Co-Chairs' Report Of The Military And Overseas Voting Assistance Task Force

(2013 Senate Bill 1)

Research Memorandum No. 516

Legislative Research Commission
Frankfort, Kentucky
lrc.ky.gov

August 2014

Co-Chairs' Report Of The Military And Overseas Voting Assistance Task Force

(2013 Senate Bill 1)

Legislative Members

Sen. Joe Bowen, Co-Chair
Rep. Darryl T. Owens, Co-Chair
Sen. Jimmy Higdon
Rep. Tanya Pullin

Citizen Members

Lindsay Hughes Thurston
Col. Charles T. Jones
James Fowler
Bobbie Holsclaw
Keith Cain

Legislative Research Commission Task Force Staff

Greg Woosley
Kris Shera

Research Memorandum No. 516

Legislative Research Commission
Frankfort, Kentucky
lrc.ky.gov

Paid for with state funds. Available in alternative format by request.

Foreword

The 2013 General Assembly passed Senate Bill 1 that established the Military and Overseas Voting Assistance Task Force to study issues relating to the process of absentee ballot voting for military personnel and overseas citizens. The task force also was directed to review the feasibility of using a secure electronic system for the return of voted ballots and the steps other states have taken to improve access to secure voting for this population.

The task force co-chairs would like to thank the task force members; all those who attended the meetings; and those who provided research, testimony, and input.

Marcia Ford Seiler
Acting Director

Legislative Research Commission
Frankfort, Kentucky
August 2014

Contents

Military and Overseas Voting Assistance Task Force

Summary

The Kentucky General Assembly established the Military and Overseas Voting Assistance (MOVA) Task Force in Senate Bill 1 enacted during the 2013 Regular Session. The task force was established to study the following topics: 1) the current time period for military and overseas voters to request and return absentee ballots; 2) the factors that limit the ability of these voters to cast an absentee ballot within the current time periods; 3) any procedures other states have adopted to facilitate more timely absentee ballot voting; and 4) the feasibility of military and overseas voters using a secure electronic transmission system to return voted absentee ballots electronically.

The nine-member task force began meeting in October 2013 and convened three times during the 2013 interim. Topics of discussion included current absentee voting procedures and changes enacted in Senate Bill 1, military perspectives on overseas absentee ballot voting, Kentucky's county clerks' perspectives on absentee ballot voting and Senate Bill 1, trends in absentee voting in other states, technology that can facilitate electronic absentee ballot voting, and security concerns with the expanded use of technology to cast absentee ballots electronically.

Current Absentee Voting Procedures And Senate Bill 1 Changes

An official from the Kentucky Secretary of State's office described the absentee ballot procedure for military and overseas citizen voting in Kentucky prior to the effective date of Senate Bill 1. A qualified voter, which includes residents of Kentucky who are members of the Armed Forces and their dependents, and citizens residing overseas, must complete an absentee ballot application by either using the state application or the federal post card application.

The timing of transmission, receipt, and return of absentee ballots for military and overseas civilians' voting is critical. A qualified voter may mail, email, or fax the absentee ballot application to his or her county clerk. The application must be received in the county clerk's office by the close of business no later than 7 days before the election to qualify for receiving an absentee ballot. After a county clerk reviews and approves the application, the blank ballot is then faxed, emailed, or mailed to the voter. If the application is received before the county clerk receives the printed ballots, the ballot must be sent within 3 days after receipt of the printed ballots. If the application is received after the county clerk receives the printed ballots, the ballot must be sent within 3 days after receipt of the application. In addition, if the application is submitted no later than 45 days before the election, the ballot must be transmitted by that date. After the voter receives the ballot, the voter marks his or her selections and must return the ballot by mail, which must be received by the time specified for closing the polls on the day of a primary, or a regular or special election.

The Secretary of State's office also presented statistics related to military and overseas ballots in some past election cycles. In the 2008 regular election, 6,565 military and overseas absentee ballots were issued. Of those, 5,236 ballots, or approximately 80 percent, were returned. Of these

totals, approximately 4,700 absentee ballots were sent to members of the military, and fewer than 3,600 (76 percent) were returned; whereas, nearly 90 percent of the ballots sent to overseas citizens were returned. In the 2010 regular election, 1,452 absentee ballots were issued, and 1,138 were returned – 82 of the returned ballots "were not counted, primarily because they were returned undeliverable or arrived after 6:00 p.m. on Election Day."[1] In the 2012 regular election, 4,608 absentee ballots were issued, and 3,601 (78 percent) were returned. Of those, 301 were unable to be counted, many because they arrived after the 6 p.m. deadline. Of those 301 uncounted votes, 191 (63 percent) were from military personnel and 110 (37 percent) were from overseas civilians.

By enacting SB 1, the General Assembly adopted a modified version of the Uniform Military and Overseas Voters Act, which has been adopted by 13 states and the District of Columbia as of January 2014. The bill requires the secretary of state to create an electronic transmission system by which a covered voter may apply for and receive voter registration materials and military overseas ballots. [1] The bill allows covered voters to register to vote or to update their voter registration information electronically. It extends the Uniformed and Overseas Citizens Absentee Voting Act protections, including to members of the Kentucky National Guard. It also establishes an electronic system for the submission and transmission of registration and absentee ballot applications and military and overseas ballots, which will ease the complications related to the timely transmission of voting materials to and from military and overseas voters. Also, under SB 1, covered voters may use the declaration accompanying a Federal Write-in Absentee Ballot to register to vote and to apply for an absentee ballot.

Military Perspectives On Overseas Voting

To understand how absentee ballot voting is implemented for military personnel serving overseas, the task force also heard testimony from several members of the Kentucky National Guard that had direct overseas voting experience.

The guard members explained that a voting assistance officer (VAO) is assigned to each unit to ensure that the deploying soldiers have all the necessary materials for requesting and casting ballots. The VAOs remind soldiers of upcoming elections and deadlines. However, even with a VAO assigned to each unit, it is up to each soldier to reach out to the county clerk's office for an absentee ballot and to follow through on the procedures required to vote, including mailing the voted ballot. A member who served as a VAO noted that he observed other states' VAOs that were able to assist their units in requesting and receiving ballots electronically, and in some circumstances to even cast a ballot electronically, which made the process much more efficient for the VAOs and their assigned units.

The guard members also detailed how the military uses a Common Access Card (CAC) for all electronic communication. These CACs are military-issued cards that are the only means for

[1] KRS 117A.010 defines "covered voter" to mean an individual who is registered or otherwise qualified to vote in Kentucky and is a member of the active or reserve components of the Army, Navy, Air Force, Marine Corps, or Coast Guard who is on active duty; a member of the Merchant Marine or the commissioned corps of the Public Health Service or National Oceanic and Atmospheric Administration; a member on activated status of the National Guard or state militia; or a spouse or dependent of one of those individuals; or a US citizen who is outside the US.

military personnel to access a computer. The cards are uniquely assigned to each soldier and contain their signatures. The cards could be used to allow secure access for voting. The CAC will work anywhere in the field that soldiers have an internet connection. The members noted that even advance units often have sufficient connectivity for at least limited computer access. They explained that training the soldiers to use the cards to facilitate voting would not be an issue and that the CACs could serve as a basis for secure, and verifiable, electronic voting.

The guard members testified that it was difficult for military personnel to adequately prepare for overseas absentee ballot voting before deploying overseas, and that any means of assisting the personnel once they are deployed increases the likelihood that they will be able to cast ballots successfully. Mail service overseas can be very unpredictable, and because mail is often delayed, the time constraints for casting ballots are difficult for personnel to meet. The guard members noted that having the time to negotiate the absentee ballot process, especially given the slow-moving nature of mail overseas, is one of the more serious issues for military personnel attempting to cast a ballot. The time constraints are further complicated because military personnel frequently change field locations, which can interfere with the success of sending or receiving mail and having mail forwarded to the personnel's current location. One member noted that because of the difficulties of sending, receiving, and forwarding mail, only 50 percent to 60 percent of his deployment team was able to execute an absentee ballot in the last election cycle.

The military members concluded by noting that while the military is adamant that deployed soldiers have the ability to vote, the largest issue impeding successful voting by overseas military personnel is the ability to get mail to and from members in their current locations in a timely manner. They noted that any effort to improve this process would likely increase the numbers of military personnel that are able to cast a vote successfully.

County Clerks' Perspectives On Absentee Ballots, Senate Bill 1, And Military And Overseas Voting Procedures

Representatives of the Kentucky County Clerks Association noted that county clerks uniformly support efforts to assist military and overseas voters with casting absentee ballots. However, the county clerks oppose the return of ballots electronically because of concerns regarding the security of the ballot and voter information. Further, the clerks stated that until there is certified security regarding the electronic return of a voted ballot, any electronic voting procedure currently in use does not comply with Section 147 of the Kentucky Constitution, which requires secret ballots for all elections by the people. This is the case because current electronic ballots can be intercepted and viewed by another party, potentially with no trace, and must be "opened" to be sure the ballot sent by a voter was actually received. By contrast, a paper absentee ballot comprises two envelopes: an outer envelope with the voter's identifying information and a sealed inner envelope containing the cast ballot, which is removed from the outer envelope and deposited into a ballot box without being examined. The use of the two envelopes provides more security from tampering or negating a secret ballot.

The clerks noted that there are still security issues, including information regularly being stolen and manipulated in electronic commerce, despite its longstanding use. In these circumstances, a mistake can usually be found and corrected rather quickly; however, a lost or compromised vote

may not be detected until after an election is certified, and in that case it is too late to remedy the problem without conducting a second election—an expensive proposition that would limit the certainty and finality of the election process. The county clerks are concerned with the secrecy and the accurate casting of ballots for military and overseas voters, and believe the risks are too great to endorse electronic voting.

The clerks stressed that civilians living overseas can request an absentee ballot online, and that the earlier a ballot is requested, the easier its return will be and the more likely that ballot will be returned on time and counted. The clerks also stated that there are no major concerns with the enacted version of Senate Bill 1, and they noted that the ability to transmit ballots electronically through the new secure system will also decrease the time required for a military or overseas voter to request, receive, and then ultimately return by mail a voted ballot.

Finally, the clerks explained that they were always looking for new ways to improve voting for all citizens, including military and overseas voters, but that their opinion was that the new provisions of Senate Bill 1 should be allowed to work in at least the 2014 elections before making any new commitments to additional changes.

Trends In Absentee Voting In Other States

Representatives from two elections software vendors, Everyone Counts, Inc. and SOE Software, provided an overview of technology used in other states for absentee voting and explained the benefits of using electronic systems for ballot delivery and return.

They noted that the first electronic ballot election was held in 1997. In 2003, the first government-wide electronic election was held, and in 2007, Australia used a system to allow all military serving overseas to use online voting. In modern electronic voting systems, a voter may use a computer, tablet, or smartphone to access a ballot regardless of location. These systems are not untested or unproven, but are not regularly deployed in the elections process in the United States. Statistics have shown that voter turnout and participation rates are higher when electronic delivery and return are used together, rather than separately. As an example, Alaska, Arizona, and Utah have either already used electronic return of ballots or will do so in the 2014 election cycle.

The vendors stated that the goal of ballot casting software that can facilitate the electronic return of a voted ballot is to minimize human errors, post office delays, and fraud. For example, Alaska has used electronic balloting for all voters, with on-screen marking of ballots possible, that includes safeguards to prevent inadvertent over voting and under voting. Additionally, electronic ballot systems are available that provide a paper trail, that are secure, and that are scalable to meet a state's elections needs. One of the vendors noted that it would soon be launching the first CAC authentication process for one of its client states.

As for the extent of current use, the vendors noted that approximately 20 states were using voting systems developed by their companies. They also stated that every state has electronic transmission of ballots from election officials to voters in some capacity, including fax and electronic mail; however, the return of ballots from voters to election officials is primarily by

standard mail in a majority of states. Additionally, several states have begun pilot programs to test electronic transmission of voted ballots from the voter to election officials in limited elections or for small groups of voters. For example, Alaska took small steps to introduce its electronic voting system, beginning first with Uniformed and Overseas Citizens Absentee Voting Act voters, and after its success, the state made the system available to all voters.

Utah's Approach To Military And Overseas Voting

An official with the Utah Lieutenant Governor's office said that Utah has 2.8 million residents in 29 counties. The state allows limited electronic voting that began with a pilot program approximately 15 years ago. Military and overseas citizens can apply for and return ballots by fax and email and have been permitted to do so for the last several election cycles. Almost all ballots sent electronically are returned successfully, and no significant issues have been reported.

In 1998, Utah began its pilot program to allow electronic voting, and initially a large number of ballots were returned by fax. By the 2012 election cycle, the numbers had dramatically switched, with two faxed ballot returns, 1,008 email ballot returns, and 1,307 regular mail ballot returns.

For the ballot to be sent to a voter and returned to the elections officials in a timely manner, the voter must request the ballot by the Thursday before the day of an election. Utah is able to do this because of the electronic means implemented to allow online voter registration and ballot retrieval. By sending a ballot electronically, the voter signs a form waiving the right to a secret ballot. The waiver is not required; however, if a voter chooses not to waive the right, the voter must send the ballot by mail to retain the right to a secret ballot.

Utah also works with the Department of Driver's Licenses to obtain residents' signatures when they apply for driver's licenses. Through this partnership, Utah has approximately 95 percent of its voters' signatures on file. When the voter receives a downloaded ballot, the voter signs, scans, and returns the ballot to a clerk's office; the clerk's first step is to check the signature against the one on file. The voter casting a ballot electronically is then "marked off" in the statewide voter database so that the voter cannot later submit a paper absentee ballot or vote at the polls.

After the signature is verified, the ballot is duplicated on to a second ballot that does not have any identifying information about the voter, and this second ballot is submitted for counting purposes. The original ballot is then locked away and stored and cannot be opened or examined unless ordered by a judge. The first cast ballot received from a voter, whether a paper ballot received by mail or an electronic ballot, is the one that is counted and recorded; no additional ballots are accepted. Utah's military and overseas balloting process was partially funded by a grant from the US Department of Defense's Federal Voting Assistance Program, which allowed Utah to establish an online ballot retrieval system. Although this system is not an online voting system, the online ballot retrieval system allows military and overseas voters to access a ballot online, and then mark, sign with an electronic signature, print, and return the ballot by regular mail, facsimile, or as an attachment to electronic mail.

According to the Utah official, over 80 percent of the voters who use the system are overseas, and over 90 percent of voters have reported they would use the system again. The biggest complaint heard by election officials from Utah voters is that the voters are not able to complete

the entire voting process online. Aside from this complaint, Utah's county clerks report that voters are happy with the modernized voting system.

As for the need for a secret ballot waiver, the official stated that when a ballot is emailed back to a county clerk's office, an election official must open the ballot and verify the voter's signature, which means an election official can see how the voter has voted. However, no more than two election officials are authorized to view the ballot, and because the emailed ballot is converted to a second ballot after the signature is verified, privacy concerns are minimized. Additionally, to date there has not been any incident where a signature has been duplicated or ballot secrecy compromised other than being seen by the two election officials who examine it.

The official noted that Utah needed a statutory amendment for its citizens to be permitted to waive their right to a secret ballot. He suggested that Kentucky might need to make a similar change to allow its voters to waive any ballot secrecy provisions.

Technology Used For Electronic Absentee Voting

The software vendors compared traditional mailed-in voted absentee ballots to electronically transmitted voted absentee ballots. The vendors noted that while technology is not perfect, the proper use of technology can improve election efficiency, security, and privacy. They also noted that the use of the CAC can increase the security of ballots for military voters.

The vendors stated that the key to electronic voting is security in the process used to transmit voted ballots. In this regard, ballot encryption is important, and a robust encryption process can result in greater security with electronic ballots than with standard glue-sealed mailed ballots. The use of electronic ballots also increases the accessibility of voting, particularly for military and overseas voters. Without specifying an amount, the vendors suggested that if sufficient funds are spent on good systems and processes, the use of electronic voting can be successful in delivering ballots on time, securely, and privately. The vendors noted that they have assisted several states and numerous countries in conducting elections with online voting or with using electronically transmitted ballots for the last several election cycles without any security issues reported. They stated that the deployed systems have passed all postelection audits conducted by elections officials. According to the vendors most, if not all, users have been pleased with the systems.

The vendors said their systems use a high level of encryption for ballot preparation, transmission, and authentication, and they are designed to resist denial-of-service attacks. Security protocols enable voters to securely communicate with elections officials in a way that is designed to prevent and detect any eavesdropping, tampering, or forgery; however, the system is also designed to allow voters the flexibility to use any HTML-compatible device. The vendors also demonstrated that there are numerous voter verification steps to be followed to submit a vote. Only after a ballot has been verified against the voter's information can it be successfully submitted.

One vendor noted that it has developed a new version of its system using the military's CAC. South Dakota has tested the system with hundreds of users in the state's National Guard and has

received positive feedback. The tested system reduced the turn-around time for military and overseas ballot requests and submissions to less than the average 60 days. The system used the CAC, which the military uses for all online access purposes and contains a digital signature. The system allowed a user to scan the barcode on the bottom of the card, which contains the user's information, and the election system would validate all of the information for the ballot and ensure that all of the required areas of the ballot were filled out accurately. If the information could not be validated, the system would alert the user and halt the electronic voting process. The voter would then be required to follow up with their election official to correct mismatched information or to return the absentee ballot by mail.

The vendors noted that several states and countries have implemented Internet voting in the last few election cycles, and that there have been slight security issues, such as unsuccessful denial-of-service attacks, which would be expected with any technology software. However, according to the vendors, there have been no detected security breaches and no evidence of voter fraud using the systems.

Security Concerns With Expanded Technology In Elections

Several computer scientists and other election security advocates expressed security concerns over expanded technology being used in elections.

Under the Help America Vote Act, the US Election Assistance Commission is responsible for establishing election system standards with the National Institute of Standards and Technology (NIST). After several years of study, NIST concluded that secure Internet voting is not currently feasible because malicious software on voters' personal computers could compromise the secrecy or integrity of electronically voted ballots. The study also concluded that Internet voting did not offer the same level of auditing that is available with in-person polling place systems because of the difficulty of validating software on remote voting system servers and voters' personal computers.[2] Additionally, the security advocates stated that with no standards for electronically cast ballots, any states that are experimenting with online voting are doing so with no solid foundation or recovery method if something goes wrong.

These advocates presented two major reasons why it is not advisable to cast online ballots: 1) the Department of Defense's Federal Voting Assistance Program does not endorse or fund Internet voting because of security concerns; and 2) there are no commercially available Internet voting systems that can prevent ballots from interception. It was suggested that states that are allowing Internet voting did so before it was understood how easy it was for ballots to be jeopardized.

In 2012, cyber attackers obtained Florida voters' identifying information and requested and obtained 2,500 absentee ballots by email. The FBI is still investigating, and no one has been caught. According to the security advocates, following the Florida breach, officials with the Federal Voting Assistance Program stated that there would be no federal funding for states to develop systems that allow Internet voting by military and overseas voters.

The security advocates cautioned that encryption is not foolproof and posited that private companies offering military-grade encryption have no clinical trials or public reviews to

substantiate their claims. The advocates suggested that before any Internet voting system is implemented, the vendors should have to demonstrate that their software is secure and should have public substantiation of their claims.

Many entities, public and private, are working to safeguard elections in the digital age. The security advocates stated that they support these efforts and the use of technology in elections where it can facilitate improvement without introducing unnecessary risks. Electronically sending blank ballots to voters or allowing voters to download and fill in a ballot before printing are options that use technology for voting purposes, but that present fewer risks to ballot security than transmitting voted ballots electronically. Extending time periods for receipt of ballots can also help more military and overseas voters receive ballots and return them in time to be counted. For example, California allows a 3-day grace period on standard mail voting, which has allowed 75 percent more votes to be counted.

The security community nearly universally agrees that online voting is one of the greatest challenges facing security professionals. The security experts generally are not opposed to electronic registration of voters or electronic delivery of ballots to voters; however, secure electronic return of ballots is one of the major challenges to ensuring the integrity of an election.

The security experts who testified described the three major types of fundamental attacks. One is a malware attack in which the actual device or machine a voter is using to vote is attacked. The second is a denial of service attack, which is designed to prevent people from voting or prevent votes from getting to their destination, which was used to disrupt elections in Canada in 2003 and Hong Kong in 2012. The last type is the penetration attack, where an attacker directly attacks the server that is collecting the ballots. As one example of how these attacks might work, an online voting system was deployed for a mock election in the District of Columbia and was subjected to tests to determine if the system was secure. Within 36 hours, the system was breached, all ballots were removed and replaced with other ballots, and the breach was not detected. The security experts did acknowledge that the D.C. system likely was not as sophisticated as the systems developed by the software vendors that appeared before the task force, but they stressed that there are no fundamental ways to prevent a similar penetration and manipulation of the elections process if electronic voting systems are used.

Recommendations

The task force concluded its study without making any specific recommendations to the General Assembly for additional legislative changes at this time. The co-chairs of the task force believe that it is appropriate to allow the changes enacted by Senate Bill 1 to be fully implemented for at least the 2014 election cycle, and possibly an additional statewide election cycle in 2015, to determine if additional changes are needed to assist military and overseas voters in casting absentee ballots. It is recommended that the General Assembly request information from the Secretary of State regarding implementation of Senate Bill 1 and how it impacts absentee ballot requests and returns, and the ultimate numbers of counted absentee ballots.

Endnotes

[1] Grimes, Alison Lundergan. "Military Matters: Protecting the Rights of Those Who Protect Us." June 3, 2013. Web; Office of the Kentucky Secretary of State.
[2] Hastings, Nelson, Rene Peralta, Stefan Popvenuic, and Andrew Regenscheid. "Security Considerations for Remote Electronic UOCAVA Voting." NISTIR Publication 7770. February 2011. Web. National Institute of Standards and Technology, US Dept. of Commerce.