Commonwealth of Virginia

SB11 Workgroup Draft Report Version 1

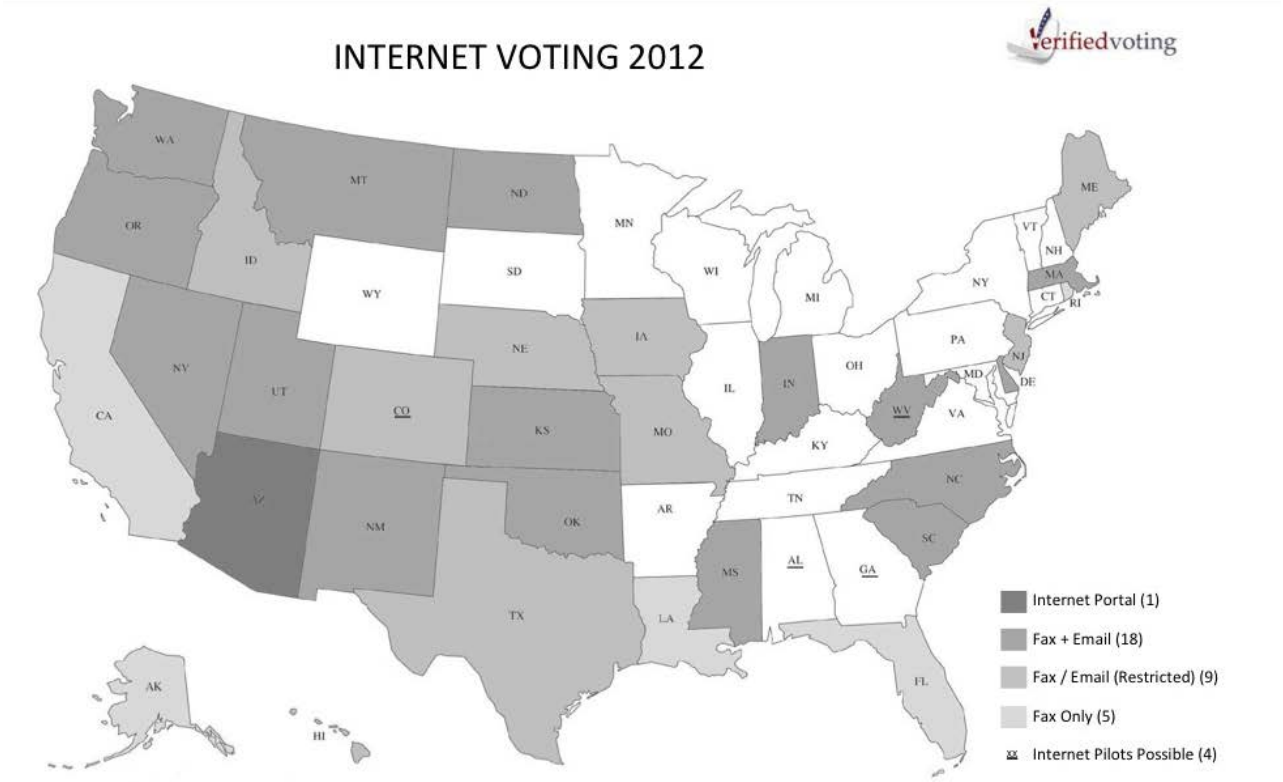
UOCAVA Electronic Voting

Introduction

The SB11 workgroup has been charged by the 2014 General Assembly to provide instructions, procedures, services, a security assessment, and security measures for the secure return by electronic means of voted absentee military-overseas ballots from uniformed-service voters outside of the United States. The bill requires the State Board of Elections to develop and update annually a security assessment and security measures to ensure the accuracy and integrity of these votes. The State Board is directed to convene a working group for the development of the initial instructions, procedures, services, security assessment, and security measures submitted annually to the Governor and General Assembly beginning January 1, 2016 on the feasibility and cost of implementation of the secure return of these ballots. The State Board of Elections convened the 1sts meeting of the workgroup in July 2015. At this meeting the group proposed a paper be drafted to document the current state of internet voting in the United States, what other states are doing with internet voting, how close races have been in the past, implementation costs, security proposals from vendors, and security risks.

Internet Voting 2012

Source: https://www.verifiedvoting.org/resources/internet-voting/ Verified Voting



Voting Methods by State

Adapted from National Conference of State Legislatures 7/27/2015

Source: http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx

				Who can use this?				
State	Email	Fax*	Web	All	UOCAVA	Emergency	Sub-class	Disabled
Alaska	•	•	•	•				
Arizona	•	•	•		•			
California		•			•			
Colorado	•	•			•			
Delaware	•	•			•			
DC	•	•			•			
Florida		•			•			
Hawaii		•			•	•		
Idaho	•	•			•	•		
Indiana	•	•			•			
Iowa	•	•			•		•	
Kansas	•	•			•			
Louisiana	•	•			•			
Maine	•	•			•			
Massachusetts	•	•			•			
Mississippi	•	•			•			
Missouri	•	•			•		•	
Montana	•	•			•			
Nebraska	•	•			•			
Nevada	•	•			•			
New Jersey	•	•			•			
New Mexico	•	•			•			
North Carolina	•	•			•			
North Dakota	•	•			•			
Oklahoma	•	•			•			
Oregon	•	•			•			
Rhode Island		•			•			
South Carolina	•	•			•			
Texas		•			•		•	
Utah	•	•			•			•
Washington	•	•			•			
West Virginia	•	•			•			

*Faxes can be sent over phone lines or over Internet

Case Study: Alaska

Source: http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx#Alaska

Alaska is the first state to offer all voters (not just UOCAVA voters) the chance to submit an absentee ballot electronically. It did so because it has a particularly a mobile voting population, with many voters not available to vote in their home jurisdiction on Election Day.

Based on this need, in 2012 Alaska developed an online system for returning ballots. UOCAVA voters can apply for an electronically transmitted absentee ballot any time. Civilian voters must apply beginning 15 days before the election. Absentee ballot applications can be sent by mail, fax or email.

When the election official receives an absentee ballot application, he or she first verifies that the voter is registered and eligible to vote and then transmits the ballot via the method requested (mail, fax or via the online system). If the voter has requested to use the online system, the election official sends him an email containing links and instructions.

Voters can mark and submit a ballot through the online system, but must print out a "voter certificate" and "identification sheet" that must be signed by the voter and a witness. The two documents can then be scanned and submitted via the online system as well. Step-by-step instructions on how the online voting system can be found on the State of Alaska's Division of Elections website.

When a digitally transmitted ballot is received by the elections office, it is printed on official ballot paper stock and counted using the same optical scan system that counts other paper ballots.

If a voter prefers to mail the ballot back, he can still use the online system to receive and mark the ballot. It can be printed and returned by mail. If by mail, he would print off a secrecy envelope, instructions and a return envelope from the online system. All these documents are available in PDF format in one downloadable zip file.

According to a press statement regarding Alaska's online ballot transmission system, it is hosted in a dedicated secure data center protected by a layer of redundant firewalls. In order to ensure the security of the system, it is under constant physical and application monitoring.

Case Study: Connecticut

Over the last few years legislators in Connecticut have expressed a continued interest in providing electronic ballot transmission of voted ballots by military and overseas voters. Because of security concerns and other issues, the state has not yet implemented a system for the return of voted ballots by electronic transmission. Below is a timeline of key steps in Connecticut's process.

July 2011: In section 59 of SB939 the Connecticut legislature directed the Secretary of the State to conduct a study of Internet voting and recommend a method to permit UOCAVA voters to submit their ballots online.

October 2011: As a part of her study of Internet voting, Secretary of the State Denise Merrill conducted an online voting symposium that brought together academics and experts in the fields of computers science, cryptography, elections administration and voting technology. The security of

online voting was a key concern for the group. Two concerns were the integrity of online voting systems and the ability to keep voting information secret. As a result of the symposium and her review of online voting, Secretary Merrill submitted a report to the Government Administration and Elections Committee concluding that there is no existing secure method of online voting.

June 2012: HB 5556 is passed by the legislature but vetoed by the governor. It would have allowed military and overseas voters to return their voted absentee ballots by fax or email. The governor cited security concerns as outlined in a 2011 study of remote voting conducted by NIST and a concern with any mechanism that requires a voter to waive his or her constitutional right to a secret ballot.

June 2013: SB647 directed the Secretary of the State to select a method for UOCAVA voters to return a ballot that maintains security, the privacy of information contained on the ballot, and reaches the election official before the polls close on Election Day.

January 2014: Secretary Merrill submitted a report concluding that her office would require further legislative authorization to proceed with electronic return of voted ballots. Her response was based on her previous review of security for online voting and determination that online voting is not secure. The report also indicated that an appropriation would be required to provide a web-based delivery system for UOCAVA voters to download their ballot. Further legislative action would be required to provide a waiver of the constitutional right to a secret ballot for UOCAVA voters.

March 2014: SJ24 proposed a constitutional amendment to permit UOCAVA voters to waive the right of a secret ballot in order to vote by electronic transmission. SJ24 failed due to adjournment of the legislative session.

Close Election Results

State-Level Elections Since 1982

Election	Office	Jurisdiction	Vote Difference	Percent Difference
2014 November General	United States Senate	Statewide	17727	0.83%
2013 November General	Attorney General	Statewide	165	0.01%
2013 November General	Member House of Delegates	31st District	228	1.00%
2013 November General	Member House of Delegates	87th District	187	0.92%
2011 November General	Member House of Delegates	87th District	51	0.47%
2011 November General	Member Senate of Virginia	20th District	644	1.36%
2011 August Republican Primary	Member Senate of Virginia	22nd District	171	2.71%
2009 November General	Member House of Delegates	23rd District	209	0.98%
2009 November General	Member House of Delegates	41st District	209	1.02%
2008 November General	United States House of Representatives	5th District	727	0.23%
2007 November General	Member Senate of Virginia	27th District	659	1.34%
2006 November General	United States Senate	Statewide	9444	0.40%
2005 November General	Lieutenant Governor	Statewide	22387	1.16%
2005 November General	Attorney General	Statewide	323	0.02%
2000 June Republican Primary	United States House of Representatives	7th District	263	0.63%
1989 November General	Governor	Statewide	6740	0.38%
1982 November General	United States House of Representatives	6th District	1655	0.01%
1982 November General	United States House of Representatives	8th District	1549	1.11%
1982 November General	United States House of Representatives	9th District	1218	0.81%
Total Races = 19				

Local-Level Elections Since 2007

Election	Office	Jurisdiction	Vote Difference	Percent Difference
2015 June Republican Primary	Commonwealth's Attorney	Henrico County	67	0.46%
2014 May Town General	Mayor	Hillsville	4	0.60%
2013 November General	Member Board of Supervisors	District 3	6	0.65%
2013 November General	Member Board of Supervisors	Garrisonville	53	1.25%
2013 November General	Member Board of Supervisors	Petsworth District	23	1.21%
2012 November General	Mayor	Suffolk City	387	1.06%
2012 May Town General	Mayor - Herndon	Herndon	38	2.01%
2012 May Town General	Mayor - Saltville	Saltville	8	1.77%
2011 November General	Commissioner of Revenue	Lee County	116	1.84%
2011 November General	Member Board of Supervisors	Braddock District	371	1.51%
2011 November General	Member Board of Supervisors	North River District	18	2.47%
2011 November General	Member School Board	District 4	12	1.03%
2011 November General	Member School Board	Leesburg District	85	1.65%
2011 November General	Member School Board	Matoaca District	175	1.69%
2011 November General	Sheriff	Nelson County	11	0.21%
2011 November General	Treasurer	Greensville County	34	1.13%
2010 November General	Mayor - Goshen	Goshen	1	1.33%
2010 November General	Member City Council	District 7	2	1.14%
2010 November General	Treasurer	Lunenburg County	48	2.27%
2010 May Town Elections	Mayor - Saltville	Saltville	6	1.40%
2009 November General	Member Board of Supervisors	District E	16	0.90%
2009 November General	Member School Board	Battlefield District	29	0.86%
2009 June Democratic Primary	Member Board of Supervisors	Northern District	6	1.38%
2009 Fairfax Co Chairman BOS Special	Chairman-Board of Supervisors	Fairfax County	1206	1.17%
2008-May-Town Elections	Mayor	New Market	3	1.27%
2007 November General	Clerk of Court	Fairfax City, Fairfax County	1701	0.94%
2007 November General	Clerk of Court	Harrisonburg City, Rockingham County	220	2.25%
2007 November General	Member Board of Supervisors	Ashland District	15	0.82%
2007 November General	Member Board of Supervisors	Blue Ridge District	28	2.76%
2007 November General	Member Board of Supervisors	District 2	16	0.76%
2007 November General	Member Board of Supervisors	South District	3	0.47%
2007 November General	Member Board of Supervisors	Ware District	21	1.01%
2007 November General	Member Board of Supervisors At Large	Greene County	58	1.29%
2007 November General	Member School Board	Catawba District	28	0.69%
2007 November General	Member School Board	District 1	10	1.60%
2007 November General	Member School Board	Rocklick District	14	1.79%
2007 November General	Member School Board	Scott District	32	1.09%
2007 November General	Member School Board	Windsor District	12	0.76%
2007 November General	Sheriff	Franklin County	217	1.54%
Total Races = 39				

Security Risks

Pros and Cons of Electronic Voting

https://blogs.mcafee.com/consumer/hack-the-vote-pros-and-cons-of-electronic-voting/

On the one hand, countries like Canada, Norway and Australia have already experienced success with their adoption of online voting systems, and proponents say going digital will boost voter turnout and Election Day efficiency. On the other, naysayers cite hacking, malware, and other security threats as deal breakers that could threaten the backbone of American democracy. In a recent interview with NBC, McAfee's Pat Calhoun argued that the biggest hurdle to secure online voting is not security technology, but the creation of a national, government-run digital ID to ensure voter identification. This type of ID is already required for members of the military and many federal employees, but the concern is that American voters would not allow a broader measure to pass due to its implications for individual privacy. That being said, if such a system were set in place, we could in theory move away from a practice like email voting, and start to develop a secure online system that relied on the national ID. McAfee VP and Chief Privacy Officer Michelle Dennedy also elaborates more on these key points in a recent interview with Bloomberg news, delving into the differences between sensitive transactions like banking, which have already been taken online, and

challenges specific to the online voting process. While online voting systems can't be written off, ongoing cybersecurity challenges don't bode well for the immediate future of these platforms. There is still significant progress to be made over the next 4 years and beyond, and we'll be keeping a close eye on emerging developments.

Verified Voting

http://www.verifiedvoting.org/resources/internet-voting/vote-online/

Computer and network security experts are virtually unanimous in pointing out that online voting is an exceedingly dangerous threat to the integrity of U.S. elections. There is no way to guarantee that the security, privacy, and transparency requirements for elections can all be met with any practical technology in the foreseeable future. Anyone from a disaffected misfit individual to a national intelligence agency can remotely attack an online election, modifying or filtering ballots in ways that are undetectable and uncorrectable, or just disrupting the election and creating havoc. There are a host of such attacks that can be used singly or in combination. In the cyber security world today almost all of the advantages are with attackers, and any of these attacks can result in the wrong persons being elected, or initiatives wrongly passed or rejected.

Banks, online merchants, and high tech companies that do business online have huge security budgets to defend themselves against cyber attacks, and even so they are frequently victimized. If these organizations with such great expertise and capability in computer and network security can be successfully attacked, then no voting system vendor or local election administration has any realistic chance of successfully defending against similar threats.

If for some reason officials learn after the fact that a particular person has succeeded in casting an illegal ballot there is no way to find it to remove it from the count. In the U.S. and most other countries once a voting transaction is complete it cannot be undone even in principle because the information needed has been deliberately lost. In that sense a voting transaction is irreversible.

Internet voting requires a strong identity verification procedure because if an attacker can figure out how to cast one illegal vote online through a weakness in the identity verification, then he can automate that attack to allow thousands of phony votes to be recorded.

In the voting world we are all familiar with the cases where, within about one decade, a senator, a governor, and a U.S. president were all elected by margins much smaller than one vote in a thousand. Small changes in vote totals sometimes have very big, even global consequences, and can push a whole city, state or nation in a new direction. Elections outcomes are thus very sensitive to small errors or frauds. Election security is thus a matter of national security, and the security standards have to be designed to reliably prevent, detect, and correct even very small problems and attacks.

There is a powerful partisan incentive to block or change other people's votes, especially if it can be done without detection. The motivation to automate that process to affect thousands of online votes is that much greater. Such attacks can be done for tens of thousands of dollars or less, while the monetary value of changing the outcome of an election can be hundreds of millions of dollars or more, and the non-monetary value can be immense as well. With Internet voting the danger is actually much worse because anyone on Earth, including foreign governments, could derive great

benefit from tampering with U.S. elections, especially since it is unlikely they will be caught or brought to justice. Online voting is thus a national security risk.

NIST

http://www.nist.gov/itl/vote/upload/NISTIR-7700-feb2011.pdf

In February 2011, NIST release NISTIR 7770, Security Considerations for Remote Electronic UOCAVA Voting. This paper identified desirable security properties of remote electronic voting systems, threats of voting over the Internet from personally-owned devices, and current and emerging technologies that may be able to mitigate some of those threats. Based on the capabilities of current computer security and voting technologies, the following three issues remain to be significant challenges faced by remote electronic voting systems. First, remote electronic absentee voting from personally-owned devices face a variety of potential attacks on voters and voters' personal computers. Since the voter's personal computer is outside the control of election officials, it is extremely difficult to protect against software attacks that could violate ballot secrecy or integrity or steal a voter's authentication credentials. These are serious threats that are already commonplace on the Internet today. Second, remote electronic voter authentication is a difficult problem. Current technology does offer solutions for highly-secure voter authentication methods, but these may be difficult or expensive to deploy. Personally owned computers may not be able to interface with these methods, such as having the necessary smart card readers for cryptographic authentication using Common Access Cards or Personal Identity Verification cards. Third, it is not clear that remote electronic absentee voting systems can offer a comparable level of auditability to polling place systems. Because of the difficulty of validating and verifying software on remote electronic voting system servers and personal computers, ensuring remote electronic voting systems are auditable largely remains a challenging problem, with no current or proposed technologies offering a viable solution. Many of the current and emerging technologies identified in this report are areas with active research and development. Pilot projects should be encouraged, including those involving the use of voting-specific cryptographic protocols, such as the Helios voting system [23]. Emerging trends and developments in these areas should continue to be studied and monitored.

A Comparative Assessment of Electronic Voting Feb 2010 Prepared for Elections Canada by Canada-Europe Transatlantic Dialogue

http://labs.carleton.ca/canadaeurope/wp-content/uploads/sites/9/AComparativeAssessmentofInternetVotingFINALFeb19-a.pdf

"Practical testing and pilot projects are the only ways of knowing what will work and what will not. Trials of particular methods will give the best insight into understanding what requirements must be met for Internet voting to work well in Canada as well as the actual pros and cons of electronic approaches. A by-election is perhaps a useful starting point, but a more expansive trial would be necessary prior to the introduction of Internet voting nationally. A regionally concentrated trial, or a group of selected constituencies that are regionally representative, would be a useful approach to testing. Only after such testing would it be feasible to offer remote Internet voting as an option for all Canadian electors, as a complement to the traditional process."

Considerations for Adopting Electronic Transmission of Votes

While electronic transmission allows voters to cast their ballots quickly and easily, and meet absentee ballot deadlines, these issues of timeliness and convenience must be balanced by other considerations.

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.

Auditability
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.

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.

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.

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

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.

Individual and independent verifiability
The voting process will provide for 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.

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).

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).

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.

Privacy
Because election officials are able to identify the person who sent a ballot via electronic transmission, ballots are not fully anonymous. Privacy of the ballot is a value for voters and for society as a whole.

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.

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

Security of the voter's computer
Election officers cannot assume that the voters' computers are secure and free from spyware, malware, viruses' and keyloggers.

Service availability
The election process and any of its critical components (e.g., voters 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.

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.

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.

Ballot Return Method Comparisons

Ballot Return Method	Risk	Ease of Use For Voter	Ease of Use for Election Administrator
Fax			
Email			
Secure Electronic Return			

Proposals

To find out what was currently available in the market, ELECT submitted an RFI (request for information) and received 10 responses from various vendors. Implementation prices ranged from $50K to $1.9 million and annual costs from $50K to $1.15 million. Most of the systems proposed by the vendors replying to the RFI would have to be built and prices are only rough estimates and do not include costs to the Department of Elections and the local Elections officials for implementation and administration.

Security Measures Comparisons

From these proposals, the following security measures and considerations were documented.

Proposal	Data Security	Authentication	Network	Marked Ballot	Authorization & Access Control	Session Management	Monitoring
1	Logging of successful and failed login attempts. All personally identifiable and authentication date stored and transmitted encrypted. Security approach conforms to FIPS 200 and NIST 800-53, moderate-impact information systems.	Voter authentication uses a combination of data elements from voter registration records and an admin system to generate a URL (GUID) unique to each voter. Secure login protocols; complex passwords required; strong password hashing.	All communication from browser and servers is through secure HTTPS protocol. Stateful firewalls on the network perimeter. Network perimeter intrusion detction. Anti-malware and antivirus for all servers, Host-based intrusion detection and	Ballot is encrypted using FIPS 104-2 compliant libraries that use voting session-specific AES-256 keys and stored in the election-specific secure drop box. Drop box is protected using a strong key known only to admin.	User based roles		Internet perimeter is continuously scanned and monitored on a daily bassis by QualysGuard continuous secruity monitoring service for vulnerability management and threat protection
2		Uses CAPTCHA visual-image verification.		All clicks are recorded including IP address, but not the voting. The ballot data is encrypted. Marked ballot is viewable by those with the	User based roles	Voter record is flagged is a user attempts more than 3 login attempts.	

Proposal	Data Security	Authentication	Network	Marked Ballot	Authorization & Access Control	Session Management	Monitoring
3	Uses HTTPS with SSL/TLS protocol to provide encryption and secure identification of the server. Metts NISTIR 7682 and 7711 standards, tested by Wyle Labs and SLI. Auditing logs.	Strong password protection. Scheduled password expiration dates. Backed of the system displays the voter's signature from the ISVRS so the admin can confirm a match to the FPCA. System will display data entered by the voter to the information from ISVRS with a symbol denoting discrepancies.		Data is encrypted while sent through SSL/TLS and resident in the SQL db. Encryption uses NIST-approved cryptographic algorithms/schemas. For those using mobile devices, votes are not recorded on servers while the system creates their marks on the PDF. (p. 22)	Various access levels	5-minute time out for idle users.	Compares mobile biometric points over time to create an identify authentication probability algorithm; compares the differences in device, location, email address, and gesture sensors to calculate a number indicating the probabily of identity. Admin sees a risk number and can click to see the reasons.
Proposal	Data Security	Authentication	Network	Marked Ballot	Authorization & Access Control	Session Management	Monitoring
4 (custom build)	System will certify and store the metadata of the voted ballot and prevent an additional ballot from being submitted. All system events would be captured in an audit log. Architecture will not embed queries. URL parameters are hashed or in-session only. Avoid use of cookies. Embed JavaScript in code behind of the pages and never reveals critical information. When necessary,	CAC card or username/password. Users are authenticated via username and pasword that are encrypted per NIST standards.	Ensure network topology is designed to protect the server from external access.	Use secure transmission	User based roles.	Configurable session timeouts and user account inactivation settings will be built in. Caan secure the data between application and database servers using a secure port to the database.	Systems administrators will monitor, handle contingencies and alternatives to address emergencies, system failures or shutdowns.

Proposal	Data Security	Authentication	Network	Marked Ballot	Authorization & Access Control	Session Management	Monitoring
5	Audit logs track all access and activity within the system.	CAC PKI as authentication device for voters. Strong passwords.	Solution would rely on the inherent security measures of		Defined user roles		
6	Generates public key pairs for distribution, inclusion of SSL connections between Voter and Delivery. Employ visual components that guarantee election components have not been tampered with. Use tamper proof digital and physical security. Passed security inspections (no specifics provided). Full auditing facility to show access credentials used by location, IP address, ballots printed, ballots	Provides alternative methods of authentication (p. 9)	Intrusion protection, performance monitoring, and denial of service mitigation protocols at the server would be deployed using the software and the failover replication site. (p. 31)	Uses a variety of encrypted return routes to the database. Combine industry standard symmetric and asymmetric encryption. Ballots can be manually duplicated (?).	Layered series of roles.		

Proposal	Data Security	Authentication	Network	Marked Ballot	Authorization & Access Control	Session Management	Monitoring
7	Extensive security measures established and fraud prevention and detection procedures built in. Highest level of security protocols. Counts all instances of ballot access by voters and restricts access following voting. Auditing controls of activities are tracked.	CAC card. Users required to build strong passwords. Option available to also require a security key for election officials to make changes.		Marked ballot is encrypted. System does not record any votes. If electronically submitted, selections are removed and only exist on the print out after printing.	Role based access.		
8	2048-bi RSA encryption of AES keys with 256-bit AES encryption of the vote.	CAC card scanning. Strong administrative password. Uses strong hashing mechanisms and cookie integrity is validated on every request.	Their data centers are geographically separate. World-class expertise in computer security.		Role based access with limited set of permissions.	Cross Site Scripting, Cross Frame Scripting and Session Hijacking, Denial of Service Attack, Distributed Denial of Service Attach, Prevention of SQL injection, Prevention of Cross-Site Request Forgery.	Man-in-the-Middle (MiTM) attack detection.

Proposal	Data Security	Authentication	Network	Marked Ballot	Authorization & Access Control	Session Management	Monitoring
9	Immutable audit logs record actions of the app and users that are digitally signed at periodic intervals. Employs cryptographic protocols and technology protected by more than 40 international patents and patent applications.	Can be integrated with CAC cards to stongly authenticate and allow for digital signatures. CAC card identification uses the PIN associated to the card. The integration is provided by Silanis and their e-SignLive technology. They also provide key-roaming technology to deliver encryption keys to the voter's device when not online. (p. 13)	Tier III data center on a fault-tolerant platform.	Sign with a digital signature and encrypts the ballot with a public key and can only be decrypted by the associated private key - known only to authorized locality individual(s).	Authorization is role based and prevents users from accessing unauthorized material.	No voter information is cached or retained. All files containing this information is destroyed upon conclusion of any project.	Recommend monitoring of infrastructure, hardware, software, and security controls 24/7/365 by trained onsite professionals

Proposal	Data Security	Authentication	Network	Marked Ballot	Authorization & Access Control	Session Management	Monitoring
10)	Secrecy of votes will be maintained through cryptography. Decryption key released to authorized users when counting is enabled.	Voter will be authenticated by Biometric test using CAC Card reader. Credentials of authorized users are entered by admin. Failed logins should trigger a lock-out after certain number of failed attempts. Account lock-out should be maintained for a number of hours to prevent and discourage the attacher from further attacks. All authentication attempts should be logged (log in, log out, failed logins, password change requests)	Network will be secured through AAA (Authentication, Authorization Accounting). Benefits of AAA: increased flexibility and control of access configuration, scalability, standardized authentication methods	Marked ballot to be stored in an encrypted packet.	Authorization will be role based. Users cannot browse past their user role rights. User cannot access unauthorized page by entering the location into the URL. User cannot enter a file path into a URL and be allowed access.	Cookies shouldn't be used to keep sensitve data. State machine shouldn't be used to authenticate user. Session ids should be assigned, unique to user and randomly generated. Session id should be protected and never contain person information. Timeout should be set for inactive sessions.	Recommend regular Vulnerable Assessment and Penetration Testing (VAPT) - Identifies weakest link, eleimnates false positives, prioritizes threats, detects attach paths missed through manual testing, facilitates regular and frequent scans, secures against business logic flaws, increases ROI on IT security.

Conclusions