National Election Defense Coalition

Testimony of National Election Defense Coalition
Susan Greenhalgh
Contact: segreenhalgh@gmail.com
917 796 8782
Montana State Senate
Senate State Administrative and Veterans' Affairs Commitee
Re: Voting Technology and Options for Disabled Electors
March 6, 2018

Thank you Chair Malek, Vice-chair Kary and members of the committee for the opportunity to testify before the State Administration and Veterans' Affairs Interim Committee on election security for assistive voting technology.

The National Election Defense Coalition (NEDC) is a national, non-partisan network of recognized experts in cybersecurity and elections administration, bipartisan policymakers, and concerned citizens and movement-builders committed to promoting policies to secure our elections. We are grateful and privileged to be able to share our expertise on election system security and welcome the opportunity to work together on this important issue.

The events of the 2016 election cycle have focused unprecedented levels of attention on the security of our voting systems. Leaders in the national Intelligence community have warned we should expect foreign adversaries to continue to try to attack our election systems. In January, CIA director Mike Pompeo warned "I have every expectation that they will continue to try."[1] We cannot overstate the gravity of the threat and how essential it is for lawmakers and election officials to protect our election infrastructure.

I vigorously commend the committee for its forethought to include election security when considering assistive voting systems and options for disabled voters. Accessibility and security are two absolutely essential elements for any voting system. It is important to consider both accessibility and security of the voting system from its inception. Too often accessibility features are added to an existing system, introducing interaction issues. Similarly security must also be built into the foundation of a system to ensure its effectiveness. Both of these elements must be baked into the system from the beginning to make sure that they do not compromise or conflict with each other. I welcome the opportunity to share with the committee important security requirements for your consideration as you explore assistive voting technology and I look forward to Michelle's discussion of critical considerations for voter accessibility.

[1] Duncan Geddes, "Russians will target US polls, CIA chief Mike Pompeo warns," *The Times,* Jan. 30, 2018

Fundamental Security Considerations –Paper ballots and post-election audits

There is a broad consensus among security and election experts that a voter-verified paper ballot is a critical and necessary security feature for any voting system - that is a paper ballot on which a voter marks her choices and is able to confirm and verify that the votes are marked correctly. A paper ballot provides a physical artifact of voter intent that is out of reach of a software bug, programming error or malicious attack. Coupled with post-election audits, paper ballots ensure security and resilience in an election system. Montana is already an exemplar of these best practices, using voter-marked paper ballots and post-election audits.

This means the paper ballot itself is an important security feature and that the ways the voter marks are recorded and verified are vital to the security of the system. I would like to discuss considerations for ballot marking to protect the security and resilience of the system when using assistive technology to allow voters to mark a paper ballot independently and privately.

Accessible Ballot Marking Devices

For some voters, marking a paper ballot privately and independently may require an assistive device. As discussed above, the ways that vote choices are recorded and verified are key security features of a voting system. When contemplating assistive technology for marking paper ballots there are also some important security and verifiability elements to consider.

1. The ballot marking device should render marks that are easily readable and verifiable by the voter and election workers for post-election audits and recounts.
   In order to conduct a meaningful post-election audit and recounts, it is critical that the audit be conducted by hand to eye examination of the vote choices on the paper ballot, as is the practice in Montana. In order for the audit to effectively provide a check on the computer-generated vote tally, the vote counts must be checked by a non-computerized tally, in other words, a manual count. This means that all ballots, including those marked by the assistive device, should render the vote choices in an easily readable form. Small, illegible text is not recommended. Moreover, the vote choice must be provided in human-readable text for the purposes of audits and recounts. Vendors are offering accessible ballot marking devices that do not mark a standard ballot. Instead these devices allow the voter to mark votes electronically on the device which stores the votes, then renders a ballot card with a summary of the voter's selections and a barcode. The barcode also reflects the voter's selections and can be used for scanning and tabulating votes. **The use of barcodes on paper ballots is inadvisable for several reasons**. The barcode introduces additional security vulnerabilities, it is not human-readable and must not be used for recounts and audits, and from most vendors it is proprietary- which means that the voter cannot use her own device to confirm the vote choices were correctly recorded in the barcode. (An exception is LA County, which is developing its own state-of-art ballot marking device which generates a standard QR code of the voter's selections that can be verified by the voter.)
   We recommend the legislature consider systems that do not provide a barcode or ask the vendor to disable the barcode feature.

2. Ballot Marking Devices that mark a standard ballot are preferable.

   From an auditability and privacy perspective, a ballot marking device that marks a standard ballot is preferable to a ballot marking device that prints a ballot summary card. Employing an assistive ballot marking device that marks a standard ballot ensures that voters that use assistive technology will not submit a ballot that is unlike the ballots marked without the device, which could compromise voter secrecy. Furthermore, devices that print only a vote summary introduce challenges to the verification process. The ballot summary only includes the choices the voter selected and does not include all candidate choices. This means the voter must recall all the candidates correctly to be able to confirm and verify her choices are correct.

Although the Automark is being discontinued, there are other devices that mark a standard ballot and I urge lawmakers and election officials to speak with the vendors and encourage them to offer devices that mark a standard ballot.
We recommend the legislature seek accessible ballot marking systems that mark a standard ballot.

3. Ballot Marking Devices should not receive or store identifying voter information.
Some ballot marking devices are activated to retrieve the correct ballot style for each voter through an activation card that is encoded with the voter's information in order for the ballot marking device to call up the correct ballot for the voter's residence. In order to protect voter secrecy the card and the ballot marking device should not receive any information that may identify the voter.
We recommend stipulating in contracts that the ballot marking device must NOT receive and/or store information that can identify the voter.

Remote Accessible Ballot Marking

There is growing interest in offering remote accessible ballot marking for absentee or vote-by-mail voters. This is an important and valuable use of technology to improve voter access. When contemplating the use of remote accessible ballot marking systems there are important principles and precautions jurisdictions can take to protect system security and voter privacy.

1. Remote Ballot Marking systems should not transmit vote information over the Internet.
There are many different remote accessible ballot marking systems on the market that are designed to allow a voter to accessibly mark her ballot from her home computer, print the ballot out and return it by mail. Administrators may assume that all these systems do not transmit vote choices over the internet because ultimately the ballot is printed on the voter's home computer but this is not always the case. Many of the systems currently available are designed so that the software that creates the ballot and retains the vote choices remains resident on a remote webserver, possibly at the vendor's location. This means that each time the voter makes a selection, that selection is transmitted over the internet to be temporarily stored. When the voter is finished, the remote server renders an image of the marked ballot which is again transmitted back over the Internet. These transmission introduce voter privacy issues and to a lesser degree, security issues. For these reasons the National Institute of Standards and Technology in its report "NIST IR 7711 Security Best Practices for the Electronic Transmission of UOCAVA Election Materials" made this recommendation:

> *"To protect ballot secrecy, the printable ballot should be constructed using software that runs solely on voters' computers. At no point should the ballot marking application transmit voter selections to the Web-server."*[2]

This recommendation was echoed in the Center for Civic Design's report "Principles and guidelines for remote ballot marking systems."

Concerns about the security and privacy vulnerabilities of remote ballot marking has led some states to legislate this best practice. In 2012 California passed AB 1929 which specifically prohibited the ballot marking system, or part of the system, from having the capability, including the optional capability, to use a remote server to mark the voter's selections transmitted to the server from the voter's computer via the Internet, store any voter identifiable selections on any remote server, or tabulate votes.[3]

There are multiple vendors that are offering systems which adhere to this very important best practice. These systems send the ballot data to the voter's computer and the ballot remains resident on the voter's computer throughout the marking and printing process.
We urge the legislature to require remote ballot marking systems must not transmit voter selections over the Internet.

I thank you very much for the opportunity to testify before the committee today and I welcome your questions and look forward to working with you in the future.

[2] NIST IR 7711 https://www.nist.gov/itl/draft-nistir-7711-security-best-practices-electronic-transmission-uocava-election-materials

[3] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201120120AB1929