



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

July 10, 2015

Dear Secretary Williams,

We are pleased to provide testimony and remarks regarding proposed rule changes to Colorado's Rules Concerning Elections 8 CCR 1501-5.

We appreciate the effort of your office to solicit preliminary comments from the public to inform the draft of the proposed rule changes and were happy to participate in the process.

We remain in opposition to Rule 16.2.1(c). However, before addressing Rule 16.2.1(c), we would first like to address proposed new Rule 16.2.8 prohibiting Internet voting because it is inextricably linked to proposed Rule 16.2.1(c).

Public comments voiced significant objection to Internet voting. The Secretary has proposed Rule 16.2.8 which states:

New Rule 16.2.8:

16.2.8 NOTHING IN THIS RULE 16.2 PERMITS INTERNET VOTING. INTERNET VOTING MEANS A SYSTEM THAT INCLUDES REMOTE ACCESS, A VOTE THAT IS CAST DIRECTLY INTO A CENTRAL VOTE SERVER THAT TALLIES THE VOTES, AND DOES NOT REQUIRE THE SUPERVISION OF ELECTION OFFICIALS.

Proposed new Rule 16.2.8 unfortunately fails to recognize that email and fax return of voted ballots (permitted and expanded in Rule 16.2.1(c)) *is* Internet voting and includes all of the inherent security risk of Internet voting. In fact, email (and digital fax) are considered by voting system experts at both the National Institute of Standards and Technology and the U.S. Election

Assistance Commission to be *even less secure*^{1, 2} than the type of Internet voting system described in proposed Rule 16.2.8.

The term “Internet voting” is correctly recognized by election authorities to include any electronic transmission of a voted ballot or vote choices over the Internet. In its 2011 report, “A Survey of Internet Voting” the U.S. Election Assistance Commission described Internet voting as:

“...any system where the voter’s ballot selections are transmitted over the Internet from a location other than a polling place to the entity conducting the election.[...] There are two forms in which the voter’s ballot selections can be returned: electronic ballot return, where the entire ballot document, including the voter’s selections, is transmitted; or vote data return, where only the voter’s selections are transmitted.”

The report goes on to identify three different methods of electronic ballot return, all three of which are identified as Internet voting.

“There are three channels, or methods, for electronic ballot return:

- a web-based communications application which uploads a digital representation of a voted ballot (e.g., pdf, jpeg, png) file to a website;*
- digital facsimile, where a voted ballot is scanned and transmitted as a graphics file; and*
- email, where a digital representation (e.g., pdf, jpeg, png) of a voted ballot is transmitted via email.”*³

We acknowledge with appreciation your intent to answer the legitimate concern of the public about Internet voting. However, we are compelled to stress that email and fax return of voted ballots is considered Internet voting by election authorities because email and fax return of voted ballots possess the same security risks of Internet voting that spurred the public’s objections. When any document is sent by email, including a marked ballot, it is easily subject to interception, manipulation and deletion. The financial services industry routinely advises clients NOT to send sensitive information like social security numbers or account numbers over email. Certainly the marked ballots of our troops are as important as social security numbers. They too should not be sent over the Internet.

We appreciate the Secretary’s personal commitment to helping overseas and military voters participate in elections. Unfortunately, it is so easy to intercept and undetectably alter email

¹ “E-mails are significantly easier to intercept and modify in transit than other forms of communication.” NIST IR 7551 A Threat Analysis of UOCAVA Voting Systems <http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf>

² “Email is about the least secure method of ballot delivery,” Brian Hancock The Canvass - “Internet voting, not ready for prime-time?” Feb 2013 http://www.ncsl.org/Portals/1/Documents/legismgt/elect/Canvass_Feb_2013_no_37.pdf

³ <http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf>

ballots that it does our service men and women a disservice to imply that their ballots will arrive safe and intact if sent over the Internet.

In a report released in 2014, the Federal Voting Assistance Program (FVAP), an agency administered by the Department of Defense to fulfill the mandate of the Uniformed and Overseas Citizens' Absentee Voting Act (UOCAVA), recognized the security risks inherent to any and all methods of electronic return of voted ballots:

“Due to unresolved security concerns regarding the electronic return of voted ballots, FVAP purposefully designed the [Electronic Voting Support Wizard] project to refrain from considering that aspect and remain in alignment with previous efforts without injecting concerns over security over the use of the internet. Electronic delivery of a blank ballot, when combined with the postal return of the voted ballot, remains the most responsible method for moving forward until such time applicable Federal security guidelines are adopted by the EAC.”⁴

The definition of Internet voting in proposed rule 16.2.8 is incomplete and misleading. We recommend deleting proposed rule 16.2.8.

PROPOSED RULE 16.2.1(c)

We object to the proposed rule 16.2.1(c) for the same reasons previously offered, and propose alternate language below.

In the Secretary's response to comments on draft rules, the Secretary rejected comments similar to our comments, writing:

“No change. The legislative intent comment appears to reference a prior version of the statute. The revised statute requires the Secretary of State to define “not feasible.” The proposed rule defines the term in a manner that leaves the determination with the military or overseas voter who is best equipped to assess his or her specific situation.”

The revised statute as passed in 2011 says:

“1-8.3-113. Transmission and receipt of ballot. (1) A covered voter who requested and received ballot materials by electronic transmission **may also return the ballot by electronic transmission:**

(a) In circumstances where another more secure method, such as returning the ballot by mail, is not available or feasible, as specified in rules promulgated by the secretary of state; or”

The legislative history from the House State Affairs Committee hearing on February 24, 2011 and the State Senate Affair hearing on April 18, 2011 clearly demonstrates a consensus among the lawmakers that the intent of the bill language was to strictly limit electronic ballot return to

⁴ “2010 Electronic Voting Support Wizard (EVSU) Technology Pilot Program Report to Congress”
http://www.fvap.gov/uploads/FVAP/Reports/evsw_report.pdf

extreme circumstances because of the security risks. The legislation directs the Secretary to promulgate rules on that order, pursuant to that intent.

The rule proposed by the Secretary instead, as stated clearly in the response to comments, is designed not to provide rules that define limited circumstances in which an elector may return a ballot electronically, but to allow the elector to determine if he or she would prefer to return a ballot electronically. The rule also fails to provide appropriate guidance to the voter as intended by the legislature. The legislation directed the Secretary to create the rules to enforce a limitation on electronic ballot return because of security issues. We propose alternate language we believe aligns more closely with the legislators' intent:

(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 A MORE SECURE METHOD, SUCH AS RETURNING THE BALLOT BY MAIL, IS NOT AVAILABLE OR FEASIBLE BECAUSE THE ELECTOR DOES NOT HAVE ACCESS TO POSTAL SERVICE THAT WILL ALLOW THE ELECTOR TO RETURN HIS OR HER BALLOT BY THE DEADLINE FOR BALLOT RECEIPT. THE ELECTOR MUST SIGN AN AFFIDAVIT ATTESTING TO THESE CIRCUMSTANCES. VOTERS SHOULD BE INSTRUCTED THAT ELECTRONIC RETURN OF VOTED BALLOTS IS THE LEAST SECURE METHOD AVAILABLE AND THAT BALLOTS SENT BY MAIL WILL BE COUNTED IF RECEIVED UP TO EIGHT DAYS AFTER ELECTION DAY.

PROPOSED RULE 20.9.1(c) and REPEAL OF RULE 6.5

We oppose amendments to Rules 6.5 and 20.9.1(c), concerning the requirements for background checks and the transportation of equipment, memory cards, ballot boxes, and ballots:

20.9.1(c) Transportation by contract. If a county contracts for the delivery of equipment to remote voting locations, each individual delivering equipment must successfully pass ~~the~~ A criminal background check ~~described in Rule 6.5~~. Any person who has been convicted of an election offense or an offense with an element of fraud is prohibited from handling or delivering voting equipment. Two election officials must verify, sign, and date the chain-of-custody log upon release of the equipment to the individual(s) delivering the equipment.

We oppose this rule change because it would strip out the requirements for the "criminal background check" to be conducted in accordance with the stipulations in rule 6.5 which states -

*6.5 The county clerk must arrange for a criminal background check on a supervisor judge and each staff member conducting voter registration activities. (a) The criminal background check must be conducted **by or through the Colorado Bureau of Investigation, the county sheriff's department in accordance with section 24-72-305.6(3), C.R.S., or similar state or federal agency.** (b) A person convicted of an election offense or an offense containing an element of fraud may not: (1) Handle voter registration applications or conduct voter registration and list maintenance activities; or (2) Have access to a code, combination, password, or encryption key for the voting equipment, ballot storage area, counting room, or tabulation workstation.*

This is a very important rule that should not be altered. The proposed change would allow individuals to handle critical, vulnerable election data, without oversight, during transport by passing a "background check" of undefined terms and parameters and without defining the qualifications of the entity doing the

background check. This opens the door for the county to accept *any* sort of review of an election worker as a "background check." Furthermore, vendors contracting with the county may assert that their employees have undergone a "background check" of unknown rigor or quality, enabling those employees to handle crucial vote data. This will acutely undermine the security and integrity of Colorado's elections by severely weakening the chain of custody procedures currently in place.

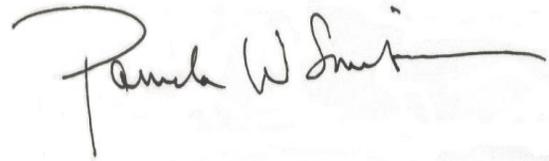
Very truly yours,

Elena Nunez

A handwritten signature in black ink, appearing to be 'E Nunez', with a long horizontal flourish extending to the right.

Executive Director
Colorado Common Cause

Pamela Smith

A handwritten signature in black ink that reads 'Pamela W Smith' in a cursive style, followed by a horizontal line.

President
Verified Voting