Andrea Gyger

From: Al Kolwicz [redacted]
Sent: Tuesday, July 14, 2015 4:53 PM
To: Wayne Williams
Cc: Colorado Voter Group (ColoradoVoter@googlegroups.com); Charles L. Heatherly [redacted]; Steve House ; Laura Woods; Senator Lundberg (senatorlundberg@gmail.com); Kent Lambert (senatorlambert@comcast.net); Suzanne Staiert
Subject: COMMENT on Election Rules – 8 CCR 1505-1

July 14, 2015

VIA EMAIL

The Honorable Wayne Williams, Secretary of State
Colorado Department of State
1700 Broadway
Denver, CO 80290
SOS.Rulemaking@sos.state.co.us

Re: Election Rules – 8 CCR 1505-1

Dear Secretary Williams:

A. The rule contains a serious flaw. 16.1.8 (c) permits a voter to return his or her ballot by fax or email.

- For purposes of canvassing, it is necessary to include a specification defining at what point the ballot is considered "cast". In our opinion, the ballot is cast when the voter relinquishes custody of the voted ballot, i.e., when the voter "presses" send.
- For purposes of canvassing, it is necessary to have a count of the number of ballots cast.

B. The rule continues to treat fax and email voting frivolously.

- It is well understood by computer and systems professionals that transmission of voted ballots by fax or email is open to undetected manipulation of the ballot box by changing, deleting, and injecting voted ballots. Such manipulation disenfranchises voters. You and your Department personnel are well-advised to respect the facts that have been well documented by the experts, and reject the reckless optimism of those who will not be held accountable for any future fiasco. See:

  The Dangers of Internet Voting
  http://www.heritage.org/research/reports/2015/07/the-dangers-of-internet-voting
  by Hans A. von Spakovsky
  Backgrounder #3034
  July 14, 2015

  Those who believe that it is "possible given current technology" to create a secure online voting system are dangerously mistaken. According to computer experts, Internet voting is vulnerable to cyber-attack and fraud—vulnerabilities inherent in current hardware and software, as well as the basic manner in which the Internet is organized—and it is unlikely that these vulnerabilities will be eliminated in the near future. Internet voting, or even the delivery by e-mail of voted ballots from registered voters, would be vulnerable to a variety of well-known cyber-attacks, any of which could be catastrophic. Such attacks could even be launched by an enemy agency beyond the reach of U.S. law and could cause

significant voter disenfranchisement, privacy violations, vote buying and selling, and vote switching. The biggest danger, however, is that such attacks could be completely undetected.

- The rule must be tightened to specify, detect, and prevent any abuse of fax or email voting. At present, the language is not precise and could not be enforced. It cannot even be uniformly implemented.

C. In this third paragraph we place on the record the fact that you personally, as well as the Department have been NOTIFIED that by implementing these vague and unenforceable fax and email voting rules, an opportunity for massive disenfranchisement of voters is being created. Now is the time to prevent this from happening. And you are the person responsible for doing so.

Al Kolwicz
[redacted]