Developing an Analysis of Threats to Voting Systems
A Response by the Florida State Association of Supervisors of Elections

Introduction

The 2000 General Election has served as the catalyst for election reform throughout the United States. State and local governments have purchased and implemented a number of different types of voting systems, many choosing either precinct count optical scan or direct record electronic (DRE) touch screen voting systems. The implementation of these systems has caused state and local governments to reassess the threats to the security of these voting systems.

Security of voting systems has always been a concern of local elections officials but has taken on additional importance by the general public and the computer technology communities as these systems have been used in more elections throughout our country. It is important to note that security, as a technical term, means something is not only secure but that it has been secured.

Since more jurisdictions have begun to use new voting systems, there has been a huge effort to require these systems to provide a paper receipt, commonly referred to as a voter verifiable paper audit trail (VVPAT.) This plea has been primarily associated with the touch screen voting systems.

Florida elections officials have worked tirelessly to ensure that voting systems are accurate, reliable and secure. Florida officials believe the voting equipment, "the box," to be only part of the voting system. We firmly believe that people, policies and procedures are critical to the efficient operation of these systems. The "Three P's," as we refer to them, are often overlooked as being an integral part of the system. Because of this oversight, these systems have taken a great deal of the blame for "failure" when the truth is the "failure" was a result of inadequate policies and procedures and human error, not voting systems. These three elements are critical to the successful administration of elections and should be included in the discussion of threats to voting systems.

Thoughts on Assessing and Minimizing Threats to Voting Systems

The Election Reform Act of 2001, passed by the Florida Legislature and signed into law by Governor Jeb Bush, required all counties to use either a precinct count optical scan system or a touch screen voting system. Fifty-two counties are currently using an optical scan voting system. These counties, as required by the Help America Vote Act (HAVA), will be implementing either a touch screen voting system in each polling place or the AUTOMARK product, pending State certification, to accommodate voters with disabilities. There are 15 Florida counties that have chosen to implement touch screen systems throughout their counties. These counties, accounting for over half of all voters in Florida, are currently in compliance with the requirements of HAVA to accommodate voters with disabilities. This point is made to illustrate the fact that although a jurisdiction

uses an optical scan system, many will be faced with implementing touch screen technology into their overall voting methodology.

Optical scan systems are "perceived" to be more secure and less of a security risk than touch screen systems because of the use of an actual paper ballot. But bear in mind, even optical scan systems use software for tabulation, and in most recount laws those ballots will not be manually recounted. Florida officials believe that all systems security should be analyzed using the same standards. However, one cannot intelligently compare or analyze voting systems without carefully examining how the technology is being implemented. Even with a VVPAT, testing, training and adhering to procedures is essential.

Florida elections officials believe that the discussion of the "Three P's" is even more important when discussing touch screen voting systems because of the perceived threats to their accuracy, reliability and security.

Local elections officials need to ensure that policies and procedures are in place that detail <u>all</u> steps and activities necessary to conduct an election. These policies and procedures need to go beyond being a document to meet some state requirement mandating elections officials to have "security procedures." These security procedures need to detail security of optical scan ballots used for absentee voting, the programming of the election parameters, the proofing and correction, if necessary, of ballot tabulation and collection parameters, the chain of custody of all election records and documents required to make the system election ready, among many others.

A copy of Florida Administrative Code, 1S-2.015, Minimum Security Procedures for Voting Systems, is attached as an example of steps taken to address security within the total process of elections administration.

The manufacturers of these systems are held to a much higher standard today than when these systems were first introduced into the market. This is a good thing. Local elections officials, generally through users' groups, have worked with the manufacturers to improve these systems. Additionally, we have worked with our State Division of Elections to address issues and improvements to these systems that the manufacturers have incorporated into their systems designs.

As previously stated, much more attention needs to be devoted to the training of local elections officials and their staffs. Local officials need to become "vendor independent," where possible. Local officials need to assume the responsibility of implementing, operating and maintaining these systems. You would no more want an untrained, untested elections official, and/or their staff, conducting your elections, regardless of the system being used, any more than you would want to fly with an untrained and untested pilot. Although this illustration may appear to be inappropriate, it demonstrates the importance of the need for training in a very specialized field and in a very politically volatile environment.

The need for competent and qualified people does not start or stop with the local elections official. The Florida Legislature has adopted more stringent standards for the recruitment and training of poll workers in an effort to minimize human error. The trend is that Florida is "professionalizing" their election day workforce.

Florida elections officials recommend that voting systems be designed to be independent systems, eliminating any networking of systems. Additionally, voting systems should not be configured in such a manner as to access the internet. This action would eliminate unauthorized access to the system from the outside.

Finally, as threats to voting systems are examined and addressed, this issue does not need to be confused with issues outside the realm of voting systems. It is a fact that these systems run on off the shelf computers with commercial operating systems. People all around the world use these computers and operating systems to transact business every day without incident. It is not logical to expect or require these operating systems to be included as part of a "voting system," making them subject to the voting systems standards. This argument only perpetuates the belief that these voting systems are incredibly complex and are unable to have malicious code detected.

Conclusion

Election reform and all its associated issues will and should continue to be "hot topics" for many years to come. Security of voting systems and the overall elections process needs to be continually reassessed and tested to ensure that our elections process is reliable, accurate and secure. Technology continues to change the manner and method of casting and counting votes. For this reason, local elections officials need to change the manner and method by which their entire system, "the box," people, policies and procedures, fit together to provide a seamless system that is not subject to outside or inside influences without detection.

There is a need to assess "real world" threats. It is important to note that just because something is possible it is not the same as saying it is probable. There has been no evidence of insertion of malicious code, attacks on individual machines at precincts or tampering with election results. Parallel testing in California and other jurisdictions has revealed that touch screen voting systems tested recorded votes with 100 percent accuracy.

As threats to voting systems are examined, it is also important to realize that voting systems technology has changed dramatically thereby minimizing, if not eliminating, many of the concerns that existed when these systems were first introduced. Many states have adopted precinct count optical scan system over central count to provide the voter the opportunity to correct deficiencies on their ballot prior to it being cast. This requirement, although seemingly minor, has eliminated many voters' choices from going uncounted. Additionally, touch screen systems have evolved into a much more sophisticated, secure and reliable system. Unlike the first generation full face DRE's, the second generation provides many more safeguards to prohibit errors from occurring or

prompting the voter of an action that needs to be taken. The differences in these types of voting technology is important, especially as noted in the results of the new CalTech/MIT Voting Technology Project and Florida's Analysis and Report of Overvotes and Undervotes for the 2004 Election. Studies have shown a reduction in residuals and the elimination of the racial gap with DRE's.

The different, and sometimes competing, communities need to work together to ensure the security of these systems. The current perception of voting systems being unreliable, unsecure and inaccurate will never change as long as misinformation continues to be offered as fact.

Florida elections officials recommend, at a minimum the following:
- more emphasis on training local elections officials and/or their staffs
- a more comprehensive set of standards for election security procedures that extends beyond the actual voting system
- that voting systems not be a "networked" system
- that voting systems not be dependent upon the internet and prohibit voting systems from accessing the internet.

On a local level, elections officials should be held accountable for providing the safeguards necessary to ensure their electorate that their voting systems are secure. On the national front, organizations such as the National Institute of Standards and Technology (NIST) should not only look at threats coming from the actual voting unit or system but through the people managing these systems and whether policies and procedures are in place to minimize the threat of abuse.