Testimony before the
Senate Committee on Rules and Administration
Hearing on Security and Reliability of Electronic Voting

February 7, 2007

Britain J. Williams, Ph.D., Professor Emeritus
Kennesaw State University

Introduction

I would like to begin by thanking the Committee for the opportunity to appear before you. I have worked in the arena of computer based voting systems for over 20 years and appreciate this opportunity to share with you my experience and opinions on this important matter of voting system security. I will begin with some background information and then conclude with some recommendations on what seems to me to be the major issues before the Committee.

Background

In 1964, the IBM Corporation introduced a voting system that utilized punch card ballots to tally elections. This system operated on IBM main-frame computers and, thus, was only available to jurisdictions that were large enough to have access to a main-frame computer. These punch card systems were viewed by election officials as a major improvement over the then available voting systems: manually counted paper ballots and 800 pound lever voting machines.

In the 1980's, when micro-computers became universally available, this punch card voting system was ported to micro-computer technology and, as a result, became available to small election jurisdictions. Soon, over 40 % of the voting population was voting on punch card voting systems.

In the late 1980's, optical scan computer technology matured and gave rise to the development of optical scan, sometimes called mark sense, voting systems. These systems had the desirable feature of presenting the voter with a ballot that resembled the familiar manually counted paper ballots. By

the end of the 1980's, the voting population was about evenly split between lever voting machines, punch card voting systems, and optical scan voting systems.

Direct recording electronic voting systems, widely referred to as DRE voting systems, appeared in this time frame. These early DRE voting systems were operated by a row of buttons arranged along the edge of a computer display. Few of early systems were sold and implemented. DRE voting systems did not become widely accepted by election officials until the 1990's when touch screen technology became reliable and relatively inexpensive. Since their introduction, DRE touch screen voting systems have been the fastest growing segment of the voting system market.

There are several reasons for the success of DRE voting systems. The DRE ballot station eliminates the need for a large volume of paper ballots in polling places. Like the lever voting machine, the DRE voting station can prevent over-voting. Unlike optical scan voting systems, the DRE voting station allows a voter to change her ballot choices at will without the necessity of voiding the ballot and issuing a new ballot.

Also, a DRE voting station can store the ballot images for an entire jurisdiction and, for most states, the entire state. This feature has enabled the implementation of vote centers, such as in Colorado, where electors from multiple precincts can vote at a vote center without the necessity of returning to a specific precinct. Ultimately, this capability will enable precinct independent voting, allowing an elector at any location in a state to vote in the nearest vote center. In addition, vote centers will reduce the need mail-in absentee ballots, for one of the major sources of fraud in elections. Another major advantage of DRE voting stations is that for the first time in history a blind person can vote entirely unassisted.

There has been a lot of concern expressed recently about the possibility of election fraud perpetrated by hackers attacking the computers in a DRE voting station. The computers used in the early mainframe based punch card voting systems, the computers used in the mini-computer based punch card voting systems, and the computers used in the current optical scan voting system are equally as vulnerable to these types of attacks by hackers as the computer in a DRE voting station.

However, in the entire 43 year history of the use of computers to tally elections, there has not been a single incident of an attempted hacker attack against the computer in a voting system. This is probably due in large part to the fact that voting system computers are not attached to computer networks and, thus, cannot be accessed remotely. In order to fraudulently attack a voting system computer the perpetrator must not only be a competent computer hacker but must also be able and willing to commit the crime of breaking and entering in order to gain access to the computer.

This is not to say that hacker attacks are not a matter of concern. NIST and the TGDC are including protections against hacker attacks in the voting system guidelines under development. However, historical evidence indicates that there are other security concerns about voting systems that should have at least as high, if not higher, priority.

As an example, let's look at some anomalies associated with recent elections.

In 2004 in Greensboro, Alabama Johnny Washington defeated Vanessa Hill for mayor by a vote of 762 to 672, a margin of 90 votes. But 211 of Washington's votes were absentee ballots compared to 52 for Hill. Hill challenged and a Montgomery circuit judge ruled that at least 148 of the absentee ballots for Washington were illegal, including ballots with forged signatures, no postmarks, and from abandoned addresses. The state supreme court unanimously upheld the decision.

In Cleveland, Ohio two Cuyahoga County election workers were convicted of illegally rigging the 2004 presidential recount. Ohio law requires that during a recount each county must randomly count at least 3 percent of its ballots by hand *and* by machine. If there are no discrepancies in those counts, the rest of the votes can be recounted by machine. A full hand-count is mandated if two random samples result in differences. Three days before the recount these two workers got behind closed doors and picked ballots that they felt would not cause discrepancies during the recount. The intent was not to try to influence the outcome of the election, Kerry gained 17 votes and Bush lost 6 in the recount, but rather to try to avoid the lengthy manual recount.

In a recent election in Sarasota, Florida18,000 voters did not register a vote in the 13th Congressional District race. There is continuing disagreement

over the precise cause, but one prevailing theory is that this under-vote was a result of the design of the ballot. Ted Selker, an associate professor at MIT and co-director of the CalTech/MIT Voting Technology Project, reported "If they just did a really, really simple thing – one race, one page – that would make a huge difference. By putting a big one and a little one (on the same page), you don't see the little one."

A review of the various anomalies reported in recent elections leads to the conclusion that threats to voting systems rarely, if ever, come from hacker's attacks against the voting system computers, but rather from the mostly accidental, but occasionally deliberate, actions of candidates and their supporters, election officials, poll workers, and voters.

So, I am going to leave the discussion of security against hackers to the other panelists and direct my remarks toward other potential security breaches.

Voting System Security in Georgia

It is well known that in November 2002 the State of Georgia implemented state-wide a DRE voting system. What may not be known is that since November of 2002 we have conducted over 3,000 elections using this system without experiencing a single incident that can be attributed to the voting system. That is not to say that we have not had problems, but that the problems that we have experienced can all be directly attributed to human factors.

This success is not a result of good luck or serendipity. This success is the results of policies and procedures that are well defined and widely articulated and an extensive training program to ensure that everyone involved in the conduct of an election knows what they are supposed to do and how to do it.

The State has defined a 64 hour training course for election officials. Election officials that complete this 64 hour program are designated a 'Certified Election Official'. State law requires that every election office in the State must have at least one employee that is a Certified Election Official.

The State does not train poll workers directly, but it does provide training classes for those county election officials that do train the poll workers. In

addition, the State offers training classes for persons that are peripherally associated with elections, such as members of local election boards and members of county commissions.

There are employees in the Office of the Secretary of State whose primary job is voter outreach. These employees travel the State presenting the voting system to civic clubs, church groups, schools, etc.

The State Election Board has published procedures for the secure storage of election management computers in county election offices and the secure storage of voting stations in county warehouses. Investigators from the Secretary of State's office conduct random inspections to verify that these procedures are being followed.

Quality control procedures are in place to ensue that ballot formats used state-wide are uniform and user friendly. The Center for Election Systems at Kennesaw State University prepares the ballots for 114 of the 159 counties in the State. Five counties prepare their own ballots and the rest contract with an outside organization to prepare their ballots. Regardless of who prepares the ballots, the final ballot formats are submitted to the KSU Center for final quality review. This review assures the uniformity of ballots state-wide.

Similarly, every component of the voting system must undergo acceptance testing by the KSU Center before it can be used in an election. This requirement not only applies to newly purchased components, but also to any component that has left the custody of the State and returned. For example, equipment that has been sent out for repair and returned.

Visitors to the State of Georgia often contend that they cannot implement the type of training program that Georgia has implemented because they have multiple voting systems whereas Georgia has only one. This is not a valid reason because the vast majority of functions necessary to conduct an election is common between jurisdictions and, for the most part, is independent of the particular voting system employed.

This is particularly true of the activities in a polling place. In the polling place there are two generic voting systems: optical scan and DRE. Once these polling place devices are programmed for an election the differences between vendor devices are minimal.

The same is true, though for a lesser extent, for election management issues. For example, good ballot formatting practice is independent of the type of voting system utilized.

States can develop training programs that concentrate on these commonalities with, perhaps, side courses that address the differences between specific systems.

In the remainder of this paper I examine the issues before the Committee and offer recommendations for their resolution.

Training

At a previous congressional hearing I was asked what I though was the most important thing a jurisdiction could do to secure the voting system. My answer was 'Train the poll workers'. A well trained poll worker can overcome almost any problem that arises in a precinct, but a poorly trained poll worker will likely exacerbate the problem.

There is available extensive documentation and training materials related to the various aspects of defining and conducting an election. There is an old saying that it is necessary to "Get the milk down to where the cats can get at it". There is a need for a training program that will 'get the information we have available down to where the people that need it can get at it.' We need to facilitate training programs for election officials, poll workers, and voters.

It is recommended that the EAC be given the responsibility and the funds to assist the states in setting up training facilities that can offer training in all aspects of election administration: defining and setting up elections, formatting ballots, managing polling places, etc. This can be accomplished through cooperative efforts between state election offices and local universities, trade schools, or commercial organizations.

Voter Verifiable Paper Audit Trails

There are two universally accepted reasons for the requirement of a VVPAT. One is that the VVPAT can be used as an audit against the electronic results. The second is that it gives the voter assurance that her ballot has been correctly recorded and counted.

According to the latest information on Electionline.org, 22 states require voting machines to produce a VVPAT. Many other states have such legislation pending and the congress is considering legislation that would make a VVPAT mandatory in all federal elections.

Some of these states and the pending federal legislation require that under certain conditions these VVPATs become the ballot of record. This requirement can possibly lead to serious unintended consequences.

There is substantial evidence that the VVPATs produced by the currently available DRE voting stations do not possess the reliability and accuracy required for a ballot. The printers used in the current VVPAT modules are not high quality, reliable printers. In every election where VVPATs have been produced by the current DRE voting stations a number of the VVPATs have been unreadable due to various printer failures.

The percentage of unreadable VVPATs has run as high as 10 % (Cleveland, Ohio and North Carolina) of the total votes cast. The voters who's VVPATs are unreadable will be disenfranchised if the VVPAT is used as the ballot of record.

This is not unusual considering that all of the currently available voting systems that produce a VVPAT were certified under the FEC 2002 Voluntary Voting System Standards (2002 Standards). The 2002 Standard contains no standards for a VVPAT.

When the State of Nevada adopted a requirement for a VVPAT their vendor complied with this requirement by quickly developing a VVPAT module that attached to their existing DRE voting station. This module employs a thermal printer and prints the VVPATs sequentially on a roll of paper. The other voting system vendors quickly followed suit and developed similar modules for their DRE voting stations.

Since the 2002 Standards do not contain standards for VVPATs there were very limited certification tests that could be performed on these VVPAT modules. The primary test that was performed was to verify that the VVPAT module did not interfere with the otherwise required features of the voting system.

The EAC 2005 Voluntary Voting System Guidelines contain minimal standards for VVPATs but these Guidelines are not required until December 2007. In the meantime, voting systems can continue to be certified under the 2002 Standards and, at present, no voting system has been submitted for certification under the 2005 Guidelines. It may well be that the vendors are waiting to see what will be contained in the 2007 Guidelines.

The Technical Guidelines Development Committee and NIST are developing what is being called the 2007 Guidelines. These guidelines, that are expected to contain standards that will produce VVPATs that have the reliability and accuracy necessary to be used as a ballot, are scheduled to be presented to the EAC in draft form in July 2007. Assuming that they will require the same time line as the 2005 Guidelines for public comment, revision, and final approval it is likely that these 2007 Guidelines will not be required until December 2008, a month after the 2008 elections.

Historically, the time between the implementation of a Guideline and the time the vendors can produce a voting system that is certified under those Guidelines is about 2 years. Unless something out of the ordinary happens, we will go through the 2010, and probably the 2012, elections with the currently available voting systems.

Hand Counted Paper Ballots

When lever voting machines were introduced in the 1930's and 1940's they were hailed as a great innovation in elections for the simple reason that they eliminated the need to hand count paper ballots. Yet, in 2007 we are considering situations in which a paper ballot will again become the official ballot of record.

There is no historical or legal precedent for an election to have two official ballots. Several state laws and at least one proposed federal law specify that the electronic ballots are the ballots of record until a particular event occurs, but thereafter a paper ballot will become the ballot of record. Legislation must be carefully drafted to insure that the courts cannot rule that there can only be one ballot of record and that that ballot of record is the paper ballot.

This decision would return elections to the slow, inaccurate ballot counts that were characteristic of the 1930's.

Open Source Code

Every agency in government and every major business entity have software that is considered mission critical. I am not aware of a single organization that makes their mission critical software available to the general public. The reason is simply that open source software is vulnerable to attack from everyone from teen age hackers to foreign terrorists.

Voting system source code is mission critical to successful elections. Placing this source code in the hands of hackers and terrorists clearly creates the potential for harm to the integrity of elections. On the other hand, there are advantages to be gained from making this source code available to responsible reviewers.

It is recommended that the EAC be granted the authority to make voting system source code available to responsible individuals. Persons wishing to review voting system source code be should be required to make application to the EAC; providing their credentials for reviewing the software, their 'need to know', and the specific voting system software they wish to review. A recipient of voting system software should be required to sign a nondisclosure agreement and to return or destroy the software when their review is completed. Source code should only be provided to individuals, not organizations.

Election Management System

A voting system can be viewed as two independent systems. One, called the election management system, is the system that defines the election, formats the ballots, programs the voting stations, tallies the votes, prints the reports, and maintains the various audit trails. The other system is the ballot stations that are used to collect the ballots.

Investigations and studies of voting system security has concentrated on voting stations and shown little interest in the election management system. Yet, many problems that occur during an election originate in the election management system. For example, if the 18,000 under-votes in Sarasota, Florida were indeed the result of poor ballot design, then this problem originated in the election management system.

NIST and the TGDC should be encouraged to expand the Guidelines to include the election management system.

In closing, I would like to state that the opinions presented in this paper are entirely my own. They do not represent the opinions of Kennesaw State University or the Office of the Georgia Secretary of State.

Again, I wish to thank the Committee for the opportunity to address these important issues. I sincerely hope that I have made at least a small contribution to the work of this committee.

Respectfully submitted:

Britain J. Williams, Ph.D.
Professor Emeritus of Computer Science and Information Systems
Kennesaw State University

Brit Williams is Professor Emeritus of Computer Science and Information Systems at Kennesaw State University. One of his primary research interests since 1986 has been computer-based voting systems. He was a consultant to the FEC during the development of the 1990 Voting System Standards and the 2002 Voting System Standards. He was a member of the NASED Voting Systems Board and Chair of the NASED Voting Systems Board Technical Committee from their inception until 2007. He represents NASED on the Technical Guidelines Development Committee created by the Help America Vote Act. Dr. Williams has been conducting certification evaluations of computer-based voting systems for the State of Georgia since 1986. He also has assisted the states of Pennsylvania, Maryland and Virginia with certification evaluations of computer-based voting systems.