Testimony Submitted by Paul Miller

Introduction

Good afternoon. Thank you very much for inviting me and extending this opportunity to testify regarding the development of standards for voting systems that can the meet federal mandates for UOCAVA voting.

My background includes eleven years working at King County Elections as its Assistant Superintendent - Data Processing where my duties included setting up and deploying voting systems in one of the largest counties in the country. For the past ten years, I have been employed by the Washington Secretary of State in a variety of roles including the testing and certification of voting systems for Washington State.

For the past nine months I have participated in a small federal task force committed to the development of standards for systems that can be deployed in remote locations. Essentially we are discussing an approach that sets up an early voting polling site overseas or at military installations where voters from any participating election jurisdictions across the country can vote.

As with any voting system, the task force approached the task with the goal of writing guidelines for a system that are testable. The responsibility for correctly implementing the standards in a product belongs to the vendor while the responsibility for ensuring a system meets those standards is the responsibility of the Voting Systems Testing Laboratories and the EAC.

The standards try to ensure that a voting system meets baseline requirements so that the system can be used in a safe manner. However, the process of ensuring the confidentiality, integrity, and availability of a system extends beyond the qualification of a system.

I am here today to provide an overview of how the system is intended to function. A more detailed description can be found in the draft security plan which I believe is included in materials provided to you.

Background

As a first step toward meeting the congressional mandate that the EAC develop guidelines for remote UOCAVA voters, our task force drafted pilot test requirements to certify remote electronic systems that support multiple voting jurisdictions.

In order to implement this project, vendors with experience in delivering online voting services will submit systems that support this model to the EAC and to a Voting Systems Testing Laboratory (VSTL) for review and testing. The successful review of a system will lead to EAC issuing a pilot certification for the system.

The EAC envisions the TGDC, using the pilot test requirements and evaluations of the pilot project implementations, will be able to develop a comprehensive set of requirements for a system that can be scaled to securely handle the needs of UOCAVA voters in the manner mandated by Congress.

Project Scope

The Pilot Project is a small-scale, limited-scope feasibility study. It is small-scale in that only a few states are anticipated to participate. It is anticipated that the number of voters participating will be large enough to provide a statistically meaningful test of the concept, but small enough so as not to affect the outcome of any electoral race.

Ballots cast using the System will count.

The participants have decided at the outset of this Project that the model will mimic 'early voting' poll sites as much as possible. Those developing the requirements for this project have a great deal of experience in and understanding of the security dimensions involved in this method of voting which is already used ubiquitously throughout the country.

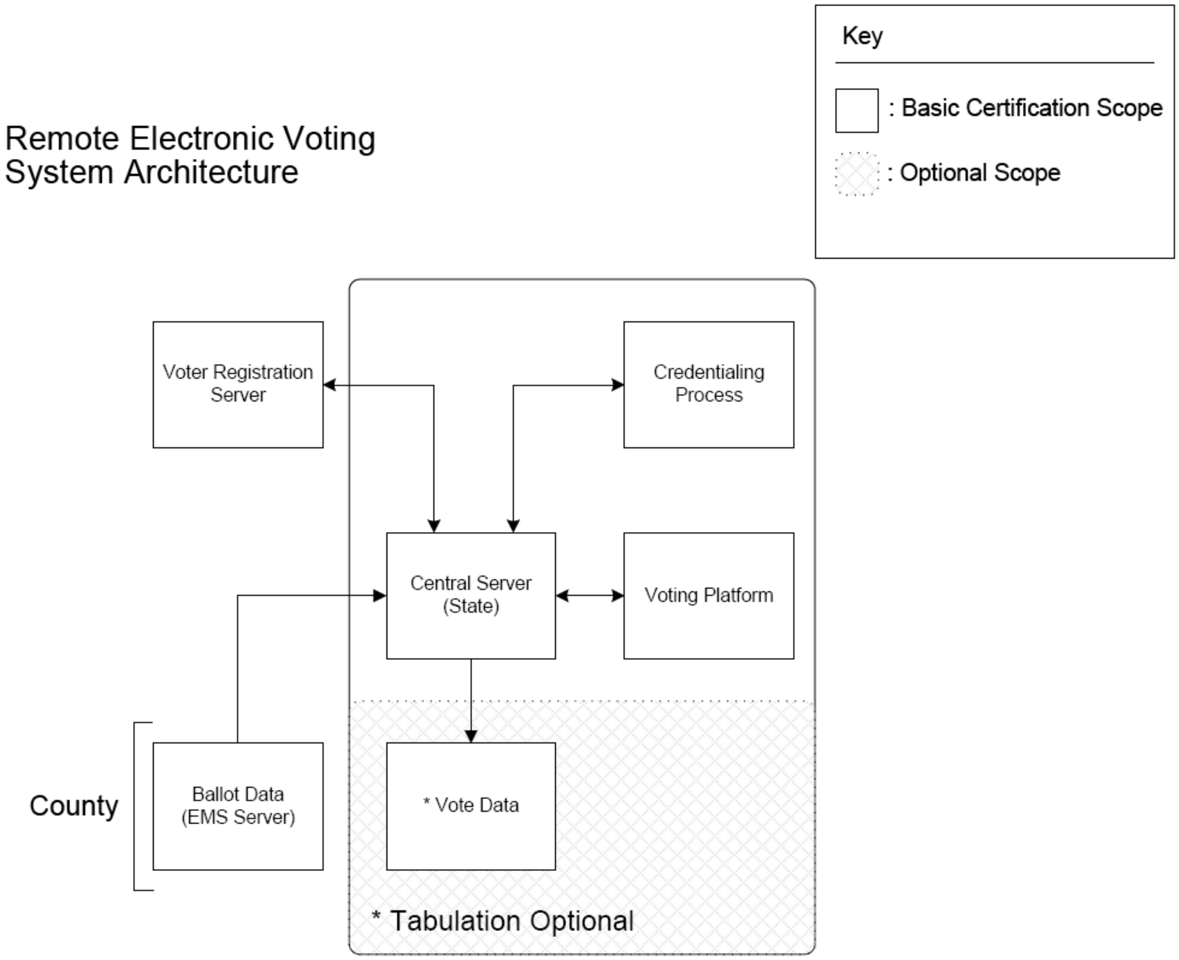
This decision has a few direct implications for the security dimensions of the project:

- The voters will go to a designated polling location to vote.
- The voters will provide ID/signature to authenticate themselves to poll workers prior to voting.
- The polling location will be staffed and controlled. The voting device at the remote location will be under the direct supervision of an election official or delegate at all times during voting hours.
- The voting platform will be set up and deployed in a controlled and known state.

As a failsafe measure, volunteer voters will be advised to use the by-mail process as a procedural back-up in the event the System experienced an unanticipated outage or other operational problem

The voting period will extend from the date of availability of absentee ballots in participating jurisdictions through the close of polls

SYSTEM ARCHITECTURE HIGH-LEVEL OVERVIEW



Polling Location

The credentialing process and voting platform are located in the remote polling location. These functions will take place on devices dedicated to these functions and under the control and supervision of poll workers during voting hours.

A voter-verified paper record of each vote will be used to audit the electronically transferred results.

Central Server (State)

The content of all transactions passed through or stored on the Central Server will be securely encrypted so only the addressing information can be read for communications routing purposes.

The system will provide for immutable logs of all system transactions that will allow state election officials to identify and correct unauthorized use of the system.

Communication

The location of the Central Server and the methods for communication with a state's sources of voter registration, and ballot definition information will be determined by its policy and existing infrastructure.

Project Risk Assessment

Confidentiality:

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]"

Access to voter registration information, including voter's signature:

- Restricted to authorized poll-workers.

- Access to the voted ballot records
    - The pilot testing requirements lists the documentation required of the vendor to describe its encryption methods protecting the privacy of the ballot record.

Integrity

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]"

- Alternate paper channel for capturing ballot choices – can be used to verify the integrity of the electronic process

- One person-one vote
    - This project envisions two basic models for protecting one person-one vote:
        - The *absentee model* requires the system to store voter information that encapsulates the voted ballot record. The election administration jurisdiction is responsible for procedures that ensure **only one ballot per voter is *counted*** even if the voter is able to cast multiple ballots.
        - The *early voting model* requires the system to prevent a voter from casting more than one ballot. The election administration jurisdiction is responsible for coordinating multiple channels of voting so that **only one ballot per voter is *cast***.

Availability

"Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]"

- At the remote location:
    - Alternate channels available – including mail, email, and fax – in the event that a connection becomes unavailable.
    - The remote location will be available for several weeks up to election day. In many cases it will be possible for the voter to return at a later time.
- At the election administration server site:
    - 24/7 availability goal
    - The activities of processing voted ballots occur over a period of days or weeks. In most cases, there is adequate time to re-establish availability of the system.

Conclusion

The impact of a security breach in this pilot project on the overall mission of election administration can be considered low in all three categories of FIPS security objectives: confidentiality, integrity, and availability. The key factors that lead to this conclusion are:

- UOCAVA voters will not be disenfranchised if the remote method isn't available to a voter. Alternate voting channels are accessible to the UOCAVA voters.
- An alternate channel for capturing voter choices that doesn't depend upon the information technology deployed in the pilot to protect it
- The current standard of privacy provided by available technology – email and fax – is considered a relatively easy standard to exceed.
- The relatively small scale of this project makes it highly improbable that votes cast using this technology would exceed the margin between a winning and losing candidate.

Within the context of the pilot project as mandated by Congress, the impact of a security breach that allowed an entity to target specific voters and determine how they voted should be considered moderate under the FIPS classification system. One requirement of the federal mandate is that an electronic voting system will maintain the privacy of the voter. Should such a breach occur it will be necessary to analyze the extent of the vulnerability to determine whether the technology can be used in large scale applications.

Finally this pilot experiment will need analysis as to whether this manned remote location approach can be scaled to meet UOCAVA needs. This approach is anticipated to be cost and labor intensive. Further research into refinements of this approach that would allow a broader implementation may be required as the next step toward meeting UOCAVA needs.