April 25, 2011

Policy Brief 2011-04.1

We respectfully ask you to defend election integrity by preferably voting down HB11-1219 in its entirety. If the bill is to be passed, two amendments offered here reduce the bill's negative impacts.

As currently drafted without our amendments, HB11-1219 allows so many people to vote insecurely via the Internet that election integrity for Colorado becomes much less likely. There are other problems with definitions and specific wording that indicate a rethinking of the bill and reconsideration in the 2012 session would be the best course.

However, in the event that haste is deemed to be required, the Board of Directors of Coloradans for Voting Integrity herein submits two amendments that will strengthen HB11-1219.

This CFVI Policy Brief gives the rationale behind the amendments. On the back page of this document, Appendix E presents suggested language for the needed amendments.

Thank you for your attention and your service to all Coloradans.

Sincerely,

Margit Johansson, Board Member
For the Board
Coloradans for Voting Integrity (CFVI)
(303) 442-1668

Coloradans for Voting Integrity is a collection of concerned Colorado citizens dedicated to fair, accessible, and verifiable and verified voting on the state and national level.

Contact Coloradans for Voting Integrity at www.cfvi.us, richey80304@yahoo.com, (970) 963-1369, or 3938 Wonderland Hill Avenue, Boulder, CO 80304.

April 22, 2011

Dear Colorado Senators,

In the past, overseas U.S. citizens have had problems voting from abroad. Recently, significant efforts have been made to overcome the difficulties of this "distance voting" for absent uniformed service personnel and overseas civilians, and much progress has been made in this regard.

Still, distance voting is always less secure than voting done with paper ballots and proper procedures in local polling places. So efforts to ensure successful voting from outside one's state, and especially from abroad, have required assuring the timely delivery of voted ballots, while minimizing the insecurities of distance voting methods.

Colorado HB11-1219, Concerning the "Uniform Military and Overseas Voter Act," currently unnecessarily permits the return of voted ballots by insecure use of the Internet and traditional fax. It also greatly enlarges the categories of voters who could use these insecure voting methods. Both these features could jeopardize the integrity of elections in which these voters participate.

We offer Colorado Senators two amendments (possible legislative language given in Appendix E at the end of this document) to address the problems in HB11-1219.

<u>AMENDMENT #1</u>: TO PROHIBIT THE ELECTRONIC TRANSMISSION OF VOTED BALLOTS.

HB11-1219 deviates from its parent Uniform Law Commission (ULC) bill "Uniform Military and Overseas Voters Act" (UMOVA) by allowing electronic[1] transmission of voted ballots under certain circumstances. The model Uniform Bill, on the other hand, avoids any electronic transmission of voted ballots because of security and identity risks. HB11-1219 should follow the lead of the ULC bill for several reasons:

- Voted ballots transmitted electronically via the present Internet cannot be made secure from hacking, as eminent computer security experts warn in Appendix A.
- Interested parties such as vendors overstate the promise of techniques such as encryption to secure Internet voting. Claiming that we have the tools to make Internet voting secure doesn't make it so. We cannot allow misinformation to permit insecure voting methods such as returning voted ballots using electronic transmission. In Appendix B, a world-class encryption expert describes what encryption, for example, can and cannot do. And our current law on allowing a pilot project on Internet voting in 2012 (CRS 2010: 1-5.5-101) promises the impossible.

1"Electronic" includes use of facsimile (which now often utilizes the Internet for transmission), email, and other forms of Internet voting.

- Major steps are already legislated to ensure that absent military personnel and overseas civilians are able to successfully vote, while not unduly imperiling voted ballots. These steps are described in Appendix C.
- Hacking happens. Hacking of time-sensitive elections could be devastating. Internet voting could be a gold mine for vendors or ruthless political operatives, and toxic to our democracy. Appendix D gives recent examples of hacking, general and election-related.
- Changes in HB1219 needed to implement this amendment are given in Appendix E.

<u>AMENDMENT #2:</u> "COVERED VOTERS" SHOULD INCLUDE ONLY <u>ABSENT</u> UNIFORMED SERVICE PERSONNEL. <u>ABSENT</u> PERSONNEL ARE THOSE NOT RESIDING IN THE U.S. STATE WHERE THEY ARE REGISTERED TO VOTE.

- Delete 1-8.3-102(2)(a) and reletter the following sections (b) through (e) accordingly to (a) through (d).
- Military service voters living in their home state do not require the special voting provisions offered the military voting from abroad. "Absent" military voters who are out of their state—but within the United States—during an election may perhaps need special voting privileges, although we have not read documented evidence of this.
- The ULC's Uniform Bill (UMOVA) was originally titled a "Military Services and Overseas Civilian *Absentee* Voters Act" (italics added). The expansion to cover non-absent military voters was proposed late in the bill's drafting and necessitated a title change, whereby the word "absentee" was removed, to the current "Uniform Military and Overseas Voters Act (UMOVA)."
- Inclusion of non-absent military as "covered voters" could cause considerable confusion for election officials, making their jobs more difficult than they already are.
- This expansion of covered voters could subject many more military voters to the insecurity of Internet voting.
- Expanding the numbers of voters—not JUST non-absent military personnel, but also more categories of overseas civilians—able to return their marked ballots by electronic transmission may allow an election's outcome to be dishonestly changed.

APPENDIX A

EXPERTS SPEAK OUT ON THE INSECURITY OF THE INTERNET FOR VOTING

1. **A computer security expert relates a recent hack by "spear phishing" to risks of Internet voting.** (http://www.freedom-to-tinker.com/blog/jeremyepstein/oak-ridge-spear-phishing-and-i-voting)

Oak Ridge, spear phishing, and i-voting

By Jeremy Epstein

Posted on April 20th, 2011, at 9:56 a.m., on "Freedom to Tinker"

Oak Ridge National Labs (one of the US national energy labs, along with Sandia, Livermore, Los Alamos, etc) had a bunch of people fall for a spear phishing attack (see articles in Computerworld and many other descriptions). For those not familiar with the term, spear phishing is sending targeted emails at specific recipients, designed to have them do an action (e.g., click on a link) that will install some form of software (e.g., to allow stealing information from their computers). This is distinct from spam, where the goal is primarily to get you to purchase pharmaceuticals, or maybe install software, but in any case is widespread and not targeted at particular victims. Spear phishing is the same technique used in the Google Aurora (and related) cases last year, the RSA case earlier this year, Epsilon a few weeks ago, and doubtless many others that we haven't heard about. Targets of spear phishing might be particular people within an organization (e.g., executives, or people on a particular project).

In this posting, I'm going to connect this attack to Internet voting (i-voting), by which I mean casting a ballot from the comfort of your home using your personal computer (i.e., not a dedicated machine in a precinct or government office). My contention is that in addition to all the other risks of i-voting, one of the problems is that people will click links targeted at them by political parties, and will try to cast their vote on fake web sites. The scenario is that operatives of the Orange party send messages to voters who belong to the Purple party claiming to be from the Purple party's candidate for president and giving a link to a look-alike web site for i-voting, encouraging voters to cast their votes early. The goal of the Orange party is to either prevent Purple voters from voting at all, or to convince them that their vote has been cast and then use their credentials (i.e., username and password) to have software cast their vote for Orange candidates, without the voter ever knowing.

The percentage of users who fall prey to targeted attacks has been a subject of some controversy. While the percentage of users who click on spam emails has fallen significantly over the years as more people are aware of them (and as spam filtering has improved and mail programs have improved to no longer fetch images by default), spear phishing attacks have been assumed to be more effective. The result from Oak Ridge is one of the most significant pieces of hard data in that regard.

According to an article in The Register, of the 530 Oak Ridge employees who received the spear phishing email, 57 fell for the attack by clicking on a link (which silently installed software in their computers using to a security vulnerability in Internet Explorer which was patched earlier this week—but presumably the patch wasn't installed yet on their computers). Oak Ridge employees are likely to be well-educated scientists (but not necessarily computer scientists) -

and hence not representative of the population as a whole. The fact that this was a spear phishing attack means that it was probably targeted at people with access to sensitive information, whether administrative staff, senior scientists, or executives (but probably not the person running the cafeteria, for example). Whether the level of education and access to sensitive information makes them more or less likely to click on links is something for social scientists to assess – I'm going to take it as a data point and assume a range of 5% to 20% of victims will click on a link in a spear phishing attack (i.e., that it's not off by more than a factor of two).

So as a working hypothesis based on this actual result, I propose that a spear phishing attack designed to draw voters to a fake web site to cast their votes will succeed with 5-20% of the targeted voters. With UOCAVA (military and overseas voters) representing around 5% of the electorate, I propose that a target of impacting 0.25% to 1% of the votes is not an unreasonable assumption. Now if we presume that the race is close and half of them would have voted for the "preferred" candidate anyway, this allows a spear phishing attack to capture an additional 0.12% to 0.50% of the vote.

If i-voting were to become more widespread – for example, to be available to any absentee voter —then these numbers double, because absentee voters are typically 10% of all voters. If i-voting becomes available to all voters, then we can guess that 5% to 20% of ALL votes can be coerced this way. At that point, we might as well give up elections, and go to coin tossing.

Considering the vast sums spent on advertising to influence voters, even for the very limited UOCAVA population, spear phishing seems like a very worthwhile investment for a candidate in a close race.

Cyber security at DOE national labs

Comment by David Jefferson
April 20th, 2011 at 11:10 am.

I think it is may be easier to succeed in targeting the general population of voters with email spear phishing attacks than it is national lab employees, at least at the national security labs like Oak Ridge.

1) Email entering our laboratory (Livermore,where I work--I am not completely sure this happens at the others) is "cleaned" before it ever gets to the recipient. There is a list of file types that are stripped as attachments to incoming mail. The attachments can come in using some other file types (e.g. a .zip file can come in if it is first renamed as .zzz) but then a deliberate action is required to open it. No one will idly or accidentally open a dangerous attached file.

   Likewise, URLs in incoming email are modified to have asterisks inserted into them so that clicking on the URL directly from the email program does not work. One has to copy the URL and edit out the asterisks. Again, no one will idly click on a URL in email that entered our lab from the outside--it takes a deliberate action.

2) There is, of course, heavier spam filtering than in most environments.

3) Unlike most other environments, there is no expectation of email privacy. All email, incoming and outgoing, is recorded and subject to analysis.

4) All DOE national laboratory employees are generally well educated, as you point out, but they also get constant, required training in security and cyber security, with more training as their jobs are closer to sensitive subject matter.

> It is hard to say how effective the training is, but it does make you constantly aware.

Yet even under these circumstances Oak Ridge was hit by this spear phishing attack, and this is not the first time something like this has happened. Thus, I think if anything you may be being conservative and underestimating the likely success rate of spear phishing attacks on the general population. I even have some personal experience as well: my mother was a victim of a spear phishing attack when she clicked on a link in email that was forged to look like it came from me. And my wife gets so much spam purportedly from me that I created a filter to sidetrack it.

Freedom to Tinker is hosted by Princeton's Center for Information Technology Policy.

2. The National Institute of Standards and Technology (NIST) has concluded that the Internet cannot be made secure for voting at this time.

A Threat Analysis on UOCAVA Voting Systems

Andrew Regenscheid and Nelson Hastings

(National Institute of Science and Technology (NIST), NISTIR 7551, December 2008. See pages 39–46 and 68 and 69. http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf)

Excerpt from pages 42, 43:

6.3.4 Electronic Mail

In most instances, voted ballots returned via e-mail would reach election officials nearly instantaneously. Communications could, however, be disrupted by malicious parties. Denial of service attacks are a significant threat to e-mail-based voting systems. Attackers could flood election e-mail servers with large amounts of illegitimate traffic. This could not only prevent voters' e-mails from reaching election officials, but could also make it difficult for officials to distinguish between valid and invalid ballots.

Eavesdropping is a potential threat whenever Internet communications is involved, and particularly with e-mailed communications, which are sent unencrypted. While eavesdropping is not a significant threat for ballot distribution, as that information is generally publically available, voted ballots must remain confidential. Voted ballots show how an individual voted, and may sometimes contain sensitive personal information about the voter. 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.

Also, e-mailed ballots are at risk before and after they are sent to election officials. Voters' computers could be infected with malicious code capable of disrupting communications with an election official. Very sophisticated attacks may be able to modify digital ballots prior to e-mailing them to election officials. Malicious code would need to spread to a large number of

personal computers before it would have a substantial effect on an election. The computer virus may be detected before election day, but there would be no way for election officials to identify affected ballots. Similar malicious code on election computer systems could have the same effect.

E-mail does not provide any guarantee that the intended recipient will receive the message. The e-mail system relies on the DNS system [11] to route e-mails to the proper servers. An attack on DNS servers could route e-mails to an attacking party. This would not only result in voter disenfranchisement, but also the loss of sensitive voter information. This kind of attack would require very sophisticated attackers focusing their efforts on major e-mail service providers. There are no known reports of a similar attack being successfully conducted on e-mail or DNS servers. However, it is important to note that a recent vulnerability was discovered in DNS servers that could have been used to construct a similar attack [13]. DNS servers were quickly patched before any significant attack took place.

Less sophisticated, but equally effective, attacks may attempt to trick voters into sending their ballots to an attacker. That is, an attacker would contact a large number of voters, claiming to be their local election official and attempting to convince them to reply with their cast ballot. While a relatively small number of voters may be fooled, it is relatively easy and cheap to contact a very large numbers of voters.

3. Computer security experts wrote a rebuttal to the DOD report that promoted use of the Internet for UOCAVA citizens.

(http://www.servesecurityreport.org/SERVE_Jr_v5.3.pdf.)

4. Computer technologists have stated their concerns about Internet voting; the introduction is quoted below.

Computer Technologists' Statement on Internet Voting (Signed by many eminent scientists)

(www.verifiedvoting.org/article.php?id=5867)

Election results must be verifiably accurate—that is, auditable with a permanent, voter-verified record that is independent of hardware or software. Several serious, potentially insurmountable, technical challenges must be met if elections conducted by transmitting votes over the Internet are to be verifiable. There are also many less technical questions about Internet voting, including whether voters have equal access to Internet technology and whether ballot secrecy can be adequately preserved.

Internet voting should only be adopted after these technical challenges have been overcome, and after extensive and fully informed public discussion of the technical and non-technical issues has established that the people of the U.S. are comfortable embracing this radically new form of voting.

APPENDIX B

FALSE CLAIMS ABOUT THE SECURITY OF INTERNET VOTING

1. The Example of Encryption (from a discussion at the "UOCAVA Remote Voting Systems Workshop" in Washington, D.C.)

In August 2010, Ronald Rivest, Viterbi Professor of Electrical Engineering and Computer Science at MIT and 2002 winner of the Turing Award—the "Nobel Prize" of computing—explained what encryption can and cannot do:

Encryption, he said, assures that an eavesdropper won't hear what is being sent, that what was sent by a PC is what is received at the other end. It doesn't ensure that what was sent by the PC was what the voter intended.

> "What I'm talking about is not attacks on the communication channel; they are attacks on the platform. The hard part here is the PC the voter is voting on, not the channel; you can use encryption for that. It doesn't protect from viruses and malware. It doesn't protect against malware that has been sent. It doesn't protect against viruses on the recipient election official's machine. Protecting communication channels is where we've made the most progress over the last three decades. We have not made progress with the PC's, such as protecting against insider attacks."

2. The Example of a Colorado Law Making False Claims of Security

In a law allowing an "Internet-based voting pilot program" for general election in 2012 (CRS 2010 1-5.5-101.(1)), unsupportable claims are made for the pilot program. For example, it says,

"The Internet-based voting system developed for use by political subdivisions that participate in the pilot program shall:

> (a) Transmit encrypted information over a secure network…
> [(b) …]
> (c) Protect the privacy, anonymity, and integrity of each elector's ballot…."

No national law requires that a state allow pilot projects such as Colorado has accepted. A state must agree to this. A pilot project using such insecure procedures as Internet voting should not be conducted in actual elections, but must be mock. Our current law on pilot projects should not deter us from prohibiting return of voted ballots by electronic transmission.

APPENDIX C

ELECTRONIC TRANSMISSION OF VOTED BALLOTS NOT NECESSARY FOR TIMELY ARRIVAL FOR COUNTING

As is stated on the Overseas Vote Foundation website,

> "Congress passed the MOVE Act in 2009 in response to chronic reports from overseas and military voters of late or lost ballots as well as unduly burdensome requirements for registering and requesting ballots.
>
> "As of the General Election in 2010, MOVE requires all states and territories to make voter registration and absentee ballot applications available electronically, provide a Federal Write-In Absentee Ballot, allow for a 45-day window for the ballot "round-trip", and several other reforms"

The Uniform Law Commission's "Uniform Military and Overseas Voters Act", the model law for HB11-1219, does not incorporate the electronic return of voted ballots for security and privacy reasons.

This is justified in its Prefatory Note: "…using electronic transmission methods for just those steps in the absentee voting process prior to the casting of a ballot (such as registering to vote, requesting an absentee ballot, and receiving a blank ballot) can alone dramatically reduce the time required to permit these voters to vote successfully."

There are also other alternatives for return of voted ballots, such as Fed Ex.
The Overseas Vote Foundation offers Fed Ex services for overseas voters in 90 countries, which runs for six weeks prior to the General Election every two years.

OVF has offered this new program to support timely casting of ballots from overseas, refraining from risking election integrity with electronic transmission of voted ballots:

"But let's also be clear that the use of the Internet to deliver voting materials is not the same thing as Internet-based voting. We at OVF - and many other voting advocates - believe there are still too much risk of identity theft, fraud and confidentiality to conflate these two. MOVE modernizes the balloting process without entering these muddy waters." HYPERLINK www.overseasvotefoundation.org/node/282.

APPENDIX D

EXAMPLES OF INTERNET HACKING

1. The Center for Strategic and International Studies (http://www.csis.org) lists 64 significant hacks between May of 2006 and early January of 2011.

http://csis.org/files/publication/110103_Significant%20Cyber%20Incidents%20Since%202006_0.pdf

2. The following hack of the Washington, D.C., Internet voting pilot project was a stunning demonstration. The hack was performed by the students of Professor J. Alex Halderman, a computer scientist in the Department of Electrical Engineering and Computer Science at the University of Michigan.

http://www.freedom-to-tinker.com/blog/jhalderm/hacking-dc-internet-voting-pilot

Hacking the D.C. Internet Voting Pilot

By J. Alex Halderman
Posted on October 5th, 2010, at 8:07 p.m.

The District of Columbia is conducting a pilot project to allow overseas and military voters to download and return absentee ballots over the Internet. Before opening the system to real voters, D.C. has been holding a test period in which they've invited the public to evaluate the system's security and usability.

This is exactly the kind of open, public testing that many of us in the e-voting security community — including me — have been encouraging vendors and municipalities to conduct. So I was glad to participate, even though the test was launched with only three days' notice. I assembled a team from the University of Michigan, including my PhD students, Eric Wustrow and Scott Wolchok, and Dawn Isabel, a member of the University of Michigan technical staff.

Within 36 hours of the system going live, our team had found and exploited a vulnerability that gave us almost total control of the server software, including the ability to change votes and reveal voters' secret ballots. In this post, I'll describe what we did, how we did it, and what it means for Internet voting.

D.C.'s pilot system

The D.C. system is built around an open source server-side application developed in partnership with the TrustTheVote project. Under the hood, it looks like a typical web application. It's written using the popular Ruby on Rails framework and runs on top of the Apache web server and MySQL database.

Absentee overseas voters receive a physical letter in the mail instructing them to visit a D.C. web site, http://www.dcboee.us/DVM/, and log in with a unique 16-character PIN. The system gives voters two options: they can download a PDF ballot and return it by mail, or they can download a PDF ballot, fill it out electronically, and then upload the completed ballot as a PDF file to the server. The server encrypts uploaded ballots and saves them in encrypted form, and, after the election, officials transfer them to a non-networked PC, where they decrypt and print them. The printed ballots are counted using the same procedures used for mail-in paper ballots.

A small vulnerability, big consequences

We found a vulnerability in the way the system processes uploaded ballots. We confirmed the problem using our own test installation of the web application, and found that we could gain the same access privileges as the server application program itself, including read and write access to the encrypted ballots and database.

The problem, which geeks classify as a "shell-injection vulnerability," has to do with the ballot upload procedure. When a voter follows the instructions and uploads a completed ballot as a PDF file, the server saves it as a temporary file and encrypts it using a command-line tool called GnuPG. Internally, the server executes the command gpg with the name of this temporary file as a parameter: gpg [...] /tmp/stream,28957,0.pdf.

We realized that although the server replaces the filename with an automatically generated name ("stream,28957,0" in this example), it keeps whatever file extension the voter provided. Instead of a file ending in ".pdf," we could upload a file with a name that ended in almost any string we wanted, and this string would become part of the command the server executed. By formatting the string in a particular way, we could cause the server to execute commands on our behalf. For example, the filename "ballot.$(sleep 10)pdf" would cause the server to pause for ten seconds (executing the "sleep 10" command) before responding. In effect, this vulnerability allowed us to remotely log in to the server as a privileged user.

Our demonstration attacks

D.C. launched the public testbed server on Tuesday, September 28. On Wednesday afternoon, we began to exploit the problem we found to demonstrate a number of attacks:

- We collected crucial secret data stored on the server, including the database username and password as well as the public key used to encrypt the ballots.
- We modified all the ballots that had already been cast to contain write-in votes for candidates we selected. (Although the system encrypts voted ballots, we simply discarded the encrypted files and replaced them with different ones that we encrypted using the same key.) We also rigged the system to replace future votes in the same way.
- We installed a back door that let us view any ballots that voters cast after our attack. This modification recorded the votes, in unencrypted form, together with the names of the voters who cast them, violating ballot secrecy.
- To show that we had control of the server, we left a "calling card" on the system's confirmation screen, which voters see after voting. After 15 seconds, the page plays the University of Michigan fight song. Here's a demonstration.

Stealthiness wasn't our main objective, and our demonstration had a much greater footprint inside the system than a real attack would need. Nevertheless, we did not immediately announce what we had done, because we wanted to give the administrators an opportunity to exercise their intrusion detection and recovery processes — an essential part of any online voting system. Our attack remained active for two business days, until Friday afternoon, when D.C. officials took down the testbed server after several testers pointed out the fight song.

Based on this experience and other results from the public tests, the D.C. Board of Elections and Ethics has announced that they will not proceed with a live deployment of electronic ballot return at this time, though they plan to continue to develop the system. Voters will still be able to download and print ballots to return by mail, which seems a lot less risky.

D.C. officials brought the testbed server back up today (Tuesday) with the electronic ballot return mechanism disabled. The public test period will continue until Friday, October 8.

What this means for Internet voting

The specific vulnerability that we exploited is simple to fix, but it will be vastly more difficult to make the system secure. We've found a number of other problems in the system, and everything we've seen suggests that the design is brittle: one small mistake can completely compromise its security. I described above how a small error in file-extension handling left the system open to exploitation. If this particular problem had not existed, I'm confident that we would have found another way to attack the system.

None of this will come as a surprise to Internet security experts, who are familiar with the many kinds of attacks that major web sites suffer from on a daily basis. It may someday be possible to build a secure method for submitting ballots over the Internet, but in the meantime, such systems should be presumed to be vulnerable based on the limitations of today's security technology.

We plan to write more about the problems we found and their implications for Internet voting in a forthcoming paper.

APPENDIX E

AMENDMENT #1: CHANGES TO TEXT OF RE-ENGROSSED VERSION

1. DELETIONS (See ~~strikethrough~~):

Page 11, line 4, **1-8.3-111. Timely casting of ballot.** TO BE VALID, A BALLOT SHALL BE RECEIVED BY THE APPROPRIATE LOCAL ELECTION OFFICIAL NOT LATER THAN THE CLOSE OF THE POLLS, OR THE VOTER SHALL SUBMIT THE BALLOT FOR MAILING, ~~ELECTRONIC SUBMISSION,~~ OR OTHER AUTHORIZED MEANS OF DELIVERY NOT LATER THAN 7:00 P.M. MOUNTAIN TIME ON THE DATE OF THE ELECTION.

Page 11, lines 20-24. ~~**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, AS SPECIFIED IN RULES PROMULGATED BY THE SECRETARY OF STATE.~~

2. ADDITIONS (See DOUBLE-UNDERLINED, ALL-CAPITAL TEXT*):*

Page 11, **1-8.3-113. Transmission and receipt of ballot.** COVERED VOTERS ARE PROHIBITED FROM RETURNING THEIR VOTED BALLOTS BY ELECTRONIC TRANSMISSION (INCLUDING FACSIMILE WHETHER VIA FAX MACHINE OR COMPUTER), AS THIS TRANSMISSION METHOD JEOPARDIZES ELECTION SECURITY AND VOTER PRIVACY.

AMENDMENT #2: CHANGES TO TEXT MUST REFLECT PREVIOUS DRAFT OF UMOVA MODEL LEGISLATION, AS PER MEMO FROM NATIONAL ASSOCIATION OF STATE ELECTION DIRECTORS (NASED).

To make this amendment, re-introduce “absent” to precede all references to “uniformed service voter” as they existed in the Uniform Law Commission's bill draft of October 2009. See Sections 2, 4, 6, and 9 through 18.

Delete 1-8.3-102(2)(a) and reletter the following sections (b) through (e) accordingly to (a) through (d). The reason to do so is that the House amendment present in (b) (limiting military personnel who may use this measure to those who are at least out of state) does not apply to the entire military population, as is mentioned in (a).