PROBLEM SOLVING AND PROBLEM UNDERSTANDING

PROJECT NAME	ELECTRONIC VOTING SYSTEM
TEAM ID	NM2023TMID10620

Summary of the Problem with Electronic Voting

The 2000 presidential election and the consequential actions of Congress and the states are dramatically
changing the American election process. The Help America Vote Act (HAVA) passed by Congress in 2002
mandates reform of the election processes of all states. HAVA provides funding to replace obsolete voting
technologies such as punch cards and lever machines with more modern technologies such as precinct-based optical scanners and direct recording electronic (DRE) voting machines.
While HAVA includes a requirement that all voting systems must provide a manual audit capacity, its
definition of that requirement is ambiguous, and there are conflicting interpretations of its meaning.
Many elections officials have concluded that HAVA does not require a paper record of each ballot, verified by
the voter at the time the ballot is cast. As a result, over 100,000 paperless DRE voting machines have
already been deployed which lack the ability to produce a voter- verified paper ballot.
We are gravely concerned about the extensive reliance of voting machines that record and tally votes
exclusively through electronic means and provide no paper ballot that can be verified by the voter. We have
three major objections to entrusting our elections to these machines:

- Software errors are unavoidable
- Without a voter- verified paper ballot it is impossible to perform meaningful recounts
- The opportunities for fraud exist on a greater scale than ever before

Software Errors

No one knows how to write bug- free software. This fact is not in dispute. The more complex the software, the more difficult it is to find and fix bugs. Election software is very complex because of the wide variety of ballot types used across the nation, and it will contain errors, regardless of the skill and dedication of the engineers who design it and the programmers who code it.

Computer glitches are not uncommon. All of us who use computers know this. Undoubtedly, software errors will cause problems in future elections, just as they have in past elections. Here are three of the many examples of computer errors reported in newspapers in recent elections:

- Cateret County, North Carolina, November 2004: software problems caused 4,438 electronic ballots to be lost and never recovered. The vendor acknowledged responsibility for the loss.
- Fairfax County, Virginia, November 2003: testing ordered by a judge revealed the several voting machines subtracted one in every hundred votes for the candidate who lost her seat on the school board.
- Broward County, Florida, January 2004: 134 electronic ballots were blank in a one-race election held on DRE voting machines in which the margin of victory was 12 votes. Florida law required a manual recount of the ballots, but that recount was impossible because there were no physical ballots to recount.

These and many other reports of computer problems present us with an obvious question: how many election results were compromised by unnoticed computer errors and malfunctions? Of course, we have no way of knowing. These reported cases were detected, but it is only reasonable to assume that were other undetected errors, and we will never know how many.

Impossibility of Meaningful Recounts

Trusting our votes to a wholly electronic process of recording and storage leaves us completely without recourse if that electronic process fails - and history shows that the process fails all too frequently. DRE voting machines do allow voters to inspect and correct their choices on the touch screen’s final summary display prior to casting their vote. But, DREs do not provide voters any method for inspecting how their vote is stored inside the DRE’s electronic memory. Thus, the electronic ballot records stored in those memory circuits are completely invisible to and unverified by the voter; they are also alterable. Yet it is the contents of that invisible, impermanent, and unverified computer memory that are used to total up the votes.

Without voter- verified paper records that accurately reflect the voters’ choices, it is simply impossible to perform a meaningful recount. While most DRE voting machines can print a paper record of the votes cast, this report is not generated until after the polls have closed, and is nothing more than a printout of the electronic records. If the electronic record is inaccurate, then the printed report will also be inaccurate. Such a printout is not voter- verified and does not provide an audit trail appropriate for a meaningful recount.

Consider this scenario, not unlike events that have occurred in past elections: A voter marks the appropriate locations on the voting machine’s touch screen, reviews the choices, and gives the command to cast the ballot. Due to a software problem or malfunction, the computer records the ballot incorrectly, or not at all. The voter leaves the booth, and at the end of the day, the poll worker prints out the ballot images. The voter’s votes are incorrectly tallied and the printed ballot image is incorrect, but this error goes undetected because the voter is not there to view the printed version. But because the printed version of the ballot images all match the electronic records (as they must, since one is simply a copy of the other), elections officials proudly report that they have successfully conducted yet another flawless election.

Opportunities for Grand- Scale Fraud

Election fraud is not unknown in previous American elections, and it is not unexpected in future elections. However, the opportunities for fraud provided by electronic voting machines surpass all the opportunities available previously. For example, a corrupt insider, working for one of the vendors of widely- used voting machines, could hide malicious code in the software. That vendor could then unwittingly distribute that malicious code to thousands of machines across the nation and alter the election results in every state where those machines are used. Existing testing and certification procedures for DREs are voluntary and currently insufficient to guarantee that this type of tampering will be detected. Elections officials are usually not computer security experts and most do not fully appreciate the security vulnerabilities of DRE voting machines.

Concerns about fraud are not simply speculation. A 2003 study by Johns Hopkins and Rice University computer experts revealed hundreds of security flaws in the software of a leading manufacturer. Two separate studies commissioned by Maryland (the SAIC and RABA reports) confirmed many of those findings and identified additional vulnerabilities. An Ohio study of the four major voting machines has shown them all to have serious security vulnerabilities. That study prompted the Ohio Secretary of State to delay the installation of DRE voting machines in that state until after the 2004 election.

A Reasonable Solution

How each voter votes is a private matter. But how those votes are counted is everyone’s business. When voters cast their ballots, they must be able to verify that their choices have been accurately and permanently recorded on that ballot. They must also be ensured that their ballots cannot be altered or deleted after they have verified them, and that their voter- verified paper ballots are available for a meaningful recount, including manual recounts where required by law.

There are now several vendors of voting machines that provide both accessibility to voters with disabilities and a voter- verified paper ballot. In addition, a major vendor of DRE voting machines is now supplying printers that can be retrofit onto its previously- paperless systems; those retrofit printers were used successfully to produce voter- verified paper ballots on the DRE voting machines used in the September 2004 primary elections in Nevada.

Accordingly, a reasonable solution to the problem with electronic voting is to pass legislation requiring all DRE voting machines to provide a voter- verified paper ballot that is saved in a ballot box for use in recounts and audits. Since HAVA mandates that all voting systems must (by 2006) provide equivalent accessibility to voters with disabilities, any such voter- verified paper ballot system must also be accessible by that date.

In the last session (the 108th), several bills were introduced in the U.S. Congress that would establish such a voter- verified paper ballot requirement for all voting systems. While these bills differed in the details of their implementation and in their effective dates, all would have established a voter- verified paper ballot requirement by 2006. As of October 2004, the combined cosponsorship for these bills included members of both parties and totaled 192 members of the House and 20 members of the Senate. Of all of the VVPB bills that were introduced into the Senate, only the Ensign amendment, S. 2437, attracted bipartisan support.