



The Honorable Wayne W. Williams
Secretary of State
State of Colorado
Department of State
1700 Broadway
Suite 200
Denver, Colorado 80290

May 15, 2015

Dear Secretary Williams,

Thank you for the opportunity to provide initial comments to address proposed changes to Colorado's Rules Concerning Elections 8 CCR 1501-5. In the letter below we outline our concerns with the proposed regulations. While we do not, at this time, have alternative language, we would like to meet with you and other stakeholders to develop regulations that would best serve all Colorado voters, increase access to voting, and bolster voter confidence in the elections process. While technological advances can create greater access for all voters, we must be careful to balance our work of improving the voting experience for all Colorado voters without undermining the fundamental integrity of our democracy.

Specifically we wish to address the following amended rules:

Amendments to Rule 16.2.1(c), concerning electronic transmission

(c) In accordance with section 1-8.3-113(1), C.R.S., an elector who chooses to receive his or her unvoted ballot by online ballot delivery ELECTRONIC TRANSMISSION may return his or her ballot by fax or email ONLY IF THE ELECTOR DETERMINES THAT A MORE SECURE METHOD, SUCH AS RETURNING THE BALLOT BY MAIL, IS NOT AVAILABLE OR FEASIBLE. "NOT FEASIBLE" MEANS CIRCUMSTANCES WHERE THE ELECTOR BELIEVES THE TIMELY RETURN OF HIS OR HE BALLOT BY MAIL IS NOT CERTAIN.

The proposed rule could open online return of voted ballots to an entirely new class of voters – those who don't "believe" that postal mail – even expedited postal mail – will work in a timely fashion.

As just recently debated by the legislature, the current law explicitly restricted the electronic return of voted ballots to very limited circumstances because of the serious security issues that remain unresolved with the email or facsimile return of voted ballots. The proposed rule would controvert both the letter and the spirit of the statute as written, creating a new class of email voters.

When this measure was introduced both the Secretary of State's office and the legislators crafting the language expressed their intent to limit the circumstances in which the electronic return option may be offered because of the security issues.

When Director of Elections Bill Compton spoke in favor of the original bill enabling email voting for UOCAVA voters in 2006, he expressed grave concerns about the security and indicated that voting by email should be limited to those who did not have access to a fax machine. He stated in his remarks during the February 28, 2006 hearing on this legislation:

“[w]e do know we want to limit this. We do not want this to become the preferred method of voting. We want to limit it to those cases where there is **no other alternative** available to these people.”

The then Election Director went on to say “[the language chosen was intended to] include email in these very narrow circumstances. It was not meant to give any leeway to the Secretary on who—which groups—could be picked or chosen.”

The language proposed would likely expand electronic return of voted ballots to any voter who suspects his or her ballot may not be received on time. Undoubtedly this will open the door for voters to whom postal mail and expedited military express mail have been and are available and accessible, but who may not know of those options, and who suspect the ballot will not be received in a timely manner.

Since the passage of the Military and Overseas Empowerment Act (MOVE), ballots for federal elections must be made available to service members 45 days prior to Election Day. These unvoted ballots can be sent electronically. Colorado state law requires that overseas and military ballots be counted if they are received within eight days after the election, provided that they are postmarked by Election Day. This gives military and overseas voters 53 days to receive, mark and return a ballot by mail. The language and spirit of existing statute reflects that return of a ballot by mail is reasonable in all but the most extreme circumstances (such as voters that may be serving on a submarine or in a location that does not have regular access to mail). Most members of the military, even those serving in forward bases, do have access to regular mail service and also to expedited service made available through the military postal service.

The National Institute of Standards and Technology (NIST), the federal agency tasked by Congress to research remote electronic absentee voting for military voters, has found that the email and facsimile return of voted ballots **is extremely vulnerable to manipulation and tampering**. In the report NIST IR 7551, “A Threat Analysis of UOCAVA Voting Systems” NIST scientists warned:

“E-mails are significantly easier to intercept and modify in transit than other forms of communication. . . .It is unlikely that election officials would be able to identify ballots that had been modified in-transit.”¹

¹ <http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf>

We share the concerns of these security experts, and urge the Secretary to reconsider the rule to maintain its limited use rather than create greater leeway for the use of insecure return of ballots.

Amendments to Rule 20.5.2(f), concerning internal controls for the Voting System

(f) If any component of the voting system is equipped with Wi-Fi capability or a wireless device, the county must disable the wireless capability or device **UNLESS OTHERWISE APPROVED BY THE SECRETARY OF STATE.**

We oppose the changes to this rule. The current rules require Colorado counties to disable the wireless capability or device on any component of a voting system because it has been shown that wireless capability on a voting system exposes it to tampering or manipulation via remote connection. By way of example, the state of Virginia recently decertified its AVS WINvote voting systems after the Virginia Information Technology Agency (VITA) assessed the voting machines and found them vulnerable to attack through the wireless ports. VITA found that an attacker within a half a mile of a polling place could remotely connect to the voting machines, access the vote data, and change voted totals without leaving any evidence of the intrusion or vote manipulation.²

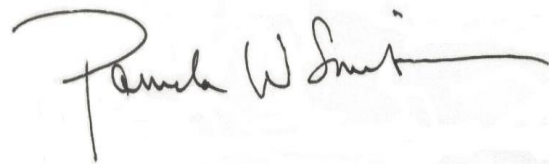
Wireless capability makes a voting system vulnerable and is not necessary for running voting equipment. Voting systems can and should be programmed with removable media to ensure security and integrity of the system. The proposed rule to permit wireless at the discretion of the Secretary of State undermines the integrity and security of Colorado's voting systems.

Thank you for the opportunity to comment on proposed changes to rules governing Colorado's elections. We believe we share the same goals. Voters should not face undue burdens when casting ballots in our elections, especially military and overseas voters. At the same time, our elections process should be a process in which the voters have confidence. Our elections should be fully auditable, verifiable, and re-countable. We look forward to working with you to accomplish these goals.

Very truly yours,

Elena Nunez

Pam Smith



Executive Director
Colorado Common Cause

President
Verified Voting

² <http://elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf>