

Joint Testimony of VerifiedVoting.org and Voter Action
Regarding House Bill 1000
Submitted to the Committee on State Government & Tribal Affairs
Washington House of Representatives
January 12, 2011

Thank you for this opportunity to submit comment on House Bill 1000, a bill to allow overseas and service voters to receive blank ballots via fax, e-mail, or other electronic means; and also allow overseas and service voters to *return* their voted ballots via fax or e-mail. We applaud the intent of this effort to provide timely access to the ballot for Washington's brave men and women in uniform and other voters abroad, and the effort to remove unnecessary obstacles to the franchise for them. We strongly support the portion of the bill that allows voters to *request and receive all blank ballots* via fax, e-mail, or other electronic means.

But returning voted ballots electronically poses unacceptable risks to ballot secrecy and security, subverts Washington's voter-verified paper record law, leaving military and overseas voters with a 2nd class voting system and elections that cannot be legitimately recounted.

Current law (RCW 29.40.150(5)) allows overseas voters to fax marked ballots to counties provided that the original, marked physical ballot is also returned before certification of the election in question. H.B. 1000 deletes this provision and replaces it with vague language requiring that instructions sent to overseas and service voters "explain how a voter may return a ballot by fax or e-mail.

If votes are to be sent electronically, a provision like RCW 29.40.150(5) is essential to the security and recountability of the election. Electronic return is unnecessarily risky, but if deployed, **we urge that any "copy" of the voter's ballot returned by electronic means serve as a placeholder for receipt of the original voted ballot, and that the original ballot be counted upon its receipt by the election jurisdiction at any point up to certification.** This can be done so long as the electronic send occurs on or before close of polls in the jurisdiction, and the original ballot received prior to certification.

In 2005, Washington's legislature enacted a law requiring a voter-verified paper record for every vote cast in government elections, after testimony noting the impossibility of effective recounts or tabulation audits, absent the independent records of their choices confirmed by the voters, e.g. the original ballot. In July 2010 the National Association of Secretaries of State adopted a resolution calling for "accessible, *recountable*, and secure" election process for uniformed and overseas voters (emphasis added).¹ The Public Policy Committee of the US Association for Computing Machinery also cites the impossibility of recounts of electronically transmitted ballots without a corresponding paper ballot.²

The rationale for Washington's law applies to Web-based voting systems, including e-mail or fax. (It should be noted that faxes today largely traverse the Internet, not dedicated phone lines.) The present architecture of the Internet makes the ballot vulnerable to tampering by anyone in the world with access to the Internet, regardless of encryption protocols. Both the voter's client system and the election administrator's server may be compromised and render encryption useless. This fact was demonstrated in stark fashion last year, when researchers working remotely from the University of Michigan hacked into the District of Columbia's pilot Internet voting system during a public test, replacing encrypted

1 http://www.nass.org/index.php?option=com_docman&task=doc_download&gid=908&Itemid=

2 http://usacm.acm.org/usacm/PDF/IB_Internet_Voting_UOCAVA.pdf

ballots *without detection*. Following this demonstration hack, the District's election officials cancelled the pilot for November, using it only for sending blank ballots.

The D.C. pilot's failed experiment was, relatively speaking, superior to a voting process that includes using e-mail or fax transmission of marked ballots. E-mail, in particular, is so insecure that one voting technology expert said, "sending ballots by email is comparable to writing them in pencil and sending them on postcards, readable and modifiable by anyone who handles them along the delivery path."³

A partial list of the severe security challenges posed by e-mail voting includes:

- Any information technology worker who operates an email relay between the voter and the ballot's destination can read the ballot, copy it and forward the copy to a 3rd party, or modify the ballot arbitrarily to change the votes, or filter out ballots he does not like and allow others to go through – all undetectably. Out of the vast volume of email traffic it is trivial to identify those messages that are ballots simply by the destination email address.
- The above manipulation need not be done while the email is being relayed. It can be done by malicious code inside the voter's own computer, again potentially undetectably.
- Email is occasionally lost in transit, or duplicated, or bounced. The sender may not know.
- The "From:" address for email is easily forged. Depending how email addresses are used in voting this could lead to a variety of organized efforts at disenfranchisement or confusion.

Highly secured computer networks have been compromised, including those of multinational financial institutions and Google, with human, technical, and financial resources beyond what any vendor of electronic voting systems or local election jurisdiction can field.⁴ As experts have testified:

*"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."*⁵

In August 2010, the United States Election Assistance Commission published final requirements for its voluntary certification program for pilot military and overseas voting systems; these requirements rightly include a voter-verifiable paper record.⁶ Michigan, Minnesota, New York, Ohio, Virginia and other States have affirmatively prohibited the electronic return of voted ballots and focused their overseas-voting efforts upon timely blank ballot delivery, and extending the deadline for acceptance of marked ballots mailed from overseas and military voters. For military voters, the Department of Defense now offers express return of voted ballots free of charge up to seven days in advance of a Federal election. As the Pew Center on the States noted in its 2009 report "No Time to Vote," a great deal can be done for voters abroad without deployment of difficult-to-secure technologies. It will be a long time before e-mail or any other form of Internet voting is reliable enough for America's voters.

Thank you for your time and consideration. We are at your service if you have questions or would like to discuss this issue further.

3 Dr. David Jefferson, national security expert, private communication, April 17, 2010.

4 http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/RIVEST_2010-08-05-uocava.pdf

5 <http://www.ur.umich.edu/update/archives/101008/dchack>

6 http://www.eac.gov/assets/1/Documents/UOCAVA_Pilot_Program_Testing%20Requirements%20August%2008%202010.pdf