September 24, 2010

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

Dear Councilmember Cheh:

As you know, Internet voting is inherently problematical and is not now, and may never be, safe, secure, or reliable. Using current technology, voters cannot validate that their votes are counted as intended, and there are numerous opportunities for bugs and security flaws to interfere with an accurate vote count. Hence, we were very concerned when the DC BoEE announced their intention to perform a pilot program. However, we were assured that a testing period would be provided for public comment; we felt confident that the testing period would allow us to provide ample evidence of the risks and vulnerabilities of such an approach.

As a result, we have been monitoring the schedule for the Internet voting experiment planned by the DC BoEE. Finally, on Monday the DC BoEE released the schedule for testing their Internet voting system for the November election. The schedule invites testers to request credentials to test the system beginning on Fri Sep 24, and concluding Thu Sep 30. See http://www.dcboee.org/popup.asp?url=/pdf_files/nr_588.pdf for the announcement.

We recognize the serious problems overseas and military voters face when attempting to exercise their voting rights. Like you, we find the current failure rate to be unacceptable and we encourage, and many of us participate in, efforts to improve the process. However, use of the internet to return voted ballots could result in much more severe disenfranchisement of the voters we seek to assist. Today, it is commonly accepted that some 30% of UOCAVA voters attempts fail to be counted in accordance with their wishes; it is not an overstatement to say that use of systems like the one proposed for testing by the DC BoEE could result in even higher levels of failure and those failures might not be apparent to the affected voters, the BoEE, or any other participant in the election.

To summarize, this voting system not only has never previously been used in an election, but it also has never been validated or certified by any agency. Nor has it been subject to any kind of independent testing at all. Given that it is a new and complex software system, it should not be used in a general election until it has been subjected to extensive independent expert testing by those not having any financial or administrative interests in the system.

We have serious concerns with the announced schedule and terms of the testing:

1. The legal terms and conditions are anything but clear. The DC BoEE memo says "Users will not be held liable for damage resulting from good faith efforts at testing system integrity." However, the term

"system integrity" is not defined. Without strong safeguards, anyone participating in this experiment to protect the larger public's voting rights unavoidably would place themselves at serious risk.

2. The terms of engagement are not defined, nor are the outcomes of successful compromise. For example, would a Denial of Service attack, in which mock voters are prevented from gaining access to the DC BoEE web site, be considered in scope? Would the success of such an attack be considered sufficient grounds for canceling use of the system for the November election? What if attacks on the network infrastructure caused mock voters to be redirected to a site under the attacker's control? (This can be done using techniques known as DNS poisoning and BGP route hijacking - both well within the skill sets of many attackers.) Would malicious software infiltrated into voter computers and modifying their votes be in scope? Without knowing what sorts of successful attacks would be considered adequate proof of the inadequacy of the system, it is difficult to know where to put our efforts, to demonstrate that this system is unsuitable for use.

3. There is no provision at all for assessing what would happen if an insider were part of an effort to modify votes. As this is a common cause of election fraud, omitting it from the experiment is inappropriate.

4. Both the notice provided and the time allotted for testing are far too short. Expecting experts to drop everything on three days notice to begin an unpaid week-long activity is disrespectful to their time.

5. There is no designated, qualified test organization (separate from the BOEE) to run the test and assess the results. It appears that the BOEE intends to act in that capacity themselves, which biases the entire process.

6. According to the BoEE announcement, there will only be a "limited number of test credentials" issued on a first come first serve basis. It is unclear whether these test credentials are to allow access to the system, or to task mock votes. Is this is a mechanism for choosing who is allowed to do the testing?

7. There is no provision for full release of the experimental data, including all server logs, so that independent experts can study what happened and make independent assessments. As it stands, BOEE will keep the data to themselves and issue their own opinion regarding the success of the tests, with no independent assessment at all.

8. Even if all of the above were not concerns, the fact remains that such tests at best show the presence of problems. There is relatively little incentive for anyone with nefarious intent to participate in such an event; the reality is that at best you get the "good guys", and find a subset of the problems, while at worst you find nothing. Return of marked ballots over the Internet is something we simply don't know how to do safely. Exercises such as this are counterproductive, because they will provide a false sense of security to the DC BoEE, while the real problems lie undetected.

9. There is simply not enough time to fix any but the simplest problems between the end of the testing period (Sep 30) and the beginning of the live use of the system (apparently beginning Oct 4). And even if any problems were fixed, there would be inadequate time to test them and ensure that new problems were not introduced (a common problem when modifying complex software).

We strongly urge you and Councilmember Cheh to insist that the DC BoEE cancel use of the experimental system for returning of voted (marked) ballots, extend the period of the experiment, and establish clear and sufficient legal protections provided to participants who are testing the system remotely. (While we are concerned about use of the system to allow printing blank ballots, we believe that risk is manageable.) Allowing this poorly conceived experiment to go forward on such an abbreviated timeline is a disservice to the DC UOCAVA voters and imperils the overall accuracy of every election on the ballot.

We are at your disposal if additional information is needed, or if testimony to hearings is required.

Sincerely,

David Dill
Professor of Computer Science
Stanford University, and
Founder, Verified Voting

Jeremy Epstein
Senior Computer Scientist
SRI International

Susannah Goodman
Director of Election Reform
Common Cause

Joseph Lorenzo Hall
Postdoctoral Research Fellow
University of California, Berkeley School of Information
Princeton University Center for Information Technology Policy

Candice Hoke
Professor, Cleveland-Marshall College of Law
Cleveland State University

David Jefferson
Lawrence Livermore National Laboratory, and
Chair of Board, Verified Voting

Douglas Jones
Professor of Computer Science
University of Iowa

Mark Lindeman

Peter Neumann
Principal Scientist
Computer Science Laboratory
SRI International

Ronald Rivest
Professor of Electrical Engineering and Computer Science
MIT

Barbara Simons
IBM Research (retired), and
Former president, Association for Computing Machinery

Penny M. Venetis
Clinical Prof. of Law and Clinical Scholar
Co-Director, Constitutional Litigation Clinic
Rutgers School of Law-Newark

Dan Wallach
Professor of Computer Science
Rice University