ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

April 22, 2015

The Honorable Secretary of State Williams
Colorado Department of State
1700 Broadway, Suite 200
Denver, CO 80290

Dear Secretary Williams:

We have received a copy of the letter you sent to Representatives Ryden and Nordberg and Senators Hill and Garcia regarding amendments to HB-1130. We thank you for your leadership in doing everything in your power to make sure all military and overseas voters get a chance to cast a ballot.

We are concerned however about your opposition to L.036 which would prohibit online ballot marking. Your comments regarding scanning and emailing back a marked ballot sends the wrong message and we worry that you may have been given technically faulty advice. In your letter you state:

> *"The state uses an innovative application from Everyone Counts that allows UOCAVA voters to specifically access their ballot online, mark it and print it out to verify their selections. The concern that the system is hackable is a nonstarter because the voter must still print it, sign it, scan it, and send it back to the clerk's office."*

While it is true that the voter may verify the printed ballot BEFORE they digitize it for transmittal – thereby observing any unintended alterations that may have occurred to the human readable part of the ballot while they were marking it online – AFTER they convert the printed ballot to a digital file for sending, it is entirely unsecured and may be subject to modification in transit over the Internet. Contrary to your implication that the system is unhackable, there is still opportunity for even a relatively unsophisticated hacker to change the voter's choices.

Marked, scanned ballots sent as email attachments are susceptible to being modified in *bulk*, by an *automated* attack program while in transit, by anyone with privileged network access. That includes the voter's ISP, network backbone operators, the Secretary of State's ISP, and even unrelated ISPs (via a technique known as IP hijacking or route hijacking)[1]. The security problem this creates is less detectable than just about any other kind of online voting attack. A ballot sent by email is relayed several times between sender and receiver. At any relay point, or even before it leaves the voter's computer, an attacker could insert a malicious program designed to recognize and filter emails containing ballots, and block, replace, or modify them. Of special note for overseas

[1] See, e.g., "
Repeated attacks hijack huge chunks of Internet traffic, researchers warn", Ars Technica. http://arstechnica.com/security/2013/11/repeated-attacks-hijack-huge-chunks-of-internet-traffic-researchers-warn/

military voters, any ISP over which the email travels, possibly including ISPs owned or controlled by foreign governments, would be able to silently and undetectably modify all the votes that traverse their network.

In the report "NIST IR 7551 A Threat Analysis on UOCAVA Voting systems," the National Institute of Standards and Technology detailed the vulnerabilities of sending voted ballots by email.[2]

It is critical to consider that in the system you propose, voters must send a digital version of the ballot back via email. Prior to uploading, during transit, and during downloading there are many avenues that an attacker could take to alter the contents of the ballot so that the voters' choices are not recorded; the hacker's choices are. Further,

1) The voter can't verify the QR codes – they are not human readable. When the ballot is marked online, a QR code containing the voters' choices is generated. Because the marking occurs online, on a remote server, there is ample opportunity for mischief or error. The QR code that was generated may have been manipulated on the server or en route– even as the voter's human readable choices remain the voters' actual choices. Since the QR code is used for generating a new paper ballot, it's possible that erroneous or modified choices will be recorded, not the voter's. Finally,

2) Undetected manipulation at the receiving end via an infected file or through other means could occur. This could even result in damage at the election official's server.

We understand that you are doing everything in your power to make sure military and overseas voters are well served. We don't believe that exposing military ballots to hackers – who can reside anywhere in the world far from the reach of U.S. law – will ultimately serve them or our country.

Respectfully,

/s/ Nate Cardozo
Nate Cardozo
Staff Attorney

[2] NIST IR 7551 "A Threat Analysis on UOCAVA Voting Systems,"
http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf
"E-mails are significantly easier to intercept and modify in transit than other forms of communication. E-mails travel through telecommunications lines, network equipment and e-mail servers before reaching the intended recipient. Anyone with access to the infrastructure could read or even modify e-mail messages. In particular, e-mail servers often store messages for a short period of time before passing them on to the next server, or the intended recipient. System operators for these servers could intercept or modify e-mailed ballots. It is unlikely that election officials would be able to identify ballots that had been modified in-transit."