SUGGESTIONS FOR ELECTION RULE CHANGES

From:
Margit Johansson
[redacted]

August 21, 2014

1. UOCAVA VOTERS SHOULD NOT RETURN VOTED BALLOTS ELECTRONICALLY

To date, Election Rules have not adequately supported the content of CRS 1-8.3-113(1).

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

Currently, there is no Rule to support the legal requirement to AVOID returning a voted ballot electronically when a more secure method is available or feasible. Yet this proviso is crucial to maximizing the chances for secure elections.

The facts are overwhelming that the current Internet cannot be made entirely secure, and that the use of electronics for returning voted ballots is unnecessarily risky. (A recent permitted hack by prominent computer security experts in a mock election for Estonia is another stunning example of the vulnerability of Internet voting. For a report and video, visit estoniaevoting.org.)

The present state law allows return of voted ballots by email or fax, as if this were an acceptable level of risk. In fact, this use of email or fax (which currently often uses email as part of the faxing process) is very insecure.

CRS 1-8.3-113 was passed in 2011, two years after additions to a federal law for military and overseas voters known as the MOVE Act made use of mail returns of voted ballots the better choice. The Act required election officials to send blank ballots to remote voters at least 45 days in advance of a Federal election; it also allowed sending blank ballots to voters electronically. It also provides free expedited mail service for voted ballots of overseas uniformed service voters. (The MOVE Act did not provide for electronic returns of voted ballots, with good reason.) Given the changes in the MOVE Act, CRS 1-8.3-113 should not have been passed.

Intended to replace 16.2.1 (c) and (d), here is a Rule suggested to address the current absence of protection for UOCAVA voted ballots in Rules:

"To minimize security risks associated with use of the Internet, voted ballots must only be returned by postal mail or Federal Express, and NOT by email or other electronic means. Any electors whose blank ballots are sent to them later than 45 days before an election may select the option to be reimbursed for the expense of an expedited or Fed Ex return."

2. ONLINE VOTER REGISTRATION ADDRESS CHANGES FOR SHOULD NOT BE MADE WITHOUT A NONRETURNABLE POSTCARD SENT TO THE PREVIOUS ADDRESS AS A CHECK AGAINST FRAUDULENT CHANGES.

SB14-161 eliminates the requirement in **CRS 1-2-202.5. On-line voter registration – on-line changes in elector information.** (7)(b) for sending a nonforwardable postcard to an elector's old address in the event of an on-line registration address change.

Online election procedures, including online registration, are very vulnerable to fraud. A nonforwardable postcard sent to an elector's old address is a check on whether an online address change was legitimate.

The removal of the nonforwardable postcard sends an all-clear signal to those who want to submit false change of address requests.

We suggest that you restore this protection in a Rule, using language similar to that deleted from CRS 1-2-202.5.

This deletion accomplished in SB14-161 signals an abdication of the Legislature of its state Constitutional duty to work to safeguard the purity of elections. The voters still have a chance to have their right to clean elections enforced if the Secretary would honor *his* duty "to secure the purity of elections and to guard against the abuses of the elective franchise" through Rules, as stated in CRS 1-1-107(2)(a) and (5).

<u>Justifications for such a Rule:</u>

1. Below is a relevant discussion by computer security expert Dr. Barbara Simons. Dr. Simons' remarks precede her citing an article in Wired magazine:

> "I believe this article has obvious connections to internet voting and online voter registration. With internet voting, not only can ballot secrecy be compromised, but a man-in-the-middle attack can, as observed in the last paragraph below, be used to modify the ballot without the voter's knowledge.
> With voter registration the risk is that a voter's address could be modified, again without the voter's knowledge. This could be a serious problem in states that are

primarily or exclusively vote-by-mail. But it could also be a problem if voters find on Election Day that they are listed at a different physical location from the one they expect. The article demonstrates that election officials need to have procedures in place to deal with the risk that online address changes could be compromised. An obvious response to an address change is to mail paper confirmation to both the old and the new addresses.Regards,
Barbara
---------- Forwarded message ----------
Someone's Been Siphoning Data Through a Huge Security Hole in the Internet
By KIM ZETTER
12.05.13
<http://www.wired.com/threatlevel/2013/12/bgp-hijacking-belarus-iceland/>"
(*Permission to quote Dr. Simons granted.)*

2. Anyone who knows the NAME, DATE OF BIRTH, AND DRIVER'S LICENSE NUMBER of a Colorado citizen registered to vote can make an anonymous ONLINE change to this eligible voter's permanent address or the address where a ballot is to be received. Not even an ostensible elector's signature is needed --- only a check that there is a signature on file with the Department of Motor Vehicles!

(With only a name, birthdate, and signature, someone can submit a voter's address change by mail or email of a scanned paper copy. We understand signatures can be forged fairly easily, given the resources.)

3. See the article cited below by NBC News a year ago when large-scale hacking of mail ballot requests was uncovered in Miami-Dade County; **in the article, election experts mention the vulnerabilities of online registration**. Later in the article a computer scientist describes how he demonstrated to the FBI that he was able to access an online address change form by figuring out driver's license numbers in two states:
http://openchannel.nbcnews.com/_news/2013/03/18/17314818-cyberattack-on-florida-election-is-first-known-case-in-us-experts-say?lite?ocid=twitter.

(An alternative to a Rule would be for the Secretary of State to assume the task of sending out nonforwardable postcards after an online address change.)