

Virginia State Board of Elections Senate Bill 11 Workgroup

Considerations for Adopting Electronic Transmission of Marked Ballots

October 13, 2015

The Virginia State Board of Elections Senate Bill 11 Workgroup presents the following considerations that must be taken into account should the Commonwealth decide to pursue the electronic transmission of marked ballots. Each consideration includes known risks and suggested mitigating controls that could be implemented to ensure the integrity and accuracy of the process.

The Workgroup acknowledges that the electronic transmission of marked ballots would enable voters to cast their ballots quickly and easily, and meet absentee ballot deadlines, however, these issues of timeliness and convenience also come with additional challenges and considerations that must be taken into account.

Consideration: Accessibility

The Internet voting process must be readily available to, and usable by, all voters eligible to vote by Internet voting, even in the presence of Internet voting-specific threats. Web accessibility means that people with disabilities can use the Web. More specifically, Web accessibility means that people with disabilities can perceive, understand, navigate, and interact with the Web, and that they can contribute to the Web. Web accessibility also benefits others, including older people with changing abilities due to aging.

Risks:

The site is not accessible to voters with special needs potentially limiting eligible voters' participation in an election.

The site is not intuitive for voters with special needs or does not render with the use of assistive technologies adding obstacles to eligible voters' participation in an election.

Controls:

Online software should be thoroughly tested using automated testing tools and also tested by users with varying abilities and needs.

Online software should be certifiable to all W3C accessibility guidelines and Section 508 of the Rehabilitation Act of 1973, as amended in 1998 (29 U.S.C. § 794 (d)).

Consideration: Auditability

Web applications potential vulnerabilities can be mitigated, to a degree, by thorough and secure auditability of transaction records. Audits of transactions can be used retrospectively to assist in determining that transactions were completed unaltered, that the code of the online applications was only changed by authorized persons, and that the system experienced no logical or technical errors that

affected the outcome of the voting process. User facing transaction audits can be used in conjunction with automated transaction logging to provide voters with confidence in the voting process.

Risks:

Electronic transmission does not allow a voter to verify if the ballot received matches the one sent, and without a paper record, a cyberattack may be undetectable.

After an election there are no artifacts that are human readable to be used in recounts or contested elections.

Applications are hacked and voting information is changed at some point in the transaction process.

Application servers experience technical failures preventing the sending or saving of vote data.

Controls:

The deployment of a secure, encrypted user validation of vote received as cast. There are several direct and indirect methods of providing this assurance.

A secure audit log of all application transactions is maintained on a secure server. All audit log records should be encrypted and there should be a methodology used to provide evidence of tampering with audit log records.

Consideration: Authentication

How to verify the identity of the voter must be determined. For example, Alaska requires that the ballot be accompanied by two authentication documents that must be printed and signed by the voter and a witness.

Risks:

Voter authentication is flawed and allows a person to impersonate an eligible voter.

Voter authentication is too restrictive preventing eligible voters from casting a ballot.

Controls:

Use a well-documented secure voter authentication process that uses information only knowable by the authorized voter.

Use a third factor authentication method.

Consideration: Ballot anonymity

The voting process must prevent at any stage of the election the ability to connect a voter and the ballots cast by the voter.

Risks:

Voters' identity and ballot selections are visible to election office workers.

Voters' identity and ballot selections can be inferred from underlying audit data.

Controls:

Ballot selections need to be saved using an encryption technology that does not expose ballot selections and voter identity at any point in the vote counting process. This can be achieved by a technical process that is akin to the absentee ballot inner and outer envelope process. There is a digital wrapper which contains voter information used to confirm voter identity and eligibility and a separate encrypted package that can be separated from the voter record once the voter has been authenticated. Then a separate technical process decrypts the voted ballot file and allows for counting of the vote.

Audit records must not store unencrypted voter information and vote information.

Consideration: Denial of service attack

Potential attackers could disrupt the system by overloading it and prevent communications (i.e. voted ballots) from getting through.

Risks:

Denial of service (DoS) attacks can be used to target specific voters' access to systems or be used to interrupt the sending or receipt of ballots.

DoS attacks can call into question the integrity of the underlying system.

Controls:

Working with the hosting provider to establish quality of service rates to limit the amount of bandwidth one customer can utilize.

Using firewalls and filtering devices to filter all unnecessary ports and protocols.

Incorporating redundancy and resiliency into designs of key systems.

Utilizing IDS/IPS to identify and block attacks in progress.

Using distributed cloud hosted systems that can reroute traffic in the event of attacks.

Consideration: Inconvenience for the local election official

If each electronically received ballot must be duplicated, probably by a bipartisan team, it is an additional burden on the local election office.

Risks:

The additional work load on a local election official will delay completion of needed tasks.

The ballot transcription process is performed inaccurately leading to votes being incorrectly tabulated.

Controls:

Systems that automatically transcribe ballots can be developed so that voters' choices can be marked on a tabulatable ballot directly from the voter's choices.

Effective documentation of processes provided to local election officials can assist in optimizing back office practices.

Consideration: Individual and independent verifiability

The voting process will allow the voter to verify that their vote has been counted as cast, and for the tally to be verified by the election administration, political parties and candidate representatives.

Risks:

Man-in-the-middle attacks could alter the voter's ballot selections without their knowledge or consent.

Voted ballot records could be manipulated by insider attacks.

Transcription processes can lead to inaccurately tabulated votes.

Controls:

As mentioned above in auditability, voter facing auditing and third factor authentication can be used.

Systems that automatically transcribe ballots can be developed so that voters' choices can be marked on a tabulatable ballot directly from the voter's choices.

Consideration: Non-reliance on trustworthiness of the voter's device(s)

The security of the Internet voting system and the secrecy of the ballot should not depend on the trustworthiness of the voter's device(s).

Risks:

Local machines used to access the system may be infected with viruses, spyware, and/or malware that intercepts information provided by the voter allowing hackers to assume the voter's identity or modify voted ballot information.

Controls:

All software should run independently from the local machine of the user and all communication should be made through secure (SSL) channels.

Voters should be encouraged to run anti-malware and virus disinfection processes prior to beginning the voting session.

Consideration: One vote per voter

Only one vote per voter is counted for obtaining the election results. This will be fulfilled even in the case where the voter is allowed to cast their vote on multiple occasions (in some systems, people can cast their vote multiple times, with only the last one being counted).

Risks:

Voters can submit more than one vote for counting and more than one vote is counted.

Voters who submit more than one vote for counting have no valid votes counted.

Controls:

Proper voter authentication can provide a mechanism to securely associate any number of submitted ballots with a specific voter. A technical and auditing process can be created that ensures that only one valid vote per voter is decrypted and sent for tabulation.

Consideration: Only count votes from eligible voters

The electoral process shall ensure that the votes used in the counting process are the ones cast by eligible voters.

Risks:

Votes are received from voters which are not authenticated for eligibility and are counted.

Votes are received from voters for offices for which the voter was not eligible.

Controls:

Proper voter authentication can provide a mechanism to securely associate any number of submitted ballots with a specific voter.

Proper voter authentication can ensure that the correct ballot style is received from the voter and ensure that ballot style is the same one received from the voter.

Consideration: Privacy

As with all contemporary online systems, citizens have an understandable concern about the improper or unauthorized use of personal information provided to a system. Voting systems also need to maintain anonymity of the voter in relation to the ballot presented for counting.

Risks:

Personally identifiable information about voters is exploited for unauthorized use.

Voted ballot information is associated with a specific voter.

Controls:

Comprehensive security audits of the system must be maintained to ensure that no personally identifiable information is accessible to unauthorized parties.

Effective security audit controls must be in place and personnel must be available to monitor logging.

See above for ballot anonymity controls.

Consideration: Process validation and transparency

The procedures, technology, source code, design and implementation details, and documentation of the system must be available in their entirety for free and unconstrained valuation by anyone for testing and review for an appropriate length of time before, during and after the system is to be used. Policies and procedures must be in place to respond to issues that arise. Appropriate oversight and transparency are key to ensuring the integrity of the voting process and facilitating stakeholder trust.

Risks:

The system integrity is called into question and no outside entity has reviewed the process.

System vulnerabilities are exploited that could have been uncovered by external reviews of code and process.

The process does not align with statute and regulation.

Controls:

The creation of external advisory group to ensure compliance with statute, regulation and administrative practices.

The publishing of source code to a public repository for code review by computer scientists and engineers.

Conducting mock elections and providing a pre-election and post-election snapshot of all source code and compiled software to independent auditors.

Consideration: Security of the election process

Many cybersecurity experts are concerned that any Internet connection could be vulnerable to hacking or other cyber-attacks.

Risks:

The voting system becomes a cause celebre among electronic voting critics.

The voting system comes under white-hat attacks by experts who exploit vulnerabilities.

Controls:

Proper engagement of the broader technology community throughout the development, testing and deployment process can lead to a more collaborative relationship with the cybersecurity community.

Consideration: Service availability

The election process and any of its critical components (e.g., voter list information, cast votes, voting channel, etc.) will be available as required to voters, election administrators, observers or any others involved in the process. If Internet voting should become unavailable or compromised, alternative voting opportunities should be available.

Risks:

The online ballot service is unavailable and voters' have no alternatives to submitting their ballots in a timely fashion.

Vote tabulation services are unavailable and election officials have no other voted artifact to tabulate preventing valid votes from being counted.

Controls:

System redundancy and distributed cloud deployment can substantially reduce the likelihood of system unavailability.

Voters should be provided with alternative channels for returning voted ballots.

Consideration: Voter authentication and authorization

The electoral process will ensure that before allowing a voter to cast a vote, that the identity of the voter is the same as claimed, and that the voter is eligible to vote.

Risks:

Voter authentication is flawed and allows a person to impersonate an eligible voter.

Voter authentication is too restrictive preventing eligible voters from casting a ballot.

Voter authentication is flawed and provides the voter with an incorrect ballot style.

Controls:

Use of a well-documented secure voter authentication process that uses information only knowable by the authorized voter.

Use of a third factor authentication method.

Proper voter authentication can ensure that the correct ballot style is received from the voter and ensure that ballot style is the same one received from the voter.

Consideration: Voter coercion

The possibility that a voter could be coerced into voting a certain way is a consideration for electronic transmission, as well as for traditional mail absentee voting.

Risks:

Because the online voting session is not necessarily private, the voter is compelled to cast a vote by a third party.

The voter can document the way in which s/he has voted to a third party in order to receive compensation for his/her vote.

Controls:

A system that can receive multiple votes from each voter and receive votes from multiple device types can remove the incentive from the coercing party. If a voter can simply cast a second (or third ballot) in privacy, the incentive for coercion is removed.