Urgent Election Situation in Washington State

Recent Events That Affect Washington Voters

Rushed Changes to Election Software

Secretary of State Sam Reed and our county auditors assure us of the safety and security of our voting systems, in large part because the ITA labs that test them are approved by the National Association of State Election Directors. But six counties have installed new election software that has not been tested or inspected by any of these approved testing labs. There wasn't time. They only began the software revisions in June.

Installing new, unexamined election software after candidates are announced is an invitation to fraud. Yet this is precisely what has occurred in six Washington counties (King, Pierce, Snohomish, Kitsap, Klickitat, and Chelan).

In Six Counties

The new optical scan software and new election management software will be used not only for the September primary, **but also for the November general election.** Why is new software being installed?

- In Kitsap and Pierce Counties (which use optical scanner manufactured Election Systems and Software) and in Snohomish County (which uses Sequoia optical scanners), the new software was required to handle the consolidated ballot, so the change was a free choice of the auditors and approved by Washington Secretary of State Sam Reed. These counties could have used four ballots as most Washington counties will do.
- King, Klickitat, Chelan, and San Juan Counties use Diebold optical scanners. Election officials in Klickitat and Chelan told us they are installing the new software to handle the consolidated ballots, and the San Juan election director said they chose not to install it so close to an election but to use four separate ballots instead. In contrast, however, election officials in King County told us that the new software was required to handle the new type of primary and would have been necessary whether or not they used the consolidated ballot.

Why is the New Software a Problem?

There is no evidence that this new software will count votes correctly. Outcomes of elections could be in error.

Risk of Errors

New software is always a risk. Changes notoriously introduce new errors. All six counties have new software in their optical scanners and in their central tabulators. So errors could have been introduced in the new software applications or in their interaction with each other, and pre-election testing might not reveal them.

According to the "Electronic Voting Best Practices Summary" prepared by the Kennedy School of Government at Harvard University:

> Testing is necessary but not sufficient for a well-run election. Testing is never perfect, as it can overlook certain factors or interactions that may be easier to detect in hindsight. Systems interact with each other in unpredictable ways, often impossible to detect in a reasonable battery of tests.

Risk of Fraud

In Washington, the risk is even greater because of the timing. When new software is installed one month before an election, the risk of fraud is unacceptably high. The software has been examined by no one other than the software developers, and the developers knew who many of the candidates on the ballot would be.
Worse yet, they knew that no one would have time to examine the software before the election. So, it would be both easy and safe for them to add secret code to elect whomever they want.

Testing the software by scanning ballots prior to the election isn't sufficient. The software could easily be set up to operate differently during a real election, based on such variables as the date or inconsistencies in the types of marks on the ballots.

Risk to Half the State

Over half the population of Washington State lives in these six counties. The Secretary of State's website boasts a new voter registration database structured to minimize voter fraud, yet Sam Reed and the county election directors have maximized the potential for vendor fraud by installing new, unexamined software immediately before the elections.

Risk from Unchecked Vendor Involvement

This last minute change is irresponsible in the extreme, especially considering the track record of the companies.

- **Election Systems and Software** voting software so bug-ridden that the mayor of Miami, Florida is now ready to ban electronic voting machines altogether. This is the same company that illegally installed uncertified software in Indiana's voting machines because the certified version didn't tabulate the votes correctly.

- **Diebold Election Systems** is currently under investigation in California for illegally installing uncertified software in 17 California counties.

What are the Potential Consequences?

Increased Vulnerability to Legal Challenges

Since Secretary Reed's installation of the software with a high risk of error and fraud violated his own "Policy on Electronic Voting Systems," his actions leave the state extremely vulnerable to valid legal challenges by candidates after the election.

Under Washington Election Law, any judge or justice could delay the conduct or the certification of an election if the Secretary's actions constitute a wrongful act or neglect of his duty to safeguard the votes of the citizens of Washington. Such a high level of uncertainty could clearly qualify.

Risk of Expensive Lawsuits and Voters Disenfranchised

Considering the fact that both major parties are lining up lawyers preparing to challenge questionable results, the state is now vulnerable to expensive lawsuits based on very real grounds. So, beyond even the risk of election error and fraud, the Secretary's actions have created a situation in which all of Washington's voters could be disenfranchised for days, weeks, or months. Even worse, in the case of the Presidential Election, the votes of Washington’s citizens could be ignored permanently if the delegation to the Electoral College cannot be certified in time.

What is the Solution?

Immediate Official Protection

This last-minute software change has put our state at risk. Now the Secretary of State and the election directors in the six counties must implement a solution that safeguards our votes and protects our state budget.

Expert Opinion

We asked Dr. Douglas Jones to comment on the current situation in Washington. He is a Professor in the Computer Science Department of the University of Iowa. He has served on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems since 1994 and chaired that board from Fall 1999 to early 2003. Among his comments were these:

> This is not a good procedure. No software upgrade should be allowed without going through the ITA process.
>
> In the rare event that circumstances require late patching of a voting system, and particularly if certification is waived or done on a rush basis, additional defenses such as California-style random recounts (for paper ballots) or parallel testing (for direct-recording voting systems) should be required.

September Primary

The only reasonable solution for the September primary is for the election directors to conduct robust random manual audits. This means:

- Hand counting the ballots in a high percentage of the precincts, randomly selected after the polls close and evenly distributed over state and federal districts.
- Comparing the manual results to the machines' results.
- If there are discrepancies, manually counting all the votes for the races in which the discrepancies were found.
- The manual count would be the official count.

The auditor of Snohomish County plans to conduct parallel testing as recommended by Dr. Jones. The auditor of Klickitat County plans to audit 16% of her precincts to check the accuracy of the new software. We believe a 16% audit is reasonable and necessary for the other five counties.

November General Election

The best solution would be to revert to the tested and certified software for use in the November General Election.

If the election directors are unwilling or unable to revert to the previous software for the November Election, they must conduct comparable audits in November as well.