MAKING VOTES COUNT

Who Tests Voting Machines?

Published: May 30, 2004

Whenever questions are raised about the reliability of electronic voting machines, election officials have a ready response: independent testing. There is nothing to worry about, they insist, because the software has been painstakingly reviewed by independent testing authorities to make sure it is accurate and honest, and then certified by state election officials. But this process is riddled with problems, including conflicts of interest and a disturbing lack of transparency. Voters should demand reform, and they should also keep demanding, as a growing number of Americans are, a voter-verified paper record of their vote.

Experts have been warning that electronic voting in its current form cannot be trusted. There is a real danger that elections could be stolen by nefarious computer code, or that accidental errors could change an election's outcome. But state officials invariably say that the machines are tested by federally selected laboratories. The League of Women Voters, in a paper dismissing calls for voter-verified paper trails, puts its faith in "the certification and standards process."

But there is, to begin with, a stunning lack of transparency surrounding this process. Voters have a right to know how voting machine testing is done. Testing companies disagree, routinely denying government officials and the public basic information. Kevin Shelley, the California secretary of state, could not get two companies testing his state's machines to answer even basic questions. One of them, Wyle Laboratories, refused to tell us anything about how it tests, or about its testers' credentials. "We don't discuss our voting machine work," said Dan Reeder, a Wyle spokesman.

Although they are called independent, these labs are selected and paid by the voting machine companies, not by the government. They can come under enormous pressure to do reviews quickly, and not to find problems, which slow things down and create additional costs. Brian Phillips, president of SysTest Labs, one of three companies that review voting machines, conceded, "There's going to be the risk of a conflict of interest when you are being paid by the vendor that you are qualifying product for."

It is difficult to determine what, precisely, the labs do. To ensure there are no flaws in the software, every line should be scrutinized, but it is hard to believe this is being done for voting software, which can contain more than a million lines. Dr. David Dill, a professor of computer science at Stanford University, calls it "basically an impossible task," and doubts it is occurring. In any case, he says, "there is no technology that can find all of the bugs and malicious things in software."

The testing authorities are currently working off 2002 standards that computer experts say are inadequate. One glaring flaw, notes Rebecca Mercuri, a Harvard-affiliated computer scientist, is that the standards do not require examination of any commercial, off-the-shelf software used in voting machines, even though it can contain flaws that put the integrity of the whole system in doubt. A study of Maryland's voting machines earlier this year found that they used Microsoft software that lacked critical security updates, including one to stop remote attackers from taking over the machine.

If so-called independent testing were as effective as its supporters claim, the certified software should work

flawlessly. But there have been disturbing malfunctions. Software that will be used in Miami-Dade County, Fla., this year was found to have a troubling error: when it performed an audit of all of the votes cast, it failed to correctly match voting machines to their corresponding vote totals.

If independent testing were taken seriously, there would be an absolute bar on using untested and uncertified software. But when it is expedient, manufacturers and election officials toss aside the rules without telling the voters. In California, a state audit found that voters in 17 counties cast votes last fall on machines with uncertified software. When Georgia's new voting machines were not working weeks before the 2002 election, uncertified software that was not approved by any laboratory was added to every machine in the state.

The system requires a complete overhaul. The Election Assistance Commission, a newly created federal body, has begun a review, but it has been slow to start, and it is hamstrung by inadequate finances. The commission should move rapidly to require a system that includes:

Truly independent laboratories. Government, not the voting machine companies, must pay for the testing and oversee it.

Transparency. Voters should be told how testing is being done, and the testers' qualifications.

Rigorous standards. These should spell out in detail how software and hardware are to be tested, and fix deficiencies computer experts have found.

Tough penalties for violations. Voting machine companies and election officials who try to pass off uncertified software and hardware as certified should face civil and criminal penalties.

Mandatory backups. Since it is extremely difficult to know that electronic voting machines will be certified and functional on Election Day, election officials should be required to have a nonelectronic system available for use.

None of these are substitutes for the best protection of all: a voter-verified paper record, either a printed receipt that voters can see (but not take with them) for touch-screen machines, or the ballot itself for optical scan machines. These create a hard record of people's votes that can be compared to the machine totals to make sure the counts are honest. It is unlikely testing and certification will ever be a complete answer to concerns about electronic voting, but they certainly are not now.