October 7, 2010

Washington State Secretary of State
Elections Division
PO Box 40229
Olympia, WA 98504

Dear Secretary Reed,

It has come to our attention that on September 2, 2010 your office filed an emergency rule-making order, WSR 10-19-006, with the Code Reviser's office. The Emergency Rules make a number of changes to the existing rules regarding elections and specifically voting for service and overseas voters. The Emergency Rules provide that, among other things, voted ballots can be transmitted electronically, including via email. The Emergency Rules also eliminate reference to the voter agreeing to waive secrecy by the voter for the electronic transmission of voted ballots.

The reason cited for invoking emergency rule making pursuant to RCW 34.05.350 was as follows: "That state or federal law or federal rule or federal deadline for state receipt of federal funds requires immediate adoption of the rule." Presumably the reference is to the Military and Overseas Voter Empowerment Act (MOVE).

It is clear that MOVE requires states to establish procedures for "absent uniformed service voters and oversea voters" to request, and for States to send, voter registration applications and absentee ballot applications by mail and electronically. 42 U.S.C. § 1973ff-1(a)(6)(A) & (B). It further requires States to establish procedures to transmit *blank* absentee ballots by mail and electronically. *Id.* at § 1973ff-1(a)(7) & (f)(emphasis added). States must also "designate not less than 1 means of electronic communication" for applicable voters to request, and the States to send, voter registration and absentee ballot applications. *Id.* at § 1973ff-1(e)(1)(A) & (B).

MOVE further amends UOCAVA to require States to establish procedures to, to the extent practicable, protect the security and integrity of the voter registration and absentee ballot application request processes[,]" *id.* at § 1973ff-1(e)(6)(A), and safeguard "the privacy of the identity and other personal data" of applicable voters throughout the processes, *id.* at § 1973ff-1(e)(6)(B). It requires States to ensure further that the procedures by which applicable voters may request, and the States transmit, absentee ballots protect "the security and integrity of absentee ballots[,]" and "the privacy of the identity and other personal data" of such voters "throughout the process of such transmission." *Id.* at § 1973ff-3(f)(3)(A) & (B).

Nothing in MOVE, however, authorizes the electronic transmission of voted ballots.

None of the new language contained in WAC 434-208-060(1)(d) authorizing the email transmission of voted ballots is required or, arguably, condoned by MOVE. For this reason, the reasons for invoking emergency rule making are not present with respect to this expansion of the law that has nothing to do with the requirements of MOVE. Hence, the implementation of this provision through emergency rule making appears to be inconsistent with the Administrative Procedures Act. *See* RCW 34.05.350.

To be clear, our organizations support the use of the Internet to deliver ballots to military and overseas voters, which the federal agency responsible for administering UOCAVA, the Federal Voter Assistance Program (FVAP) of the Department of Defense, is working to provide this year. What FVAP is not providing for the 2010 federal election, and about which we are concerned, is any voting system that uses the Internet, whether by email, web applications, or web-based fax and phone, to deliver ballots that are marked with votes.

The fundamental concern is that the electronic transmission of voted ballots is insecure and subjects those votes to tampering and other unintended outcomes. Inherent with digital media, as recounted in detail in the attached document sent earlier this year to the Election Assistance Commission, it has become ever clearer, even in the past few months that cybersecurity is a very real threat to U.S. national security. The Congress is concerned about it, as are many other experts advising the U.S. on national security issues. S*ee* attached letter by prominent computer scientists. Your office should be deeply concerned as well and not permit the electronic transmission of voted ballots.

These concerns were illustrated last week when hackers successfully infiltrated the District of Columbia's Internet voting platform. Dr. J. Alex Halderman of the University of Michigan and his students gained complete access to the system while it was live online for a public trial, reporting that they were able to change ballot choices at will. The D.C. Board of Elections and Ethics have suspended the online return of voted ballots as a result of the hack. Emailing voted ballots has even more inherent security risks due to the infinite and uncontrollable variables that make the medium completely uncontrollable.

We are not improving access to voting, but instead jeopardizing the vote of our service and overseas voters by implementing such an insecure system in our state. We all share the desire to make every vote count, but permitting electronic transmission of voted ballots introduces a very dangerous approach to seek to achieve that end.

Sincerely,

John C. Bonifaz
Legal Director
Voter Action

Kelly Reese
Cooperating Attorney, Washington State
Voter Action

Pamela Smith
Executive Director
Verified Voting

Susannah Goodman
Director of Voting and Election Reform
Common Cause

Attachments: EAC letter, document signed by prominent computer scientists