5. Testing and Certification of Voting Systems

Background

The current system for testing and certification is essentially a four-step process in many states:

1. Vendor testing

2. Qualification testing: For the past several years, qualification testing has been conducted by the National Association of State Election Directors and contracted Independent Testing Authorities. This task will now be the responsibility of the United States Election Assistance Commission (EAC). The National Institute of Science and Technology will staff the Technical Guidelines Development Committee of the EAC and will accredit laboratories under the National Voluntary Laboratory Accreditation Program. Hardware, software, and documentation of the voting system are to be defined, reviewed, and tested for conformity with the federal voting system standards. To be qualified, a system must contain a method to create elections, provide a ballot, record votes, report tallies, produce an audit trail, and ensure voting is secret, accurate, and reliable. An Independent Testing Authority reviews code and documentation to ensure it will provide an accurate election. Qualification testing does not mean the system complies with state standards.

3. State certification: State personnel or contractors perform testing under the direction of the state to ensure the voting system complies with all of the state's requirements.

4. Local acceptance testing: Individual jurisdictions perform testing before each election.

When it comes to voting machines, among the biggest but least focused on problems by reformers is that some states do not adhere to the voluntary federal voting system standards. A great many states do not have sufficiently rigorous state testing and certification programs to complement the federal process, and some states have no independent system for reviewing voting machines at all. Both federal and state procedures are important.

As the Leadership Conference on Civil Rights has pointed out,

> Certification standards serve a number of vital functions. Federal standards protect voters through such requirements as the new "second chance voting" provision. They deal with such issues as reliability, audit techniques, and security standards that are basic to ensuring that the voter's vote will be effective. Certification also protects state and local governments from voting machine manufacturers by providing technical specifications, testing and reliability measures, and operational standards. The national standards exist to ensure that a vote in California is as likely to be counted as a vote in Virginia, and they cover an extremely wide range of physical and administrative issues pertaining to the machines. It is through the national certification standards that policy goals and technical specifications are brought together. Bypassing the certification process undermines the important protections that ensure that voting systems meet basic accuracy, security and access goals.[39]

And in congressional testimony, Michael Shamos, a professor of computer science at Carnegie Mellon University, explained,

> Many states that formerly had statutory certification procedures have abdicated them in favor of requiring no more from a vendor than an ITA qualification letter, in some cases, even less. Alabama, for example, requires no certification at all, but relies

> on a written guarantee by the vendor that its system satisfies that State's statutory requirements. Mind you, these are requirements over which experts may differ as to their meaning. My own State, Pennsylvania, I am embarrassed to say, abandoned certification in the year 2002, because it believed the ITA process was sufficient. We are, therefore, less safe in 2004 than we were 20 years ago, and possibly less safe than we even were in the year 2000.
>
> Even certified machines may not operate properly when delivered to a jurisdiction, and must undergo acceptance testing, but I am not aware of any State that makes such testing a statutory requirement. It may be recommended in the standards, and the ITAs may recommend it, but there is no body that actually forces the states to go through acceptance testing.[40]

According to a 2004 report by Electionline.org, thirty-five states required voting systems to meet state and federal standards; nine relied entirely on federal standards; five used state standards; and Mississippi and Oklahoma had no voting system standards. The nine states that did not have their own standards were Alaska, Delaware, the District of Columbia, Georgia, Hawaii, Oregon, Rhode Island, Utah, and West Virginia.[41]

One potential model for state testing and certification is the system used in Georgia. After the state replaced all of its voting machines with the same DRE-style voting system statewide in 2002, Kennesaw State University established the Center for Election Systems to oversee and conduct Georgia's state certification program as well as to assist in its county-level acceptance tests. While there may be disagreement with some of the conclusions Kennesaw has come to with respect to the electronic machines Georgia uses, the idea of using an unaffiliated, nonpartisan, nonprofit institution composed of experts in the field to assist the state at every stage of the process of setting up, testing, and running voting systems is promising and should be explored further.

For states that opt to conduct testing and certification programs "in-house," we recommend looking at the rigorous procedures and standards put in place by the states of New York, Florida, and California. For example, New York imposes a number of requirements and obligations upon vendors on top of the federal standards. These include:

- Retesting of modifications;
- State board supervision of all local acceptance testing;
- Quarterly testing and annual testing for all new equipment;
- Escrowing of all source codes, software and design drawings.

The state also works with its own independent testing authority to examine and test all voting systems in the state. When a vendor applies to the state board, staff provides it with ballot format and test requirements, and the Independent Testing Authority establishes a test script for the examination and oversees testing and evaluation. The testing authority then provides a comprehensive report to the board.[42]

California has a Voting Systems and Procedures Panel working with the secretary of state to review systems submitted for certification. The panel works with an advisory committee and technical consultants, and its meetings are open to the public. The system is tested by conducting two mock elections, one a presidential primary, the other a gubernatorial election. The secretary of state schedules a public hearing regarding any item the panel considers. State procedures require local jurisdictions to conduct acceptance testing.[43]

In addition, last year California began a Parallel Monitoring Program, which "provided for the random selection of DRE voting equipment to be set aside for use by experts to test on Election Day, simulating actual voting conditions, to determine the accuracy of the machines to record, tabulate and report votes."[44] On election day in 2004, test teams comprised of employees of the secretary of state, consultants, and video operators did such testing in eleven counties.[45]

RECOMMENDATIONS

5.1 All states should adopt the new federal standards that will now be devised by the EAC and NIST.

5.2 All states should require voting systems to meet federal voting system standards *and* comply with the state's own testing and certification process and standards. As Douglas W. Jones, professor of computer science at the University of Iowa, has pointed out, the

purpose of the state certification system should be not only to ensure that the systems comply with any addition requirements the state might impose but to fill in any gaps in the vendor and Independent Testing Authority testing.[46] Changes or upgrades to software in electronic systems should be subject to a de novo review and certification, and penalties for installation of uncertified software or software upgrades should be stiff.

5.3 As suggested by the Leadership Conference on Civil Rights and the Brennan Center for Justice at New York University School of Law:

a. State elections officials should hire an independent security team to examine the potential for operational failures of and malicious attacks on the system.

b. The assessment performed by the independent experts should cover at least the following areas of concern:

i. Hardware design;

ii. Hardware/firmware configuration;

iii. Software design;

iv. Software configuration;

v. Election procedures;

vi. Physical security.

c. Elections officials should implement the critical recommendations of the independent expert security team and should demonstrate to experts and voters alike that these recommendations have been implemented.

d. Elections officials should provide a thorough training program for all elections officials and workers to ensure that security procedures, including those recommended by the independent expert security team, are followed even in the face of election day exigencies.

e. Elections officials should develop procedures for random parallel testing of the voting systems in use to detect malicious code or bugs in the software. Parallel testing involves selecting a random sample of the DREs to be used in the election and setting them up in mock precincts. Then, using all of the same procedures and during the same hours as the real election, mock elections are conducted in the mock precincts. Two separate mock elections should be conducted, one with real volunteer voters and one with trained personnel following a voting script that represents as accurately as possible the statistical voting profile of a precinct in the county. The entire process, and in particular what happens on the DREs' screens, should be videotaped. At the end of the day, after the mock precincts have been closed down, the mock election results must be reconciled with what the videotape shows that the results should have been.

f. Elections officials should have in place a permanent independent technology panel, including both experts in voting systems and computer security and citizens representing the diverse constituencies involved in election oversight, to serve as a public monitor over the entire process outlined above and to perform a postelection security and performance assessment.

g. Elections officials should establish standard procedures for regular reviews of audit facilities and operating logs for voting terminals and canvassing systems to verify correct operation and uncover any evidence of potential security breaches.

h. All jurisdictions should prepare and follow standardized procedures for the response to alleged or actual security incidents that include standardized reporting and publication.[47]

5.4 In states where more than one system is employed and/or machines are procured by localities, the state should encourage localities to have their own on-site demonstrations and testing. The focus of these tests should be usability by the voter, including disabled voters, and ease of use by poll workers.[48]

5.5 Machines should be tested again just prior to the election to make sure they are still working as they did when undergoing original testing and to verify that the machines are correctly configured for the specifics of the particular election.[49]

5.6 No state should contract with a manufacturer that has not been certified by the EAC; that will not make software open to the public, including source code and object code; or will not document the chain of custody.

5.7 No state should certify a system that exceeds the residual ballot standard established by the EAC. The residual ballot standard is the maximum error rate based on overvotes, spoiled or uncountable votes, and undervotes, less what the best research says is the estimated intentional undervotes.

◆ ◆ ◆

On a different machine issue, it is of great importance to note the problem of insufficient numbers of operating voting machines at a number of jurisdictions throughout the country in 2004, leading to long lines and wait times of several hours. For many working people, this could be tantamount to disenfranchisement. As Daniel Tokaji testified before the Committee on House Administration,

> Many Ohio voters waited for hours on or before November 2, 2004 in order to exercise their right to vote. The problems appear to have been particularly acute in some urban precincts here in Franklin County, where voters reported waiting for up to four or five hours. And at one polling place near Kenyon College in Knox County, Ohio, voters waited as long as ten hours. These lines posed a special difficulty for working people who could not be away from their jobs for that long, and for parents of younger children. It will probably never be known how many people were discouraged from voting, either because they arrived at the polling place to find lines stretching around the block or because they heard about how bad the lines were and thus never went to the polls in the first place.[50]

States and localities should reassess their voting system needs and base the number of machines deployed on election day on the number of registered voters in the jurisdiction as of the latest possible count. Jurisdictions ought also to take into account the following: voting-age population; voter turnout in recent elections; the number of voters who have registered since the most recent election; the educational levels and socioeconomic features of the jurisdiction; length of the ballot; and the needs and numbers of disabled voters and voters with limited English proficiency.