Presentation to
U.S. Election Assistance Commission
May 5, 2004

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

1. Introduction

After the November 2000 general election a small group of political activists captured the attention of the media with the conjecture that direct recording electronic (DRE) voting machines are inherently not secure. Furthermore, they contend that the only way that these systems can be made secure is by the addition of a Voter Verifiable Paper Ballot (VVPB). These activists' conjectures gained respectability when they were joined by several computer scientists from major universities. These academics claim that computer systems in general and voting systems in particular cannot be made secure.

A DRE voting system is a comparatively simple computer application. The main line of the system is to respond to a touch at a specific location on a touch-sensitive screen and add one to the appropriate register. There is no requirement for intricate or complex computations. There is no requirement to compute any logarithmic functions, trigonometric functions, or even take the square root of anything.

The conjecture that using current technology we are unable to make such a simple system secure and accurate is contradicted by the facts of our everyday existence. We build secure and accurate computer systems that fly our airliners. We build secure and accurate computer systems that guide our submarines under the ice cap. We build secure and accurate computer systems that guide our astronauts to the moon and bring them safely back to earth. We submit to open heart surgery while a computer monitors our vital signs and controls an artificial heart and lung machine. The list of secure and accurate computer systems that monitor, control, and improve our lives is large and growing daily.

This is not to imply that our current DRE voting systems do not need to be improved. They do. But there are many aspects to a voting system other than accuracy and security. These include availability, reliability, maintainability, usability, and even affordability. Any change to a voting system must be evaluated on the basis of its impact upon the entire system. To this end Congress has created the Election Administration Commission (EAC). This Commission has the resources and authority required to effect an orderly and disciplined evaluation of the state of the existing voting system technology and implement improvements to voting systems in an orderly manner.

In this paper and in my presentation to the EAC First Public Hearing on the Use, Reliability, and Security of Electronic Voting Systems I will present to the Commission evidence that a rapid, poorly formulated forced addition of a paper ballot or receipt to the existing DRE voting systems is unnecessary and could have adverse consequences that far off set any perceived advantages. I will argue that this action is unnecessary because we are in no imminent danger and have sufficient time to allow the organizations and processes defined in the Help America Vote Act to perform their assigned duties and responsibilities. I anticipate that many presenters to the hearing will make these same points so I will use the majority of my assigned seven minute presentation to describe several recommendations that will improve the security of all existing computer-based voting systems, optical scan as well as DRE. These recommendations are such that they can be easily implemented and will be consistent with the mission of the EAC.

2. Voter Verifiable Paper Ballots

When we vote to elect the members of the board of directors of a company, to elect the officers of a social or civic club, or to elect the officers of a labor union we cast a 'ballot' (sometimes called a proxy). This ballot contains unique identifies such as our signature, social security number, or member number that can be used by the election monitors to validate the ballots. Given the ease with which the individual ballots can be validated it is unusual for the persons conducting the election to expend the effort and expense necessary to purchase and implement a commercial, NASED Qualified voting system. They typically gather the votes and use their in-house computer technicians to develop a system to tally the votes. Any anomaly or challenge can be resolved by resorting to the verified ballots.

When we vote in a municipal, state, or federal election we do not cast a ballot in the sense described above. We cast a 'secret' ballot. This ballot, by law, can contain no unique identifier that will enable anyone, including the voter, to identify the person that cast the ballot. Thus, in a municipal, state, or federal election there cannot exist a 'Voter Verifiable Ballot', paper or otherwise

What can be added to a DRE voting system is the capability to produce a paper 'receipt'. There are at least three DRE voting systems that have either completed NASED Qualification or are in the process of obtaining NASED Qualification that have the ability to produce a paper receipt. These systems demonstrate the problems that can result from attempts to implement modifications to a voting system in the absence of defined, well thought out standards.

The EAC Voting System Standards (formerly known as the FEC Voting System Standards) do not contain a specification for a paper receipt produced by a DRE voting machine. The voting systems that produce paper receipts are being NASED Qualified under a provision of the Standards that allows optional features. In particular, the Standards require that a voting system comply with its own documentation. If the voting system documentation defines an optional feature (i.e. a printed receipt) then the Independent Test Agency (ITA) verifies that this feature is implemented in the system exactly as defined in the documentation.

As a result, the paper receipts produced by the currently Qualified DRE voting systems do not comply with the EAC Standards requirements for a ballot. For example, these systems cannot comply with the Standards requirement for high contrast or increased print size to accommodate a person with impaired vision. Also, they cannot comply with the Standards requirement to produce ballots in multiple languages.

Furthermore, all of the paper receipt DRE voting systems implement what appears to have become a de facto standard: that the receipt appear under glass so that the voter cannot touch or handle the receipt. It is not clear how this de facto standard became practice or even whether or not it is appropriate. For the entire history of elections in America voters have handled their own ballots (receipts) and deposited them in a ballot box. Further investigation may determine that a ‘receipt under glass’ should not be nationally dictated but rather should be an optional feature that the local jurisdiction can decide whether or not to implement.

The concept of a ‘recount’ of an election originated with paper-based voting systems. It is well known that a manual count of paper ballots almost always contains errors. As a result close elections were recounted, if necessary several times, until the outcome of the election was determined to the satisfaction of all parties. On rare instances, the recounts were indeterminate and the outcome was decided by chance, the toss of a coin. Since punch-card and optical scan voting systems were also subject to counting errors, the practice of a recount was continued on these voting systems.

For a DRE voting system the concept of a recount in the classical sense does not apply. If a DRE voting system can be demonstrated to be valid (i.e. correctly set up and functioning properly) then the results are 100% accurate. Thus, for a close election, confidence in the results is obtained by validating that the system is operating correctly. Although the name ‘recount’ is stilled used for this validation process there is no actual recount of anything. Instead, tests are run to demonstrate that the ballots are correctly defined, that the precinct setups are correct, that the vote images were correctly transferred to the central site, and the computer that computed the tally is functioning correctly. It then follows that the election results are 100% accurate.

3. We Are Not in Imminent Danger

Computers have been used to tally elections in America since October, 1964 when DeKalb County and Fulton County, Georgia were the first jurisdictions in America to employ a punch-card voting system. Since then the State has used every type of computer-based voting system: punch-card, central count optical scan, precinct based optical scan, and direct recording electronic voting systems. During these forty years there have been many attempts to defraud a Georgia election, but not a single one of these attempts has involved an attack on the computer system. This is probably due, at least in part, to the fact that many people believe that they know how to successfully alter a piece of paper, but very few people believe that they have the ability required to successfully alter a computer system.

The Georgia DRE voting system is both accurate and secure. Measures are in place to insure that the voting system computers are as accurate and secure as current computer technology permits. In addition, physical security and procedural security measures are in place to compensate for the remaining vulnerabilities that have been identified in the computer system. An extensive, State-wide training program has been implemented to prepare our election officials and poll workers to recognize and react to any problems that may occur during the course of an election.

4. Computer System Security in the Georgia Voting System

Georgia has been a full participant in the EAC Voting Systems Standards project since its inception. Before a voting system can be considered for use in Georgia, it must be examined by the ITAs for compliance with the EAC Voting System Standards. Georgia considers a voting system to consist of a *specific* version of each of the system components: hardware, voting system software, and operating system software. Any change to any component, no matter how insignificant, is considered a different system and requires re-examination, both NASED Qualification and State Certification, of the entire system.

When the system successfully completes ITA qualification testing and is issued a NASED qualification number, it can be brought into Georgia for State Certification Testing. The system to be tested is not obtained from the vendor but is transmitted to the KSU Center for Election Systems directly from the ITAs.

The KSU Center for Election Systems conducts a series of tests on the system. Some tests examine the level of difficulty associated with operating the system. Another tests the capacity of the system to accommodate the maximum number of ballots that might be cast in a large precinct or at an in-person absentee voting location. One test is specifically designed by the KSU Center for Information Security, Education, and Awareness to detect fraudulent or malicious code that might be present in the system. This test is designed to wake up any, so called, Trojan horse that might be present. In all of these tests a known pattern of votes is cast and the compared with the output of the system.

If any of these tests result in a modification to the system, the *entire* system is returned to the vendor for correction and the NASED Qualification/ State Certification test cycle is repeated.

When the system successfully passes State Certification and is certified for use in Georgia, the KSU Center for Election Systems prepares an electronic signature of the system and archives the software source code and object code. The vendor is then authorized to install the system in the 159 county election offices. The primary reason for allowing the vendor to perform the installation is to protect the warranty on the system. If State employees performed the installation there is the chance that they might inadvertently perform some act that would void the warranty on the system.

When the vendor notifies the State that they have completed installation in a particular county, the KSU Center for Election Systems sends a team to the county to conduct Acceptance Tests. These tests verify that the hardware is operating correctly and that the correct version of the software has been installed. During these tests the electronic signature of the software installed in the county is compared with the electronic signature of the software archived by the KSU Center for Election Systems to validate that the county system is identical to the system that was State certified.

The foregoing paragraphs describe three distinct activities that are performed in order to insure the security and integrity of the Georgia voting system.

Activity 1: Verify that the voting system, as delivered from the ITAs, is free from extraneous or fraudulent code.

- Setup and conduct sample elections with known outcomes that are representative of Georgia general and primary election.
- Conduct high-volume tests to determine capacity limits of the system.
- Conduct tests to determine the systems ability to recover from various types of errors.
- Conduct tests to detect extraneous or fraudulent code.

Activity 2: Verify that the system as installed by the vendor in the local jurisdictions is *identical* to the system received from the ITAs and certified by the KSU Center for Election Systems.

- Prepare a validation program that will detect any changes to the system installed in the local jurisdictions.
- Run the validation program against the system installed in the local jurisdiction (after vendor installation).
- Provide the local jurisdiction with the ability to run the validation program.

Activity 3: Verify at specific and random times that the system has not been modified in any way.

- Run the validation program immediately before beginning to define an election.
- Run the validation program immediately upon the completion of an election.
- Run the validation program after any suspicious event.
- Run the validation program at random times.

The electronic signature that is used to validate the correctness of installed systems is based on NIST certified SHA-1 contained in FIPS 180-2, August 2002 and includes the following:

- 32 bit CRC
- 128 bit MD 5 Hash
- 160 bit SHA-1 Hash

It is estimated that the chance of modifying the software in such a manner that this hash would not detect the modification is over 1,000,000,000 to 1.

5. Procedural Security in the Georgia Voting System

Rigid policies and procedures are in place that control who can access to the election system, when they can access the system, what components they can access, and what function they are allowed to perform. The most familiar of these procedures is the process that a voter must go through in order to cast a vote on the system. Other procedures define the activities of election officials and poll workers.

Many of these procedures are directed toward insuring that the correct versions of the system software is initially installed in the GEMS computers and voting stations and, subsequently, testing at various times to insure that this software has not been altered. We have already discussed this process.

Accuracy and uniformity of the ballots is critical to the success of an election. If a county so desires, the KSU Center will prepare the county ballot. Before the 2004 Presidential Primary Election the KSU Center prepared the ballots for 102 of the State’s 159 counties. To achieve ballot accuracy and uniformity, the KSU Center for Election Systems reviews the ballot formats from all counties prior to each election.

Other security features are designed to prevent or detect attempted terrorism or election fraud during the course of an election. These are included in the next section.

6. Physical Security in the Georgia Voting System

The first line of security defense in any system is physical security. All other security measures go for naught if you leave the doors unlocked. The following is an overview of the physical security implemented in the Georgia voting system.

- The GEMS computers are kept in locked offices within the county election offices.

- The GEMS computers are not connected to any communication system, including the Internet, and contain no software other than the Windows operating system and the Global Election Management System object code.

- A security program, similar to a virus detector program, is run against the GEMS object code and the static portions of the operating system related to the GEMS system prior to beginning the definition of an election to verify that the code has not been altered. This program is repeated after the close of the election to verify that the code did not change during the election.

- No person is allowed access to the GEMS computer until his or her identity has been clearly established by the county Election Superintendent.

- The voting stations are stored in their voting booth cases in locked county warehouse facilities.

- At the precincts the PC memory cards in the touch screen voting stations are in a locked compartment on the voting stations. The Precinct Manager is the only person in a precinct with a key to this compartment.

- After the polls close a printed report of the precinct results is posted on the precinct door. This places the results from the precinct in the public domain and any subsequent alteration of these results is easily detected.

- The PC memory cards from a precinct are transported from the precinct to the county elections office by a sworn election official or a sworn law enforcement officer. Precinct managers may, at their option, send the precinct results to the county office via modem. However, these modem results are unofficial and are for the benefit of the press and the candidates.

- The area of the precinct that contains the voting stations is secure. A voter is not allowed to enter this area until a voting station is available for his or her use. However, there are no enclosed voting booths and the secure area is in plain view of the poll workers, candidate representatives, party poll watchers, advocacy poll watchers, and media representatives.

7. Training and Ballot Building for Georgia Elections

One benefit of using a uniform technology throughout the State is that many ballot building procedures can be centralized. This enables better error detection and correction as well as efficiency in the production of redundant ballot content (federal and statewide races and issues). Ballots can be reviewed for compliance with State law as well as proper district and precinct information. In the most recent statewide election the KSU Center for Election Systems prepared the ballots for 102 of the States' 159 counties. The KSU Center reviews all ballots, regardless of who prepared them, for accuracy and completeness. Following this review the ballots are returned to the counties for final review and acceptance.

The training issues in election technologies are unique. The process is heavily dependent upon personnel that are both volunteer and infrequent users of the system. The processes are a combination of manual and computerized operations that are the result of state and federal election law, state election rules, election tradition, and functional requirements of the election technologies. The processes are dynamic and change in varying degrees from election to election, requiring a constant vigilance of training objectives, materials, and curriculum. The KSU Center is responsible for working with the vendor and state and county officials in the development and maintenance of training programs.

In 2003 the State of Georgia enacted legislation that requires all election superintendents to successfully complete 64 hours of training. This training program is prepared and administered by the KSU Center and includes election law, ethics, and election procedures, including those unique to the current DRE technology use in Georgia. This training helps to insure that appropriate security procedures are understood and implemented at the county and precinct level.

8. Recommendations

This section contains three recommendations to improve the overall security of all electronic voting system, including optical scan and DRE.

Secure Voting System Software Library

NIST currently maintains a Secure Software Library for law enforcement software. A HASH signature similar to the HASH used in Georgia to validate election software is made available to any law enforcement agency that wishes to validate a law enforcement software system.

It is recommended that this Secure Library can be extended to include NASED Qualified voting system software. When a voting system completes NASED Qualification the ITA could submit a copy of the qualified software directly to NIST for inclusion in the Secure Library.

Previously qualified voting systems could be included in the Secure Library at the request of a using jurisdiction. The jurisdiction would be responsible for uniquely identifying to NIST the software to be included. This identification could be either by NASED Qualification number or by vendor version and revision number. The requested software would be obtained directly from the ITA by NIST and included in the Secure Library.

This Secure Library could be used by local jurisdiction to validate that the voting system software they are using is, in fact, the software that the ITA qualified and has not been altered. It could also be used to resolve challenges where the claim is that the software in a jurisdiction has been altered.

Formal, Vendor Specific Training Programs

The importance of well trained election superintendents and poll workers cannot be overstated. An examination of election anomalies will disclose that almost all could have been avoided or at least minimized by well trained poll workers. Most reports of anomalies in the setup of an election such as candidates not appearing on the ballot are the result of poorly trained election superintendents.

The KSU Center for Election Systems has developed a 64 hour sequence of courses that lead to recognition as a Certified Election Superintendent for the State of Georgia. Not every state or jurisdiction has the resources of such a Center at their disposal. However, every state has area vocational institutions and university centers for continuing education.

The EAC could offer grants to these organizations for the development of certification programs similar to the Georgia certification program. A requirement for these grants would be that the program must not be general in nature but must address the specific voting systems in use in the local jurisdictions.

System Specific User Manuals and Training Materials

The vendors provide manuals describing the operation of their specific systems. These manuals contain descriptions and instructions for all of the various options available in the system. As a result, the vendor manuals are usually unacceptable for use as a training manual without extensive editing to remove the portions that do not apply to the local jurisdiction and, in many cases, simplify the language and presentation of the manuals.

EAC Office of Election Administration has prepares documents addressing the various aspects of election management. These documents are general in nature and usually do not contain information that is specific to any given jurisdiction.

These two types of documents need to be combined into a series of documents suitable for use by local organizations to train election officials and poll workers and by the organizations described in the above recommendation to develop their programs. These documents need to be modular to allow a local jurisdiction to customize manuals for use by ballot builders, poll worker trainers, poll workers, etc.

KSU Center for Election Systems Support for these Recommendations

The KSU Center for Election Systems has experience in each of the areas recommended above. We are knowledgeable of the techniques involved in using the Secure Library to validate voting system software. We have developed a curriculum and materials for a 64 hour course for election superintendents. Our staff has experience working with vendors and election officials in all phases of elections including: voting system certification, secure warehousing of voting equipment, ballot preparation, precinct setup and procedures, election superintendent and poll worker training, manual and documentation development, problem resolution, and election validation.

We are pleased to offer our knowledge, experience, and facilities to agents of the EAC in the implementation of the any of the above recommendations.

About the Author: Brit Williams is a Professor Emeritus of Computer Science and Information Systems at Kennesaw State University. He was a consultant to the FEC during the development of the FEC Voting System Standards in 1990 and again in 2002. He is currently a member of the NASED Voting Systems Board and Chair of the NASED Voting Systems Board Technical Committee. He has been conducting certification evaluations of computer-based voting systems for the State of Georgia since 1986. He also assists the states of Pennsylvania, Maryland and Virginia with certification evaluations of computer-based voting systems.