Testimony on Voting Equipment Selection

Phillip J. Windley

Oct 20, 2004

Chairmen Ferrin and Hickman, members of the committee:

My purpose in speaking to you today is to discuss issues that I believe present a real danger to the integrity of Utah's voting system. I am here as a computer scientist, a concerned citizen, and a former state CIO.

The vast majority of computer scientists, many voting organizations, and the ACM, the premier professional association for computer scientists, agree that electronic voting equipment is subject to subtle and potentially dangerous bugs and security vulnerabilities. These are not doomsday scenarios but very real and likely events given the nature of computer systems.

The consensus of computer and security experts is overwhelming: in a poll of members of the ACM, over 95% of the respondents felt that voting systems should provide a recountable physical record such as paper. On the other side of the issue, by contrast, we hear the same few national "experts" testify over and over again.

The most straightforward way to provide independent auditability is to add what's called a "voter verifiable paper ballot" or VVPB. A VVPB simply records the voter's intentions, allows the voter to verify that the ballot has correctly printed those intentions and is deposited separately from the voting machine to allow for an independent recount of the election results if needed.

Paperless voting proponents cite the expense of adding printing systems to voting equipment and caution that mechanical printing systems would be subject to frequent breakdowns. Inexpensive, reliable printers are used everywhere in our daily lives. We all insist on a receipt at the grocery store or the bank, why shouldn't we expect the same from our voting systems?

Some people believe that simply recording the vote on two different devices in the voting machine achieves the objective of creating an audit trail, but computer security experts know that this sort of plan is flawed. It's all too easy for the computer program, *regardless of how thoroughly it is tested*, to record the same mistake in two places. The only way to avoid this is to give the voter the control over a permanent copy, that can be deposited in a separate container for review if needed.

The State of Utah has approximately $28 million to spend on developing or purchasing new voting systems. The State's Elections Office recently issued a request for proposals (RFP) for voting equipment. I along with over a dozen other local computer science professors and voting experts sent a formal response to the Elections Office citing over a dozen deficiencies. Among those deficiencies were two of special import:

a.) The RFP does not require a voter verifiable paper ballot or any other kind of independent audit trail.

b.) The RFP does not specify what security requirements the equipment will have to meet in sufficient detail or allow enough time to complete such a security evaluation of the proposed equipment.

I believe that the RFP process is well intentioned, but nevertheless seriously flawed. The correct way to conduct the RFP would be to have the security discussions up front and then to write an RFP that requires vendors to meet specific requirements. Because this wasn't done, the RFP process has inadvertently, I believe, hidden the equipment selection behind a wall of secrecy. Consequently, I and many others are concerned about the evaluation process, who will do the evaluation, and the believability of the results. Hiring friendly consultants to do the evaluation is not acceptable. The State should not be afraid to subject their choice to the most stringent evaluation process possible.

Because selecting the proper equipment is so crucial to the integrity of the voting process, I urge the committee to take whatever action is necessary to ensure that the process is above reproach. The following are some possible actions that the committee might want to consider:

- Introduce legislation that requires voter verified, unalterable audit trails
- Ensure that the security evaluation is performed by independent, credible security experts, not friendly consultants.
- Examine the RFP process in detail to ensure that an acceptable outcome is still possible. If it is not, consider delaying the purchase until an acceptable outcome can be assured

Thank you for your time and for your efforts in this important work. I'd be happy to answer any questions that you might have.