

This letter is to request that you act to protect the privacy and security of our military and overseas voters ballots.

Email and Fax Voting is not secure or private

Voter Action urges you not to vote on HB 2483 and its companion SB 6238 in their current forms which would allow a ballot to be returned by email and fax. Further we urge you not to vote for HB 1624 and its companion SB 5522 which would permit internet voting without providing adequate security and privacy, undermining the integrity of the voting process for our military voters and the election itself.

HB 2483 and SB 6238 provide that an overseas or service voter may receive a ballot by fax, e-mail, or other electronic means. The bill further provides that an overseas or service voter may return a voted ballot by fax or e-mail if the voter's signature on the declaration accompanies the ballot and that the county auditor must establish procedures to protect the secrecy of the voted ballot.

This legislation as written is not required by The Military and Overseas Voter Empowerment Act (MOVE). The Act requires the provision of voter registration applications, absentee ballot applications and transmittal of blank absentee ballots by mail and electronically. The Act further requires that the security and integrity of the voter registration and absentee ballot process must be protected. It does not, however, require that voted ballots be returned electronically. Indeed, those two things – security and electronic transmission of voted ballots - cannot coexist, as referenced below and in the attached materials.

We have additional concerns that security measures in the current form of the bills have not been specified nor is there a provision to develop standards or review by independent computer security experts knowledgeable about voting technology. Also worth noting is the perception that email is separate from the internet. To be clear, **email is always transmitted through the internet and subject to the same vulnerabilities**. Please see enclosed comments highlighting these serious threats by two nationally recognized security and voting experts who have reviewed these specific bills.

Therefore we urge you to modify HB 2483 and SB 6238 to provide only for the provision of voter registration applications, absentee ballot applications and transmittal of blank absentee ballots, but not permit voted ballots to be returned electronically. This would comply with MOVE without creating unnecessary privacy and security risks.

Internet Voting is not secure

HB 1624 and SB 5522 authorize internet voting for service voters and overseas voters. We urge you not to support these bills. Internet voting is inherently insecure, as prominent computer scientists have repeatedly advised. Internet voting and electronic voting transmission systems compromise the privacy and security of the vote. Currently, the Washington State Constitution safeguards voters by upholding some of the strictest voter privacy language in the nation.

- In January 2009 the Pew Center on the States issued a report on overseas and military voters stating that "simply sending blank ballots out via fax or e-mail can give military citizens abroad enough time to complete the process [of voting in a timely fashion]." The report further stated that electronic return of ballots created a risk of violating the privacy and security of those ballots.

- In December, 2008 the National Institute of Standards and Technology (NIST) issued a report stating that "Technology that is widely deployed today is not able to mitigate many of the threats to casting ballots via the web."ⁱⁱ
- In June, 2007 the U.S. Government Accountability Office (GAO) found that email and Internet voting is "more vulnerable to privacy and security compromises than conventional methods now in use" and that available safeguards may not adequately reduce the risks of compromise."ⁱⁱⁱ
- Both internet voting and transmitting marked ballots via fax or email jeopardizes voter privacy by assigning a traceable and identifiable unique user login or pin number to each voter. The security of these voting systems has been deemed insufficient by a 2004 study and subsequent report by the Secure Electronic Registration and Voting Experiment (SERVE)^{iv} resulting in the closure of an internet voting pilot program implemented by the Pentagon.
- Further, internet voting and electronic ballot submission removes the ability to perform critical, and in some instances, legally mandated recounts and audits. Internet votes cast in the 2004 gubernatorial election, for example, would not have been able to be recounted in the determination of Seattle's governor, thus invalidating those votes. HB 1624 and SB 5522 unwisely exempt those voting over the internet from the requirements that currently exist that require verifiable votes.
- Recent evidence cited in the Wall Street Journal regarding tampering with the United States electrical grid by hackers in both Russia and China^v and the increased security measures due to the highly sophisticated targeting of Google's infrastructure^{vi} reveals the susceptibility of these programs to outside interference.

During the 2009 legislative session, the internet voting bills in the House and Senate were defeated due to the original fiscal note not reflecting the cost to voters and counties to institute a new voting system. The internet voting pilot program conducted by the Pentagon cost an estimated \$6.2 million for one voting cycle, only to later be scrapped due to security concerns. Washington State cannot afford to unduly burden counties and taxpayers with a voting system that has been proven insecure and unreliable.

Voter Action supports Washington State initiatives to address problems military and overseas voters encounter when accessing the ballot. Voter Action's recommendation to ensure these voters are allowed ample time to cast a ballot, without sacrificing the integrity of the vote, is to allow for ballots to be printed from an online source and the paper ballot returned via express postal mail.

Voter Action encourages you to implement a solution that offers equal access for military and overseas voters to a secure and meaningful vote.

ⁱ *No Time to Vote: Challenges Facing America's Overseas Military Voters*, Pew Center on the States,

http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Election_reform/NTTV_Report_Web.pdf, January 2009.

ⁱⁱ *A Threat Analysis of UOCAVA Voting Systems*, Andrew Regenscheid and Nelson Hastings, National Institute of Standards and Technology, December 2008.

ⁱⁱⁱ *Action Plans Needed to Fully Address Challenges in Electronic Absentee Voting Initiatives for Military and Overseas Citizens*, June 2007, pg. 30. [GAO Report 07-774]

^{iv} *A Security Analysis of the Secure Electronic Registration and Voting Experiment*, Jefferson, et al., <http://servesecurityreport.org>, January 2004.

^v *Electricity Grid in the US Penetrated by Spies*, The Wall Street Journal, Siobhan Gorman, <http://online.wsj.com/article/SB123914805204099085.html>, April 8, 2009.

^{vi} *A New Approach to China*, The Google Official Blog, David Drummond, <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>, January 12, 2010.