VoterAction COMMON CAUSE 40 Years Holding Power Accountable 1970–2010 verifiedvoting

September 23, 2010

The Hon. Mary Cheh
John A. Wilson Building
1350 Pennsylvania Ave. NW, Suite 108
Washington, DC 20004

Dear Councilmember Cheh:

We write to express serious concerns that our organizations have with the proposed "digital vote-by-mail" pilot program for military and overseas voters, as described during Executive Director Suleman's testimony before your committee on 1 July, 2010.

Under DC Official Code § 1-1001.09(k)(1)(B), by 2012, elections administered by District officials must be done in such a way as to "create a voter-verifiable record of all votes cast." In short, the "digital vote-by-mail" program does not create such a system. The question then is why public money is being spent on a pilot, which, by design, thwarts the spirit of the newly enacted DC law. Moreover, if this internet voting system is ultimately adopted, by 2012 it will thwart the letter of the DC law. This is of concern especially since there are other ways of expediting ballot delivery and return to UOCAVA voters which are not being considered as part of this pilot.

Exec. Dir. Suleman's testimony indicated that the process for "digital vote-by-mail" under this program would be: a voter requests a personal identification number, which is then physically mailed to the voter; the voter then logs on to the DCBOEE site and, after entering her PIN number, receives an electronic ballot; the voter marks the electronic ballot on the screen, then "secures" her choice; finally, a paper version of the electronic ballot is printed, scanned and archived at DCBOEE on Election Day. These printed ballots will be double-blind, so that it will be impossible for the DCBOEE to tie a ballot to any individual voter. (It will also be impossible for the voter to inspect the printed version of her ballot for accuracy.) Finally, DCBOEE will notify the voter that a ballot in her name has been received and processed.

This system fails to meet the requirements of § 1-1001.09(k), as the final "ballot" used to determine the voter's intent will be the print-out at the elections office, which can neither be inspected by a voter, nor traced back to its origins. Since voters will not be able to independently verify that their selections were recorded as intended on the documents that represent the permanent record of their votes, this process is inadequate to fulfill the District's legal requirement that voting systems provide a voter-verifiable record of the votes cast. The final, official form the ballot takes--the printed paper ballot--cannot be inspected by voters. Voters will only be able to verify that e-ballots associated with their i.d. were received by the elections office, but neither voter nor official can confirm those e-ballots accurately represent voters' choices.

Additionally, the new law in Washington, DC requires post-election audits under DC Official Code § 1-1001.09a(b). These audits can only properly occur with records that have been verified by the voter. The ballots of UOCAVA voters will therefore not be able to be audited, again, contravening the new DC law.

Voter verified records are critical to maintaining an accurate count and to conducting an accurate audit. Ballots which have been cast over the Internet cannot be protected adequately and therefore cannot serve as the voter verified record. We can provide additional detailed information on the many ways ballots cast by UOCAVA voters in remote locations can be corrupted and why the ballot printed out at the DC BOEE is not a voter verified record. However, there are three major points of attack where the ballot can be corrupted. These include:

- In the voter's computer, as a result of malicious software such as viruses causing the choices the voter expresses to be invisibly modified before sending the ballot to the DC BOEE voting server. Accidental bugs in the voter's computer may also cause incorrect transmission of the voter's intent.

- In the network, where deliberate or accidental misrouting of messages could allow an attacker to prevent access to the DC BOEE server, or reroute the ballot to a fake server.

- In the DC BOEE server, where an insider (e.g., an employee) or an outsider (e.g., a hacker) could manipulate the records stored in the server to change or delete the ballots submitted by voters, or introduce new ballots.

The proposed "digital vote-by-mail" system violates the rights of the District's voters to verifiable balloting, and if fully implemented in 2012 would violate both the spirit and the letter of § 1-1001.09(k) and § 1-1001.09a.

We respectfully ask that you do what you can to oppose the adoption of this unlawful and insecure program as designed, and instead urge the pursuit of the responsible use of technology to assist UOCAVA voters in participating in the election, through the expedient delivery of blank ballots to qualified voters and other means which do not risk the integrity of the election.

Blank ballots can be transferred to voters over the Internet, and once marked, there are a number of ways they can be returned to the District for counting. The Overseas Vote Foundation has created a number of successful models for delivery of marked ballots back to election jurisdictions without jeopardizing the privacy and security of the ballot. A number of states which prohibit the type of Internet voting the DC pilot envisions, successfully partner with groups like the Overseas Vote Foundation. In other words, undermining the newly enacted very important DC law is not necessary to properly and honorably serve UOCAVA voters.

Sincerely,

Susannah Goodman
Director of Election Reform
Common Cause

Pamela Smith
President
Verified Voting

John Bonifaz
Legal Director
Voter Action