

Input to SB 11 Working Group Oct 2015

Virginia Verified Voting

Status

- **We recommend focusing the report on identifying 3 high level items:**
 - Risks posed by electronic ballot return
 - System requirements intended to reduce those risks
 - Technical and policy ramifications derived from those requirements
- These 3 items could serve as the starting point for a designing and procuring a system to meet the requirements, but many of the detailed necessary steps to derive a system from high level requirements are out of scope for the time remaining in 2015.
- The report should also note that on-line ballot submission has not significantly improved turnout in other states.
- In particular, reaching consensus on system requirements is key. Until there is agreement on the system requirements, there is no way to make informed comment on the possible cost, designs and risks of any proposed system.

High Level Risks (Incomplete, Partial Threat Model)

Prior to defining the security requirements and processes for a proposed system, it is important to identify the security risks that the system should be required to prevent (aka a threat model).

A common approach is to focus principally on threats from internal and external adversaries, although similar problems often arise from system failures related to software design flaws, equipment malfunctions, human error during operations. These sources of errors are common and expected.

So the phrase “Adversaries could ...” should be interpreted as shorthand for “Adversaries, system failure, privileged insiders, or unintentional human error could ...”.

Any system should be required to protect against risks regardless of the source.

- Adversaries could deny voters access to the system during an election
- Adversaries could observe the contents of voters’ ballots, opening them to coercion or enabling vote selling.
- Adversaries could intercept ballots en route and selectively prevent some or all from being received, (especially vulnerable if ballots are not encrypted.)
- Adversaries with control of malware on voters’ computers could cause ballots to be corrupted prior to encryption and submitting
- Adversaries could masquerade as the state and collect ballots in its stead
- Adversaries could alter ballots en route (especially if ballots are not digitally signed)

- Adversaries could usurp another's identity to cast ballots in a voter's stead.
- Adversaries could enter the system and alter or destroy cast ballots
- Adversaries could enter the system and publicly disclose identities of voters along with their cast ballots
- Insiders could alter or destroy cast ballots, or disclose voters' ballots
- Adversaries could attack ballots in transit between the SBE and localities
- Adversaries and/or insiders with access to both this system and the registration system could create records of absentee ballot requests and cast ballots to introduce fraudulent ballots
- Adversaries could submit ballots containing malware to corrupt or damage election internal networks
- Adversaries could cause the wrong ballot types to be provided to voters
- System overload could occur (e.g. a Hurricane Sandy scenario)

High Level System Requirements

To counter the potential risks, any on-line balloting system must meet the following system requirements. Note, that existing absentee balloting procedures have corresponding protections enforced with witness signatures, multiple sealed envelopes, election observers and other procedures.

- **Authenticate each voter's identity using trusted certificates**
 - Cast ballots should be digitally signed using a DoD CAC with a key signed by a trusted certificate authority
 - Self signed certificates are worthless for establishing identity
 - Insecure methods such as passwords and PINs distributed by email are not acceptable for verifying voter identity.
 - Election officials must review ballot signatures prior to counting ballots to compare the certificate name with the voter name, as done currently with mail in ballots.
 - This requirement corresponds with the current signed and witnessed outer envelopes that are reviewed by election officials before accepting ballots in the current system.
- **Preserve ballot secrecy using robust encryption**
 - No one should be able to discover how an individual voted
 - Cast ballots should be encrypted end-to-end during transit.
 - Cast ballots should be encrypted during storage.
 - The encryption methods use for transit and storage may be (and probably will be) different.
 - Note that there are many tricky details involved to securely encrypt ballots in a usable way without allowing the voter's identity to be discovered when the ballot is decrypted. Significant care is necessary to design a system that balances competing requirements for ballot secrecy and integrity.
 - This corresponds with the current sealed inner envelopes that prevent anyone, even election officials, from seeing how a voter voted.

- **Preserve ballot integrity with digital signatures or a secure hash**
 - Once received, cast ballots must be stored in a fashion that prevents them from being altered, duplicated or destroyed – and that retains a strict audit trail to demonstrate chain of custody
 - The best method to prevent altered ballots is to sign them with a digital signature, or a hash generated checksum, which will be invalidated if any bit is modified
 - The identity of the voter must remain separate from the ballot to preserve secrecy, so any signature used for storing ballots will need to be different from a voter digital signature used for transmission
 - This requirement corresponds with the current physical security measures such as locks and seals used to protect cast ballots.
- **The system should have a single entry point for a narrow attack surface**
 - The state should collect remotely cast ballots at a *single* secure site
 - The state should not expect 140+ localities to develop secure systems
 - Critically, the state should also not deliver cast ballots to localities electronically after collecting them from voters
 - Delivering cast ballots to localities electronically would expose the system to compromise at each locality. See the open questions section for further discussion.
- **The system should be completely under state control**
 - It is not acceptable to host this system in a vendor's cloud environment, using software and systems that are opaque to the state
 - Vendors will offer inexpensive solutions that involve turning the entire process over to their private systems, with little oversight or real security, regardless of marketing literature. Do not accept private control of our elections.
 - This requirement does not mean that the state should not contract for outside technical expertise to assist in the implementation and operation of a voting system, but that the state should control the system, retain complete oversight including over any software developed, and the requirements and procedures should be determined by the state, not fit to a vendor's current offerings.
- **Provide secure ballot storage while preserving secrecy**
 - The system should give an election official (with observers) the ability to confirm the name on the digital signature of a ballot matches the voter who was sent the absentee ballot
 - Once voter identity has been confirmed, the association of voter identity with the (sealed) cast ballot should be permanently severed
 - If a ballot is not accepted, the system should preserve all relevant information so that the ballot can be considered during a canvas or recount (according to the Code)
 - The system should implement this requirement in a way that does not display the voter identity and ballot together

- This requirement corresponds with the current process of having election officials validate information on the outer envelope before separating it from the inner sealed envelope (thus preserving ballot secrecy), and setting questionable ballots aside to be considered by the local electoral board.
- **Ensure only qualified voters cast ballots, and they vote only once**
 - The system should interface with the voter registration system to record when ballots are received and verify that an absentee ballot was requested and sent
- **The system should prevent and detect attacks, intrusions and insider threats.**
 - Note that this is only possible at the server end; not the voter's end; and is a challenging requirement even for a single server
 - The system should not allow any single person to perform critical actions (e.g., open or close the election, examine or delete an individual ballot) without an observer and audit log.
 - The system as a whole should meet stringent security standards, and be subject to periodic review for compliance
 - At least DoD Protection Level 2 (PL2), preferably PL3
- **The system should be open to meaningful oversight by election officials and authorized election observers.**
 - The system should log all activity to support audits and intrusion detection, and in a way that is difficult for intruders to alter
 - Oversight of a system that preserves ballot secrecy is complex
- **The system should only collect cast ballots**
 - The state should not attempt to create an interactive on-line voting system. That would require each ballot throughout the state to be programmed each year increasing cost, complexity and risk
- **The state should develop detail plans for recovery in the event of compromise of each part of the voting system**
- **The state must have a regular program to test, patch, upgrade and audit the system, with safeguards to ensure that changes do not undermine security**
 - Procedures should include regular system review by security experts, including but not limited to, penetration testing.

Ramifications

Technical Ramifications

- The system will likely need to use a web site to receive ballots instead of email to ensure encryption throughout transit. Web based encryption (HTTPS/SSL) is an end-to-end solution, but email based encryption (SMTP with TLS) can be only be enforced for the final hop. However, the requirement is to transport digitally signed ballots with end-to-end

encryption, a design that meets that requirement with either transport protocol could be feasible.

- The system should interface with the DoD CAC network via the published API
- Voters would need a CAC card and a web browser that supports HTTPS connections, along with a way to record an image of their cast ballot to return
- Cast ballots would be image files of marked ballots. The blank ballots would have been provided by the locality as done currently.

Policy Ramifications

- The state should maintain the system on networks that it controls, not hand control of ballot return to a system under vendor control
- The current process of requesting and sending ballots to overseas military can be maintained
- The name checks that are currently performed at the locality CAPs with observers, would instead be performed for these voters at the state level
- The state will need a process in place to distribute cast ballots to the localities after the polls close (see the first open question)
- The SBE should have procedures to regularly test the security of the system, conduct security audits, identify intruders, and apply security patches
- The SBE will need to have particular safeguards on whatever system is used to open the submitted ballots, as those ballots may contain malware
- The SBE should have plans in place on how to respond to security breaches and incidents
- In addition to designing, implementing, operating and reviewing the system, the state should have independent security experts (separate from the implementers) review the design, code, procedures and perform penetration tests [before determining if safe to deploy] and regular audits.

Open Questions

- How should cast ballots be distributed to the localities?
Doing so electronically raises many costs and risks. One recommendation is to use a physical courier system after the polls close to make a one-time delivery from the state to jurisdictions so that the ballots can be counted in time to certify the election. This will likely require a revision to current code, which requires ballots to be provided to the clerk of the court by noon on the day after an election. Alternatively, the state could count these absentee ballots centrally, and provide the totals to the localities first, possibly electronically, and then deliver the cast ballots to the clerks in each locality. Centrally counting military absentee ballots at the SBE would be a new model for the Commonwealth, and would likely require Code changes.
- Would it be possible to have localities send some sort of electronic form (e.g., PDF, HTML) for blank ballots that voters could then mark off-line and return electronically?

That would be more convenient for voters, but more work for localities. If only some localities made that effort, would it raise equal protection issues?

- What changes are needed to code and procedures for observers, canvasses and recounts?
- What process should the state employ to certify this system? There are no federal guidelines for electronic ballot return to certify against. The EAC has not created federal guidelines for remote ballot return because the National Institute of Standards (NIST) has determined that the technology to remotely authenticate voters identity and to securely return voted ballots does not yet exist for the current Internet.