ELECTION ASSISTANCE COMMISSION HEARING ON THE USE, SECURITY AND RELIABILITY OF ELECTRONIC VOTING SYSTEMS

STATEMENT OF
ALICE P. MILLER
EXECUTIVE DIRECTOR
DISTRICT OF COLUMBIA
BOARD OF ELECTIONS AND ETHICS

Wednesday, May 5, 2004

Good afternoon Chairperson Soaries and Members of the Election Assistance Commission. Thank you for the opportunity to appear before you and present this testimony on the use, security and reliability of electronic voting devices. I am Alice P. Miller, Executive Director of the District of Columbia Board of Elections and Ethics. I have served in this capacity since 1996. Prior to my appointment as the Elections Director for the District of Columbia, I served as the General Counsel for the Board. I worked in the General Counsel's Office as either the senior staff attorney or the General Counsel for a total of eight years prior to my current appointment.

With a combined total of over 16 years in Election Administration, I have been working in the field of elections for the greater part of my professional career. My experience has provided me an opportunity to observe, and review a multitude of election operations from both the legal and the administrative perspective. Clearly, this does not make me more or less competent to testify on the issues at hand but it does allow me to offer testimony based on practical and real experiences with voters, candidates and pollworkers.

This hearing is on the "use, security and reliability of electronic voting systems." These terms mean different things to different people, so let me begin by defining what they mean in the context of the District of Columbia.

What is an electronic voting system? Does this term apply only to systems that record the votes electronically, or does it also apply to voting systems that tally the votes electronically. For example, while optical scanners require voters to record their votes on paper ballots, the tallying is performed electronically and, in our case, the tallying occurs at the precinct on Election Day. Therefore, the District of Columbia, which uses both optical scan and electronic touch-screen voting systems, essentially uses an all electronic system.

When looking at the "use" of electronic systems, the first question to ask is, "Who is the user?" User in the context of elections must include, not only the voter, but also the pollworker. If the voting system is not "usable" by pollworkers, then the voter may never have the opportunity to become a user. The challenge of making systems usable by pollworkers applies to both the optical scan and the DRE systems.

When we talk about the security of an electronic system, security should not be confined to the security of the system itself but must include the administrative procedures in place to secure the system. It is, I think, misleading to look at the issue of security as an isolated feature of the voting system. These systems are not used in a vacuum, they are one component of a much larger system.

Some of the security vulnerabilities that computer security experts point to can be easily remedied with simple administrative procedures. While many of these procedures are just common sense, they nevertheless require time and manpower – two elements that are in very short supply in most election offices.

Similarly, when we talk about the reliability of voting systems, it is a mistake to look only at the reliability of the machines themselves. How reliable are the administrative processes for maintaining the machines?

In short, we need to take a more "holistic" approach to ensuring that voting systems are usable, secure and reliable.

On January 13, 2004, the District of Columbia held its Presidential Preference Primary. At this election the District of Columbia debuted its dual voting system, i.e. an optical scan voting system and an accessible touch screen voting system. Both systems were available in all of the District's precincts statewide. Voters could select the system they preferred to vote on. The use of the dual system in the District of Columbia provides a case study that raised issues every election official will need to address in using electronic voting systems.

First, as I said, the pollworkers' interaction with the voting system is, in effect, equally important as the voter's. If one voter cannot use the system, one voter is disenfranchised; if one pollworker cannot figure out how to operate the system – from something as simple as turning it on to a more complex matter as recovering from an error – then many voters are potentially disenfranchised.

The average age of a DC pollworker is 68. While they are willing to learn how to use electronic systems, many of them do so with fear and trepidation. At some polling stations, we found that pollworkers had positioned the new DREs in dark corners, hopeful that the voters would not notice them or ask to vote on them. Despite the reluctance of some pollworkers to encourage the use of electronic systems, a third of our voters chose to vote on the touch-screen machines. Voters like voting electronically.

Prior to the January election, we recruited “precinct technicians,” a new pollworker position. We trained these technicians exclusively on the operation of the DRE. Their presence at the polling place increased the comfort level of our senior pollworkers. Yet even with the assistance of the precinct technicians, we still experienced problems with some of the DREs that were only solved with the assistance of the vendor.

In the future, we will look for ways, including more focused training, to empower and enable pollworkers to perform basic troubleshooting operations without the assistance of the vendor’s technicians.

Pollworkers also had difficulties with transmitting the results from the optical scanners. Approximately one third of the precinct workers failed to send the results by modem from each precinct to the central office. As I said, many of our pollworkers are uncomfortable with the new technology.

Pollworkers are also responsible for implementing one of the important features of the optical scan systems, that is, facilitating second-chance voting as required under HAVA. A pollworker stands by as the voter feeds the ballot into the scanner and then advises the voter whose ballot has been rejected. This is a sensitive situation that could potentially compromise the secrecy of the ballot. I bring this up to drive home the point that the pollworker is an essential part of the voting system. The machines must be usable by pollworkers.

And then there’s the voter’s interaction with the ballot review process. For whatever reason, many voters appear to be reluctant to remake their ballots. Perhaps they do not want to take the time. Or perhaps they are embarrassed. Or perhaps, even, this is what they intended – to over-vote and essentially cast a ‘no vote’ in a specific contest or in all contests. In any case, while the optical scan system provides the opportunity for second-chance voting there are more obstacles than with an electronic system. This means, in effect, that a voter using a DRE can easily, and with a perceived higher degree of privacy, change his or her ballot choices before casting the vote. These voters are more likely to make any desired changes to have their vote counted as intended.

When we talk about reliability, we need to talk about reliability on Election Day and reliability over time. In January, the Board got a fairly clear picture of how reliable the systems are on Election Day; we still do not know how reliable they will be four years from now. And this question leads to another important question: what is the cost of maintaining these systems over time?

Also, issues of reliability on Election Day are closely tied to issues of usability. What at first looks like a machine problem may, in fact, be a problem with pollworker training. Or the problem may be the result of an administrative glitch. For example, is there a double check to ensure that the correct voter card

activators – these are the devices that tell the voter card which ballot should be called up on the touch-screen machine – have been deployed to the precinct.

These issues are distinct from issues specific to the voting device such as voter cards getting jammed or re-calibration problems. The end result is the same, however: voters potentially are disenfranchised.

Finally, let me address the issue of security. Public debate on this issue has focused on the machine itself. As Brit Williams has pointed out, there are a number of administrative procedures that can mitigate the risks and certainly prior to the November election, every election official should review administrative procedures with an eye toward strengthening security.

In the District of Columbia, we have set up a system that combines prohibiting access to sensitive equipment and software as well as monitoring access. We recently implemented new software that allows us to monitor every attempt – successful and unsuccessful – to gain access to the server. This server is not connected to the Internet and is kept in a locked closet. Currently, the biggest risk to our system has to do with climate control problems in our headquarters.

Like Georgia, we restrict access to the voting systems and once the ballot information has been loaded we hire a private security firm to guard the machines. The warehouse is not identified as belonging to the Board of Elections; there are no identifying signs. Voting machines are sent to the polling place before the election and security is provided in all polling places where the machines cannot be locked up.

These administrative procedures provide a layer beyond whatever safeguards exist in the machines themselves.

I have heard speculation that corrupt insiders might be able to hack into electronic systems and tamper with the software. I would suggest that if you have employees who are willing to help rig an election through software tampering, your problem is a lot bigger than just the voting system.

The District of Columbia is unique. The combined optical scan and DRE system works very well for this jurisdiction. Using both optical scan and DREs shielded the District of Columbia to a certain extent – voters who did not feel comfortable voting electronically had the option to vote a paper ballot. Also, arguably, it is harder to tamper with or rig results coming from two separate systems.

A lot of attention has been paid to the security risks involved in using electronic voting systems. The concerns that have been raised are certainly valid. That is why I would urge Congress to fully fund this Commission. We desperately need standards that have the full confidence of the public. I look forward to working and cooperating with the Commission in this effort. In this spirit I hope the

Commission will be able to devise a system or process that will track the problems, challenges, and successes associated with the voting systems. This is something that could be done in conjunction with the development of any relevant standards produced by the Commission working in conjunction with NIST.

If, however, we are talking about relative risks to valid votes, there are, unfortunately, far more likely scenarios costing eligible voters their votes such as voters not understanding how to complete the ballot or pollworkers giving voters the wrong ballots.

The challenge of training both new and veteran pollworkers how to use new systems cannot be overstated. Even with ballot review and in-precinct scanning, the voters themselves are likely to make errors. Absentee voters will not have the advantage of in-precinct scanning. And then there is the chaos of Election Day. Accidents happen. Things go wrong. In some ways, the most important security measure for any election administrator is to make sure there's a Plan B. Between now and November, these are the issues that must be addressed to ensure that every eligible voter in the District of Columbia is able to cast a vote and have that vote counted as cast.

Thank you for the opportunity to present this testimony and I am available for questions.