★ VIRGINIA ★
DEPARTMENT *of* ELECTIONS

SB 11 Workgroup Report

Building a Secure Electronic Return of Marked Ballots Solution for our Overseas Military Voters

Contents

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.[1] 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 1st 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.

Problem Statement

SB 11 seeks to increase participation of Virginia's uniformed service members who are stationed overseas, both in increasing the number of applications for ballots and in increasing the number of ballots returned in a timely manner for counting, through deploying a secure means of returning a marked ballot. As the following discussion will show, when comparing general public voters who apply to vote absentee by mail and uniformed service members stationed overseas, there is a significant difference in the percentage of ballots that are never returned for counting. There does appear to be no significant difference in the percentage of voters whose ballots are rejected, no matter their status.

For the general elections from 2010 - 2014, 5,050 ballots have been requested by uniformed service members who are stationed overseas.[2] Of those, 2,231 (44%) ballots were returned by mail or in person in time to be counted, 134 (3%) ballots were rejected and not counted, and 2,675 (53%) ballots were never returned.

Uniformed Service Members Stationed Overseas Absentee Statistics

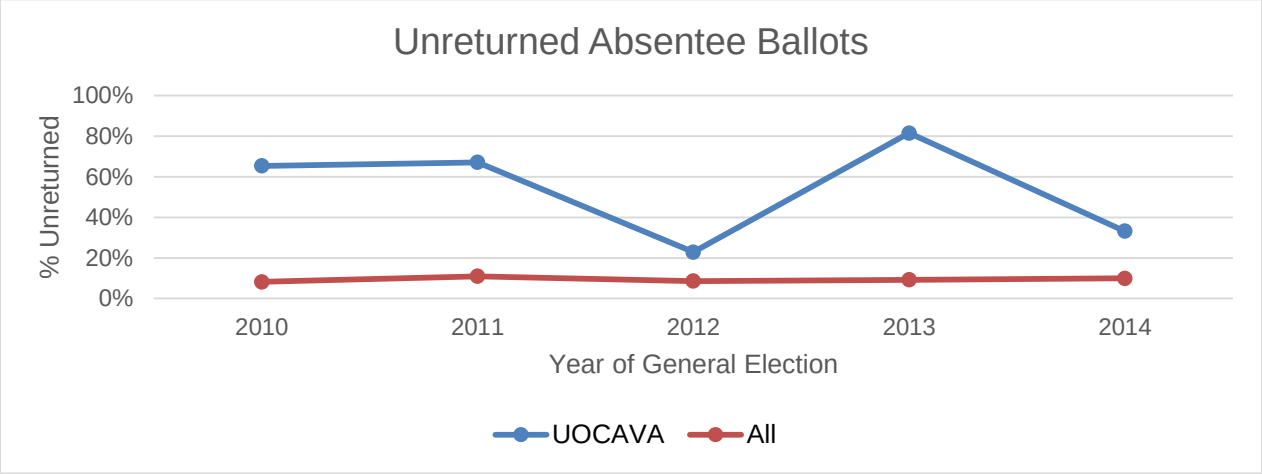
YEAR	2010	2011	2012	2013	2014
APPLICATIONS	1793	170	1741	1134	202
ACCEPTED BALLOTS	588	51	1273	193	126
REJECTED BALLOTS	33	5	70	17	9
UNRETURNED BALLOTS	1172	114	398	924	67
% UNCOUNTED BALLOTS	67%	70%	27%	83%	38%

For the general elections from 2010 - 2014, 321,385 general public voters have applied to vote absentee by mail.[3] Of those, 286,118 (89%) ballots were returned in time to be counted, 6,104 (2%) ballots were rejected and not counted, and 29,163 (9%) ballots were never returned.

[1] SB 11 (2014) available here: http://lis.virginia.gov/cgi-bin/legp604.exe?ses=141&typ=bil&val=sb11.
[2] The Department of Elections tracks these voters as 6E voters according to the reason identified on their absentee ballot application.
[3] For the purpose of this chart, mail includes couriers and postal service.

General Public Absentee Voting by Mail Statistics

YEAR	2010	2011	2012	2013	2014
APPLICATIONS	40050	27681	162226	45333	46095
ACCEPTED BALLOTS	36338	24343	145060	40062	40315
REJECTED BALLOTS	414	303	3121	1091	1175
UNRETURNED BALLOTS	3298	3035	14045	4180	4605
% UNCOUNTED BALLOTS	9%	12%	11%	12%	13%



Status of Absentee Voting in Virginia

Virginia voters can vote absentee if they have one of 19 qualifying reasons. A voter can make an application to apply vote absentee online, in-person or by mail. Military and overseas citizens are extended additional accommodations for absentee voting that include the ability to request that all ballots for the current calendar year and the next full calendar year be automatically sent to them a minimum of 45 days before each election (by mail or e-mail). These voters can also vote an emergency write-in absentee ballot if they believe that their regular ballot will not be returned in a timely manner. It is important to note however that all ballots, no matter the class of voter, must be returned either in-person, by courier, or by mail.

Other State's Answers to This Problem

Each state is grappling with the issue of increasing successful voting experiences for the members of our military. The focus of these efforts has been on the electronic return of marked ballots (e.g., internet portals, e-mail, or fax).

In July 2015, the National Conference of State Legislatures produced the following chart showing the options for electronic return of ballots. Two states provide an Internet portal for the return of marked ballots, while 27 states provide for e-mail return of marked ballots and 31 provide for fax return of marked ballots.

Electronic Return of Military and Overseas Citizens' Ballots

	Delivery Method			Who can use?				
State	Email	Fax*	Web	All	Military & Overseas Citizens	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	•	•			•			

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

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

Case Studies

Deploying a successful secure return of marked ballot solution is not unique to Virginia. Therefore, it is instructive to look to other states and how they have attempted to address this issue. Below are two case studies provided by the National Conference of State Legislatures (source: http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx).

Alaska Case Study

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.[4] [The voter certificate waves the right to a secret and secure ballot.]

When a digitally transmitted ballot is received by the elections office, it is transcribed onto 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.

Connecticut Case Study

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

[4] In addition to the NCSL report, ELECT research indicates that the voter's certification also includes an acknowledgment that the voter is waiving their right to a secret ballot and is assuming the risk that a faulty transmission may occur. *See generally*, https://www.elections.alaska.gov/vi_bb_by_fax.php.

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.

Identified Risks for a Secure Return of Marked Ballots Solution

In order to build a worldwide secure system that will enable Virginia's voters to return their ballot electronically, the General Assembly must determine the level of risk that it is willing to assume. Many individual risk cases can be identified, but all of them fall into two high level categories: ensuring the integrity of the ballots and process, and ensuring the confidentiality of the ballot and voter. The following risks have been identified by the workgroup, however additional risks will likely be identified and addressed as the workgroup proceeds:[5]

1) Denial of Service
    i) Just like any Internet facing system, the solution would be vulnerable to a denial of service attack, which could disenfranchise voters.

2) Interception of Ballots

[5] The workgroup recommends that a threat model be developed before electronic return of ballots is implemented. The threat model should identify risks and ramifications with mitigation strategies and defenses.

i) Due to the digital transmission of the ballots, it could be possible for a voted ballot to be intercepted in transit and destroyed, re-routed, modified or simply viewed.

3) Corruption of the Software and Data
   i) Controlled devices cannot be installed worldwide; therefore, the solution will have to rely on electronics accessible to voters and outside of the control of election officials. This equipment could be infected with malware.
   ii) Software and data on the Department of Election's computers may be manipulated or modified by submission of ballots containing malware.

4) Phishing, Identity Theft and Social Engineering
   i) Because of the lack of personal interaction with a worldwide solution, voters could be susceptible to complicated phishing, identity theft or social engineering schemes intended to disenfranchise a voter.

5) Observing Contents of Ballots and Voter Coercion
   i) Absentee voting through any means has the potential risk of being susceptible to a loss of privacy and/or susceptible to voter coercion since the ballot is marked and cast outside of the controlled space of a polling place.

6) Ballot Box Stuffing
   i) Fraudulent absentee ballot applications could be submitted resulting in fraudulent ballots being returned. In addition, without proper control, more ballots could be returned for counting than were sent out in the first place.

7) Ballot Spoofing
   i) Ballots could be swapped or modified prior to delivery to the voter, resulting in voters casting incorrect ballots which would ultimately disenfranchise the impacted voters.

Identified Considerations for a Secure Return of Marked Ballots Solution

Any technology solution has additional items that must be part of the requirements in addition to addressing known risks. The following considerations have been identified by the workgroup; however, additional considerations will likely be identified and addressed as the workgroup proceeds:

1) Accessibility
   i) Federal law requires that all online governmental systems for the public meet minimum accessibility standards. The solution must be built to comply with these standards and any state standards for accessibility.

2) Auditability
   i) The entire application, ballot transmission to the voter and the returning of the ballot must be auditable by an independent third-party.

ii) Care must be taken to minimize those who can view decrypted ballots. The solution must enforce separation of duties. Only local election officials should be able to ever view a fully decrypted ballot.

3) Availability
   i) The election process and any of its critical components (e.g., voter list information, cast votes, voting channel, etc.) must be available as required to voters, election administrators, observers or any others involved in the process. System redundancy is necessary and if the deployed solution should become unavailable or compromised, alternative voting opportunities should be available.

4) Authentication
   i) Absentee voting by mail and in person has several checks in place to determine a voter's identity. Uniformed service members have Common Access Cards (CAC) and incorporating their use into the authentication scheme for the solution would greatly enhance the trustworthiness of a submitted ballot.[6] In addition, use of the Commonwealth Authentication Service (CAS) would provide an additional layer of authentication.
   ii) The authentication method(s) must ensure that only one vote per authorized voter is cast per election.

5) Ballot Anonymity
   i) The solution must prevent at any stage of the election, the ability to connect a voter and their cast ballot. The encrypted voted ballot should be stored separate from the voter identity information in a manner that mimics the current inner and outer envelopes used in absentee voting by mail. Audit records must maintain ballot anonymity.

6) Encryption
   i) The solution must encrypt the voted ballot in transit and at rest.

7) Process Validation and Transparency
   i) 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.

8) Usability by the Voter
   i) Minimal effort and equipment must be needed by the voter to cast a ballot. Access to equipment such as scanners and fax machines may be limited in various deployment zones.

9) Usability by the Local Election Officials
   i) Impact to local election administration must be kept to a minimum where possible. Incorporating the solution into the workflows already in use for election administration and absentee ballot processing, while maintaining security and anonymity is key.

10) Technical Infrastructure

[6] A CAC card is administered and maintained by the Department of Defense and are used to identify the military member.

i) The solution must be hosted in an environment under the contractual control of the Commonwealth (e.g., the VITA/NG data centers). The use of firewalls, intrusion detection and prevention devices are required to help mitigate denial of service and other hacking attempts.
ii) Backups and redundancy must be built into the infrastructure to ensure maximum up time in the event of physical infrastructure failure.
iii) All physical infrastructure must be managed, maintained, and procured at the state level.

11) Vote Tabulation
    i) The solution shall not have the ability or data to tabulate votes. Vote tabulation must be completed in the local election offices as part of the existing election administration processes.

12) Implementation Timeline
    i) 2016 is a presidential election year. The workload for election officials is non-stop. Since the implementation of this solution will require funding and significant workload for both state and local election officials, a pilot launch of the solution for the 2017 June primaries is recommended with a full launch of the solution for the 2017 November General election.

Legislative Considerations

Certain legislative changes would significantly enhance the experience of voters using a secure return of marked ballots solution in Virginia. The General Assembly is encouraged to consider these recommendations during the 2016 session.

1) Voting System Certification
    a. Since this system is collecting ballots, it may fall under the requirements of certification for a voting system. It is unclear what level and type of certification is necessary for the State Board of Elections to certify ballot marking (as opposed to ballot counting) systems. This will result in a significant increase in the cost of the project and an extension in the timeline.

2) Witness Signature
    a. Current law requires that a witness sign the outer envelope of an absentee ballot submission attesting that the person submitting the marked ballot is who they say they are. This requirement should be waived for voters using this system as there is no known practical way to collect a witness signature. The use of the Common Access Card (CAC) by the military voters specifically targeted in SB 11 should be considered to be sufficient validation of the voter's identity for this specific purpose.

3) Secret Ballot
    a. Voters will have to waive their right to a secret ballot to use this system.

4) State Ballot Design and Seal
    a. Current law requires that the seal of the local electoral board appear on the back on a ballot. Ballots submitted through this solution should be exempt from this requirement as the ballots will have to be hand counted in each locality on the night of the election.

5) Ballot Duplication
    a. Current law prohibits the duplication of marked ballots; however, technical solutions exist (and are used in other states) that enable a marked ballot to be submitted with a barcode on them. The barcode can be scanned and a machine readable, properly marked version of the ballot can be printed immediately for counting.

Walk-Through of a Possible Approach

The workgroup presents a possible approach to enable military members who are deployed overseas to cast their ballot online. Here is a walk-through of the possible experience of the voter and local election official.

1) Voter applies to vote absentee and self identifies as a military member who is stationed overseas on election day. The voter may request that he be allowed to vote using the online solution and must provide a .MIL e-mail account; otherwise, these voters may use currently available methods to cast their ballot.

2) The local election official reviews the application and approves it.

3) The voter receives an e-mail at their .MIL account (which requires the use of a Common Access Card issued by the Department of Defense to access it) with instructions on how to access the Virginia ballot portal.

4) The voter goes to the ballot portal and logs in using a strong authentication system, such as his Common Access Card, Commonwealth Authentication Service (CAS), or other solution. All additional communication with the portal is encrypted.

5) The voter is presented with their ballot in their browser.

6) The voter marks their ballot and then reviews their selections.

7) The voter submits their ballot.

8) The marked ballot is converted into a PDF document, encrypted, and then stored in an encrypted database along with the name of the locality where the voter is registered.

9) A record is also saved in a separate database indicating that the voter has submitted a ballot successfully.

10) An e-mail is sent to the voter's .MIL account indicating that the ballot has been successfully submitted.

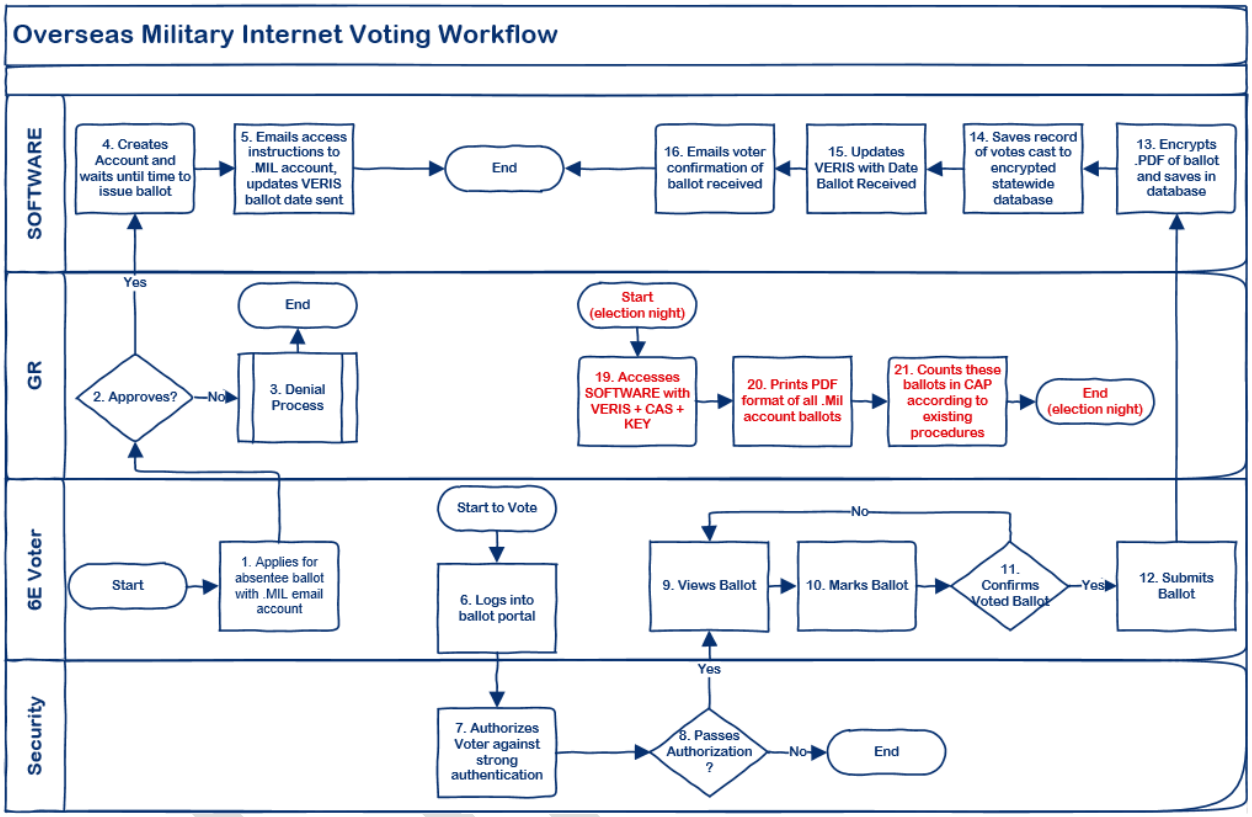
11) On the night of the election, the local election official accesses the ballot retrieval system by providing their credentials for the voter registration system and by authenticating against the Commonwealth Authentication Service.

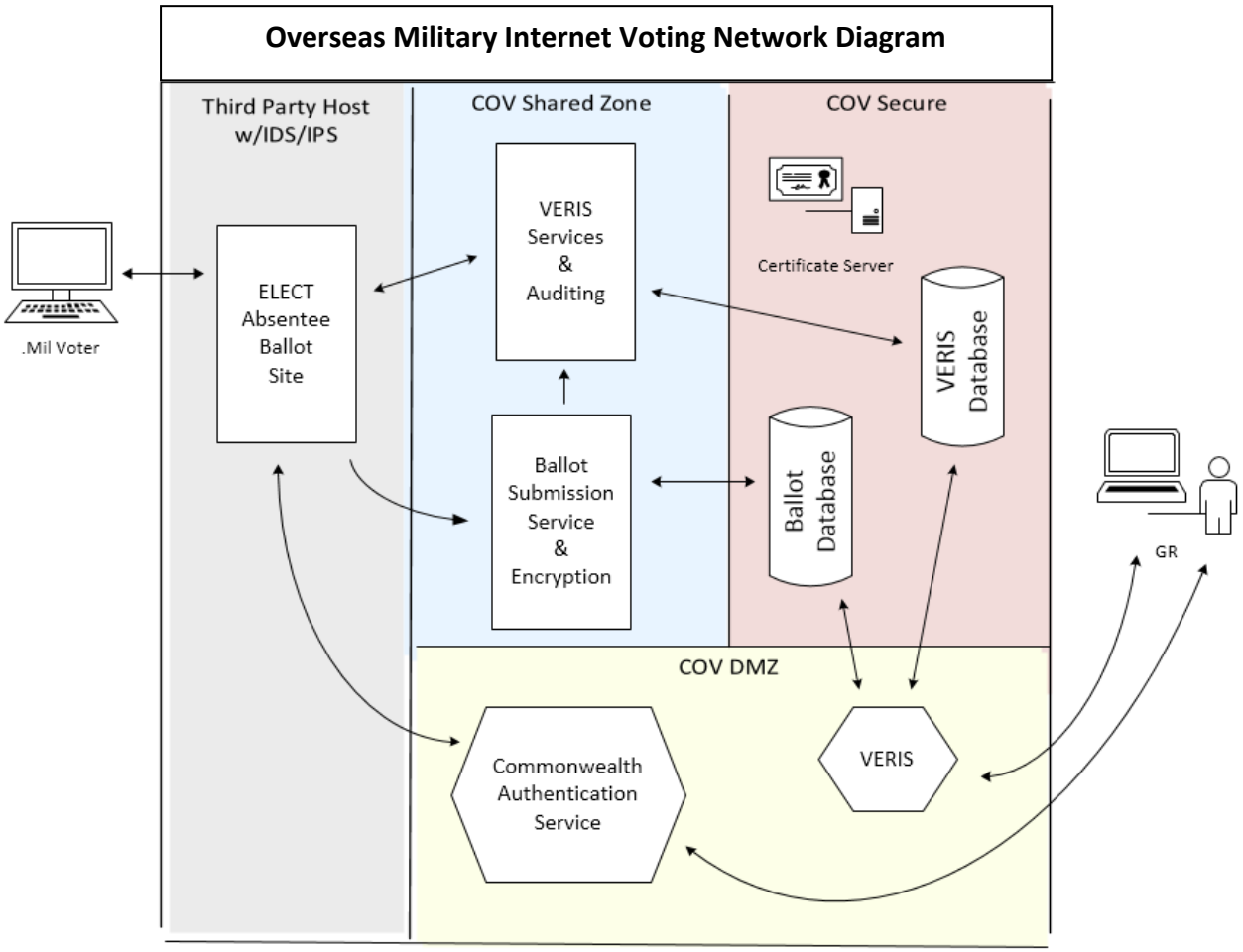
12) The local election official is given a single PDF document that contains all of the marked ballots for their locality.

13) The PDF is printed and given to the officers of election.

14) The officers of election hand count the marked ballots in the central absentee precinct according to currently established standards.

The following two charts provide visual representations of the walk through and a sample of how the network architecture would be built.




Overseas Military Internet Voting Network Diagram
Third Party Host w/IDS/IPS
COV Shared Zone
COV Secure
VERIS Services & Auditing
Certificate Server
VERIS Database
.Mil Voter
ELECT Absentee Ballot Site
Ballot Submission Service & Encryption
Ballot Database
GR
COV DMZ
Commonwealth Authentication Service
VERIS

Costs

In 2011, Virginia applied for and received a grant from the Department of Defense's Federal Voting Assistance Program (FVAP) to build and deploy an online ballot delivery portal for Virginia military voters. Under the terms of the grant, the use of this portal is not allowed in a system that includes the secure return of a marked ballot; therefore, Virginia will have to build a full new ballot delivery solution alongside the ballot submission system. It therefore makes sense to build a single solution that will deliver ballots and enable voters to submit ballots.

In early 2015, the Department of Elections issued a request for information to the vendor community to determine if there was a solution already in place that could be implemented in Virginia and to also determine what it might cost to deploy such a solution. Prices, licensing schemes, hosting requirements and functional requirements were all over the board. Implementation prices ranged from $50,000 to $1,900,000 and annual costs ranged from $50,000 to $1,150,000. When considering these proposals and the Department of Elections' experience with the FVAP grant project, an implementation budget of $1,400,000.00 for the development, deployment and associated training would be required along with an annual budget of $849,977.08 to stand up a solution in time for the 2017 November General Election.

1) Annual Costs: $849,977.08
    a. Annual hardware costs at FY16 VITA rates: $269,977.08
        i. Four production servers with disaster recovery and a total of 1.05 TB of disk space.
            1. $14,454.76/month
        ii. Three user acceptance testing servers with a total of 750 GB of disk space.
            1. $5,681.85/month
        iii. Two integration development servers with a total of 400 GB of disk space.
            1. $2,361.48/month

    b. Annual staffing (increase for ELECT of 2 MEL): $250,000.00
        i. One security engineer/architect: $130,000.00/year
        ii. One business analyst: $120,000.00/year

    c. Annual third-party security audit and penetration and vulnerability testing services: $60,000.00

    d. Solution licensing and support: $150,000.00
        i. The request for estimate yielded licensing costs of up to $1,000,000/year.

    e. Commonwealth Authentication Service: $120,000.00

2) One-Time Development Costs: $1,400,000.00
    a. This assumes that the solution is turned completely over to the Department of Elections and that no further licensing or support costs are required. This assumes the changes to VERIS can be done by existing staff. This does include independent security review and testing of the solution.
    b. This does not include the development of voting system standards or voting system certification.

In Fiscal Year 2017, the Department of Elections would spend $2,249,977.08 to stand up a solution. In the following fiscal years, the Department of Elections would spend $849,977.08 to keep the solution going. Assuming that the 2017

November General Election is the first election for which ballots are cast in this solution and assuming that we see an increase in participation by the overseas military voters (total of 2,000 voters estimated), the per voter cost for this solution would be $1,549.98. Each year after that, the cost would be $424.99 per voter.

Conclusion

The right to vote is at the core of our democracy and those men and women who are serving in uniform overseas deserve extra attention and assistance in exercising their right to vote. SB 11 required the State Board of Elections to provide a report on the feasibility and cost of deploying a solution that would both increase the number of applications for ballots and in increase the number of ballots returned in a timely manner for counting.

The solution provided for in this document will provide a way for our overseas service members to more quickly cast their ballot which should improve their rates of timely return of their ballots. Certainly cheaper alternatives could be provided however each alternative that was considered had risks that the workgroup was not willing to ask the General Assembly to accept. The proposed solution provided for in this document is the feasible solution that can be built which would also provide a high level of integrity in the voting process.

Most importantly however, in today's limited resources and significant cyber security threat, the General Assembly must weigh whether or not it is willing to accept the risks and costs of deploying a secure return of marked ballots solution for the members of the military who are deployed overseas.