VotersUnite!

Ellen Theisen
Executive Director

John Gideon
Information Manager

www.VotersUnite.org

May 25, 2004

U.S. Election Assistance Commission
1225 New York Ave. NW - Suite 1100
Washington, DC 20005

To the Members of the Election Assistance Commission:

For the past 22 years, I have written technical documentation for software. I have been involved in the software development process of dozens of companies, have tested software, and have a working knowledge of the way software is written and debugged. Nine months ago I heard that electronic voting was on the increase. Ever since, I have been working very hard to educate the public about the serious dangers inherent in electronic voting.

People who do not know software are not aware of how much they don't know about it. Yet, in general, the people with decision-making authority do not have a background in software. Because of this, too often, those in authority are relying on irrelevant information when they make decisions about our voting systems.

The purpose of this letter is to point out 20 important items of information that are relevant to voting systems. Unfortunately, this information is not obvious to those who have not been involved in the process of developing software, and many of these points have not been made by the computer professors who have provided testimony to you.

Please note that these 20 points are interrelated. They are different facets of a complex issue, and together they show that the use of electronic voting is an unfixable problem. I encourage you to check the accuracy of my software assertions with a random group of software developers who have not been active in the issue of voting machines - just to verify my claims about the software development process.

1) Released software has bugs - always. Some of these flaws are known when the software is released. Some are detected later. No one knows how many are never detected.

2) A software "glitch" is a software malfunction. "Glitch" implies something not very serious, something like a bump in the road. But "glitches" have been known to lose votes and to hand votes to the opponent. Moreover, if the software malfunctioned once, it will do it again. That's the nature of software. If it does the same process twice, it will do it exactly the same way both times.

3) Fixing a bug may introduce a new bug. Often a "fix" introduces a new bug or gives an old, undetected bug new life. That's why software companies test and test and test again after bugs have been fixed. "Patch" is an innocuous word, like "glitch". But a patch means that the code has been changed, always a risky venture. Software is so very, very precarious. Developers know that. The general public doesn't.

4) Elections are beta tests of the voting software. This was the point of the letter I wrote to you before your hearing on May 5. It is a crucial point that, unfortunately, has not been given enough attention by computer experts who work with software theory and are not involved in the day-to-day development process. A beta test is a field test of the software. It is well known in software development circles that in-house testing (alpha testing) only catches some of the bugs. So reputable companies do beta testing before releasing a product. They send the software product to target users, have them work with it for a while and report the problems they encounter. The company fixes the problems, and then - only then - is the product worth the purchase price. Only then can customers be reasonably certain it will operate fairly accurately without causing problems on their computers.

Elections are field tests for Diebold, ES&S, Sequoia, Hart, and the other voting machine manufacturers. It isn't possible to find the variety and quantity of users required for an adequate field test except by holding an election. It's as simple as that. The problems we have seen in recent elections prove the truth of this point. They are exactly the types of errors that would show up in a beta test. They are bugs that were not found during the in-house testing, so they were encountered by the target users.

However, elections don't provide the normal benefits of beta tests. They don't provide for systematic reporting of bugs so that the bugs can be fixed. Neither voters nor election administrators are requested to watch for problems and report them to the manufacturer. So, the next election on the same equipment is yet another beta test, with the risks and not the benefits.

5) Only inadequate software allows user errors to cause serious problems. Software development companies spend a great deal of time, energy, and money to ensure that users can make errors without destroying data or wasting time recovering from errors - thus the "Undo" command that is now a standard part of virtually all software. So when an election is chaotic because of user error - either poll workers or voters or both - the fault lies with the software. ALWAYS.

6) Voting software is used differently than any other software. This means that the reliability of any other software DOES NOT APPLY to voting machine software. Virtually all other software applications are designed to give feedback to the user. That's their purpose. The user enters input, the computer does something to it and hands back the results to the user. This is true in a spreadsheet, a word-processor, a computer game, an aviation program.

As users work with the software on a daily basis, if they notice things that don't mesh, they often they report it to the manufacturer to be fixed in the next release, or they ask for a refund. We are so used to working with software that gives constant feedback, and gives it correctly, that we now take it for granted. When I save a file and then open it again tomorrow, I see the same data I had in the file yesterday. It is important to realize that it was complex software processes that accomplished both the saving and retrieving tasks correctly. It seems natural for software to do its processes correctly. But it isn't natural. Software companies spend an enormous amount of time, effort, and money to make sure that the feedback their applications give to users constantly, daily, minute-by-minute, is accurate. That's the only way they can make a profit.

Voting machine software is completely different. It is specifically designed NOT to give feedback to the user, except for the screen feedback at the time of the voting. Note that the screen image is only a representation of the ballot, not the ballot itself. The user never views the actual ballot. Then, the significant processes - the recording and counting of votes - do not give feedback to the user. Once the data is saved, the user never looks at it again. The people who see the results are those who have no idea what the input was. This presents an insurmountable barrier to determining the reliability of the software.

So comparisons to ATMs or any other software at all are irrelevant.

7) An electronic record is not a permanent record. One of the hallmarks of electronic records is that they are easy to change, and they can be changed without any indication that a change took place. HAVA requires a permanent record of each vote. Electronic records do not satisfy that requirement. Printing ballot images at the end of the day does not qualify as a permanent record, since there is no assurance that the image matches the actual ballot as cast.

8) Electronic elections aren't transparent. Neither election administrators nor the public can watch the ones and zeros moving around recording votes, retrieving votes and counting them, tabulating the results. Election officials can have all their procedures in place perfectly, but the processes that do the most important work of an election are not visible to them, and they are not in control of them at all.

Only a transparent election can give voters confidence in the outcome. Electronic elections, by definition, are NOT transparent.

9) Version control will remain a permanent problem. Version numbers are carefully controlled in companies that depend on the accuracy of the tracking to maintain high profits and good customer relations. It is difficult to accurately track the many different preliminary versions that are built during the development process, so software management applications have been created simply to help software engineers track and manage the versions. When multiple programmers are involved in the process, the management task is more complex and more crucial.

More importantly, checking the version number stamped on installed software is no assurance that the version indicated is the one installed. It is trivial to create and install software stamped internally with an inaccurate version number.

10) The certification process hinders the development of good voting machine software. When a bug is found - a common occurrence - it should be fixed. But with the NASED qualification process followed by the state certification process, costing something around $100,000 for each new version and taking anywhere from six months to two years, how can voting machine vendors fix bugs in an efficient manner? They can't. The certification process is incompatible with the software-development process. What if Norton had to get every virus definition file ITA-qualified and certified? What if Microsoft had to wait six months to two years between Windows updates (which, as you may know, are bug fixes)?

11) The qualification-certification process has proven itself to be a failure. Hundreds of serious election problems have occurred on voting machines in the last two years. All of them have occurred with federally-qualified, state-certified equipment. Having a NASED number is absolutely no indication that the machine will function properly.

12) The people who made the malfunctioning hardware also made the software. It is not unusual to hear of voting machines overheating and breaking down during an election. How many times has your Dell or Compaq overheated and broken down? It just doesn't happen. Voting machine hardware isn't even adequate. Sometimes these computers take 40 minutes to boot up. They just quit working correctly, right in the middle of an election. Touch screens are misaligned. Sensors don't sense correctly. The people who developed these inadequate hardware devices also designed and developed the software that runs on them. There is only one reasonable conclusion - the software is equally inadequate. And, of course, we see the evidence in election after election.

13) Vendors control electronic elections, regardless of election administrators' diligence. With electronic voting, ballots are recorded and tabulated by software processes, which are:

- Developed by software engineers, who are hired by vendors.
- Federally qualified by testers, who are hired by vendors.
- Installed and maintained by technicians, who are hired by vendors.
- Trade secrets of the vendors and therefore not open to public scrutiny.

If Direct Record Electronic (DRE) voting machines are equipped with a printer to print voter-verified paper ballots (VVPB), the printers and the software that drives them will be developed, tested, qualified, installed, and maintained by the vendors.

Attempting to manage an electronic election with administrative procedures is like using a metal detector to find a ghost. Election procedures are irrelevant to whether or not the software will perform correctly. We see evidence of this in election after election. Administrators are being held responsible for something over which they have no control - and most of them don't even realize it.

14) People who don't understand computers are managing computerized elections. Election officials all over the US are attempting to run electronic elections using procedures adapted from the procedures for paper ballots. Most of the officials aren't knowledgeable about computers or software. They may be trying diligently, but they aren't qualified to do what they are being asked to do. Many of them realize they are over their heads, and so they attempt to maintain a good relationship with vendors whose help they rely on. Since virtually none of them are computer professionals, in general, they have no idea how far over their heads they are.

As a software technical writer, I have dealt with novice users for 22 years - intelligent, competent novices. They are completely befuddled by computers. Most people are. Other than computer professors and computer professionals, everyone is befuddled by computers. Procedures for running electronic elections are being established and implemented by people who are befuddled by electronics.

15) Poll workers are monitoring equipment that is a mystery to them. Chairman Soaries has recently expressed concern that it is difficult to find enough poll workers. As elections become more and more technical and complex, the crisis becomes more severe. Most people are computer novices. Yet in an electronic election, poll workers are required to be in charge of operating computers. Even if employers give people the day off to work at the polls, it will be difficult to find enough people who want to do this and who also are knowledgeable about computers.

16) VVPB does not provide a true audit of the machines. In a recent letter to the Sante Fe Reporter, Denise Lamb, Director of New Mexico's Bureau of Elections, pointed out the inherent impossibility of conducting a true audit on VVPB:

"It cannot be on a continuous roll of paper, since that would erase any secrecy of the ballot and allow each voter to be identified by the order in which the ballot was cast. If the tape is separated, then the integrity of the trail is lost."

This means that VVPB does not provide a way to audit the systems, as required by HAVA.

17) VVPB will not safeguard our elections. It cannot safeguard against:

- Bugs or malicious code in the software.
- Inadequate testing.
- Legal restraints on fixing software bugs in a timely manner.
- Legal restraints on fixing software bugs before an election.
- Historically inadequate certification process.
- Intimate involvement of vendors in the electoral process.
- Computer novices running electronic elections.
- Security procedures developed by officials who are befuddled by computers.
- Malfunctioning hardware.
- Nonexistent checks and balances, since there is no input/feedback process.
- Printed records that might not match the electronically recorded votes.
- Printed records that trusting voters have not verified.

Adding VVPB is adding a printer that may or may not break down onto a machine that may or may not operate correctly, in order to print a record that may or may not match the electronic record of the vote, and which may or may not have been actually examined by the voter, and which may or may not ever be looked at election officials.

This is not a safeguard.

18) Open source code will not safeguard our elections. Software has bugs. Even qualified programmers cannot examine thousands of lines of source code and find all the errors. ITA qualification, which has been repeatedly awarded to malfunctioning software, has proven this fact many times.

19) Random recounts of VVPB are not a realistic safeguard. Unless we can be certain that voters examine the VVPB, then we cannot be certain that a manual recount reflects the will of the voters. However, when voters complete a paper ballot, we know that voters have examined the ballots that are being recounted.

Note also, that if random recounts showed a significant difference between the paper ballots and the electronic tally, all elections run on the same type of machine - everywhere in the United States - should also be manually recounted.

20) Auditable, less expensive, more reliable voting systems are available. Optical scan systems with a disabled-accessible ballot-marking device such as the AutoMark, or ballot-printing systems such as the Open Voting Consortium system, are significantly less expensive and more transparent. In addition, they provide a permanent source document - as is required by any valid auditing system.

The many complex, interrelated problems inherent in electronic voting make it very clear that election integrity is not served by electronic voting. I urge you to advise against it.

Respectfully,

Ellen Theisen

Ellen Theisen
Port Ludlow, Washington
www.ellentheisen.com
Co-founder of VotersUnite!
www.votersunite.org