software has not been modified or altered in any way. For more instructions, visit

<http://www.nsrl.nist.gov/votedata.html> for step-by-step instructions and to find the listing of software versions and voting system providers currently on file with the NSRL.

Pre-Election Logic and Accuracy Testing (conduct as provided under your respective State law): Pre-Election Logic and Accuracy testing has been a fundamental aspect to the voting process for decades. Follow your normal procedures for conducting a logic and accuracy test, including the requisite number of ballots to verify the tabulation of all ballot choices. In addition, it is recommended that you prepare your own test deck in order to properly verify the operation of an optical scan voting system.

For electronic voting systems, it is recommended that you use a test deck, or test script, to verify the logic and accuracy of your absentee voting system and use another test deck to verify the logic and accuracy of early voting and Election Day votes cast. Some jurisdictions may opt to use the test deck to cast ballots directly into the electronic voting system. This will enable you to verify the logic and accuracy of the entire system and provide the opportunity to print your electronic ballot images, as you would in a manual recount, to verify the integrity of the electronic ballot images versus the original test deck. This method of conducting a logic and accuracy testing will document the integrity of your system as it originates from a paper ballot to an electronic cast vote record and then back to a paper record. This is essentially the same process incorporated by jurisdictions using an electronic voting system with a Voter Verifiable Paper Audit Trail (VVPAT).

Election Day Parallel Testing (Election Day) is a powerful tool to ensure that the voting system has been properly prepared and secured. Taking random samples of Election Day equipment to a central point for an Election Day Logic and Accuracy Test provides an immediate and sure check on the equipment, the election definition, and full system programming.

Post-Election Hash Code Testing (Conduct immediately preceding your post election logic and accuracy test): Post-Election Hash Code Testing is another tool to verify that the integrity of the software throughout the end-to-end process, after the distribution of the equipment to pollworkers and following the completion of your early voting and/or election day period.

Post Election Logic and Accuracy Testing (as needed based on state law): As a final check of verification of the tabulation settings, follow the same procedures as you administered for the pre-election logic and accuracy test.

Perceived Threats and Mitigating Steps

Perceived Threat #1: External Entry into Central Tabulation Computer

The perception that an external party could gain entry into the central tabulation computer is a common concern expressed about the inadequacy of electronic voting system security.

Mitigating Steps:

This threat is easily countered through the adoption of state and/or local requirements that tabulation computers are not connected to the Internet or any open network at any time, and by assuring that the physical and procedural security of the Central Tabulation Center is maintained at all times. For reporting of election results on election evening, the common practice of exporting the unofficial cumulative report summaries to an external device for transfer and subsequent upload to the Internet removes this threat in its entirety.

addition, sealing those ports on the units which are not relevant to the voting process will provide another layer of protection for evidence of tampering and possible quarantine on election evening for further review.

The use of parallel testing, as permitted under your State law, is also a strong mitigating step against this threat.

Perceived Threat #4: Insertion of virus through corporate malfeasance

This threat implies that a corporate insider would attempt to subvert the election process through the insertion of malicious code which is timed to coincide only within the election period itself and then shut itself down.

Mitigating Steps:

Logic and accuracy tests are normally performed to verify the correct tabulation of votes as the voter intended. You may undertake these additional procedures to provide greater protection and transparency:

1. Conduct your Pre- and Post Logic Accuracy Testing in full Election Mode **NOTE: Extreme caution should be used in this procedure to ensure that ballots used in the Logic and Accuracy Test are not inadvertently included within the official tabulation record;**
2. Work with your vendor to use test units and adjust their internal clock settings to mirror those of the early voting period and/or Election Day. **NOTE: Extreme caution should be used in this procedure in order to prevent these records/ballots from being inadvertently included within the official tabulation record;**
3. Perform Pre- and Post-Election Hash Code Testing;
4. Audit VVPATs (if available) through random sampling;
5. Election Day Parallel testing.

Summary:

Conducting these procedures will provide valuable information and evidence reflecting chain-of-custody controls and the proper function of your voting system. In their entirety, these procedures will position your jurisdiction well to respond to public concerns about system security or prepare for post election evidentiary hearings. Although each jurisdiction should maintain full control of their voting platform independent of their chosen vendor, it is recommended that election officials work with their voting system provider to develop clear procedures to foster this independence in a responsible way. The integrity of your election rests upon a robust series of interlocking procedures as outlined above and recommended by your voting system provider. Be sure you adhere to all recommended management techniques including password controls for length, structure, and frequency of change.

If you have not recently done so, invite your local media outlets into your office and brief them on the full array of procedures you employ to assure security, accuracy and integrity during your election setup. With the upcoming primary season and the general election, the need for a proactive media strategy and thorough poll worker training is very clear. As you are well aware, well-executed elections involve multiple processes coming together and this is certainly true when it comes to deploying election technology.

It is the hope of the Election Technology Council that these recommended steps and their real-world applicability will further assist you in your efforts to conduct fair and accurate elections. The Election Technology Council would also encourage you to visit the website of the United States Election Assistance Commission (EAC) at www.eac.gov and review their Quick Start Guides as they outline additional procedures and best practices for administrative procedures.