

From: [Pamela Smith](#)
To: votingsystemguidelines@eac.gov
Subject: comments - UOCAVA Pilot
Date: 04/30/2010 03:50 PM
Attachments: VWF comment UOCAVA Pilot Guidelines04-30-2010.pdf

Attached please find Verified Voting's comments on
http://www.eac.gov/program-areas/voting-systems/docs/requirements-03-24-10-uocava-pilot-program/attachment_download/file

These comments should supercede/replace any comments sent by our organization previous to this date on this subject (we submitted comments on 04-15-2010).

Thanks very much!

Best,
Pamela Smith, President
Verified Voting Foundation
and V
cell: [REDACTED]



April 30, 2010

U.S. Election Assistance Commission
1201 New York Ave, NW., Suite 300
Washington, DC 20005

RE: UOCAVA Pilot Program Testing Requirements: Public Comment

Dear Commissioners,

Thank you for the opportunity to comment on the proposed *UOCAVA Pilot Program Testing Requirements*. We appreciate the invitation for public input to such an important initiative. In this letter we confine our comments to the broad outlines of the pilot program and core precepts to which we believe any pilots should adhere.

The Verified Voting Foundation has benefited greatly from prominent experts whose professional work duties include achieving U.S. national security objectives within digital networks and computer communications. This expertise leads us to set forth this core understanding: Federal election security is a fundamental component of U.S. national security. Applying this principle, we submit that election security should not be compromised for convenience or transmission speed.

Internet voting (which for purposes of these comments we define as transmission of voted ballots over the public Internet) is in a security class by itself. In comparing Internet transmission of voted ballots to paper absentee ballot voting, we agree with the oft-made point that voting systems for UOCAVA voters should not be held to a higher security standard than domestic absentee voting. Nor should UOCAVA voters be required to use a system that is *less* secure than those used by voters back home.

Unfortunately, few analyses acknowledge two major security risks that threaten voted ballots transmitted over the public Internet: (a) large scale *automated* attacks, and (b) *invisible* attacks by *remote control*. The attacks could be against the terminal machines that voters use, the servers collecting ballots, the Internet infrastructure over which the ballots are transported, or the development systems of the vendor (as in the recent Chinese attacks on Google and others). And they can be perpetrated by anyone, anywhere—a disaffected insider, a third party IT technician, a self-aggrandizing hacker, or an adversary nation's intelligence agency. Neither potential attack threatens large numbers of absentee paper ballots mailed via traditional methods, or a mail-in paper ballot election system as a whole. We believe, therefore, that no Internet voting systems should be fielded without built-in protection against these threats in the form of end-to-end auditing.

Verified Voting recommends that all voting systems satisfy fundamental security policies:

1. The systems are auditable through independent, voter-verified audit records (which in current technology requires paper records), preferably through the use of voter-marked paper ballots;

2. They include robust (ideally risk-limiting) audits of the published vote tallies, using a hand-to-eye count of the voter-verified paper ballots or records, conducted prior to finalizing the election results; and
3. The systems permit, to the maximum extent possible, the principle of the secret ballot (preserving the anonymity of the voter from his/her choices).

All voting systems should also incorporate desirable usability and accessibility features to maximize their availability to all voters. We hope that the EAC will incorporate more thorough requirements which will allow the testing of such features for UOCAVA voters.

While we recognize that this particular document is contemplated to be an equipment standard, we strongly believe that what is needed is a security standard. The introductory section 1.1.2 of the Pilot Requirements document states:

In 2009 the EAC convened a UOCAVA Working Group to consider how to adapt the EAC's Testing and Certification Program to accommodate UOCAVA pilot systems. It was concluded that two products were needed: a modified set of system testing requirements; and a revised testing and certification process. It was determined that the working group would assist the EAC in drafting the testing requirements and EAC staff would adapt the certification process to accommodate the UOCAVA pilot program.

We believe that the two described products alone will not be sufficient to effectively support the states conducting electronic voting projects for UOCAVA voters. The EAC's role in promulgating these guidelines as stated in the language of the MOVE Act can extend to best practices and standards, going beyond merely defining rules for how equipment should be manufactured, to how it should or should not be deployed.¹ Given that a number of states do plan to conduct real pilots with real ballots in 2010 using systems such as those sketched out in these draft guidelines, such additional guidance on usage from the EAC is essential.

Section 1.1.3 states:

the certification process must retain sufficient rigor to provide reasonable assurance that the pilot systems will operate correctly and securely.

It is not possible to provide such assurance through the certification process alone. It is necessary to require those deploying these systems to undertake certain minimum security practices as well. Of course we recognize that many if not most of those jurisdictions will do so of their own accord, but the point remains that such reasonable assurance that a system will operate correctly and securely can only be obtained through confirmation such as that provided by a robust post-election audit.

The proposed UOCAVA pilot guidelines draft includes two very important features. First, the initial pilot under consideration does not contemplate voting from private PCs, but instead only

¹ MOVE Act), Subtitle H, the Technology Pilot language: *(e) Technical Assistance- (1) IN GENERAL- The Election Assistance Commission and the National Institute of Standards and Technology shall provide the Presidential designee with best practices or standards in accordance with electronic absentee voting guidelines established under the first sentence of section 1604(2) of the National Defense Authorization Act for Fiscal Year 2002 (Public Law 107-107; 115 Stat. 1277; 42 U.S.C. 1977ff note), as amended by section 567 of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (Public Law 108-375; 118 Stat. 1919) to support the pilot program or programs.*

from secured terminals staffed by election officials. This restriction is an essential minimum step toward being able to assure security of the election, if Internet-based pilots are conducted in the future.

Second, to make electronic vote tallies potentially auditable, one minimum requirement is the ability of a voter to check on a physically robust independent hard-copy record that his/her vote was recorded the way it was intended. The proposed guidelines call for the production of voter-verified paper records of each ballot cast, an indispensable design feature for remote voting system architectures. It would be a significant improvement to require that these records be at least as robust and durable as other absentee ballots.

With these points in mind, we offer our suggestions on how best to support the conduct of UOCAVA pilot project(s), consistent with the best engineering evaluation practices and with the intent of governing federal law.

1. Conduct pilots in mock elections only for the first several rounds.

The MOVE Act authorizes (but does not require) the conduct of “*1 or more pilot programs under which the feasibility of new election technology is tested,*” and such pilots “may” involve the transmission of ballots over “military networks” and perhaps other networks as well. But we emphasize: the MOVE Act does not require that “pilot programs” be conducted with real ballots in real Federal or State elections.

The EAC can require that before any live deployment in real elections, pilots to be conducted are in mock elections, with subsequent technical and security forensic evaluations conducted by forensic teams of experts in computer and network security that are independent from contractors conducting the pilot or supplying its software. This would fully implement the congressional intent without suffering the substantial risks that are unavoidable if a system is essentially test-run in the fire of a real election. We realize that mock elections have limited value for security tests, but we have far less enthusiasm for the deployment of such systems in live elections.

It is important to understand that with the exception of e-mail and fax voting (both of which are dangerous) the current Internet voting systems are not only brand new, but are also a brand new *category* of voting system. While there have been many previous “pilots” of such systems over the last decade, as far as we know no Internet voting system for public elections has ever been used more than once in the U.S., and no vendor has participated in more than one such pilot in the U.S. In several cases, fewer than 100 votes have been cast in those pilots. In most cases these pilots lacked any transparency and did not include independent auditing to assess their successes or problems. Thus, the national experience with such systems is so extremely limited that it would be irresponsible for the EAC to authorize their deployment in the context of a real federal election until extensive testing and post-mortem evaluations have occurred within mock elections.

2. Require extensive security testing before the pilot.

As part of any pilot project which involves the electronic return of voted ballots, and before any Internet voting system is used in a real public governmental election, we believe that it is important for independent experts to assess its security. Internet voting systems are attackable by anyone or any agency in the world, and can be attacked remotely from anywhere, from outside the reach of

U.S. law and from within nations that are deeply opposed to the American government. Attacks on the servers or development machines used could go undetected long in advance of an election.

Only an independent expert assessment of the system can give any confidence of its suitability for use in real elections. We strongly recommend that studies of such Internet voting systems be conducted and patterned along the lines of the California Top to Bottom Review (TTBR) of Voting Systems, the Ohio EVEREST study, and the Florida ODBP study (the latter conducted as part of certification). Such a study should include red-team penetration attack experiments, both with and without benefit of source code. And after some confidence has been achieved, a mock election should be conducted that is open to attack by anyone who wishes with assessments thereafter.

3. Include a robust election auditing process within the scope of any pilot.

We are pleased to see that with the production of voter verifiable paper records for each ballot the initial pilot will be auditable *in principle*. But we believe that actually conducting an audit is an essential part of any election process, and that includes all remote voting systems.² While we recognize that it may not be possible for the EAC to impose these requirements in an equipment standard, or as part of the EAC certification process itself, we believe that pilots should include an audit and that the EAC can make this requirement part of a security standard that supplements the equipment standard and certification process. Hence, all pilots should include as part of the project post-election auditing of the published vote tallies using the voter-verified paper records, preferably a risk limiting audit as described in the auditing literature.

On the point of the paper records the Pilot Program Requirements document requires them to be produced, and to have a unique ID attached to them, but as currently written, it does not require anything to be done with them. Figure 1.1, for example, shows that the paper records are produced, but shows no subsequent use of them at all. Likewise section 2.4.2.2 requires the production of the paper records, but specifies no subsequent review or processing of them, i.e. they are not required to be randomized, or collected, or transported back to the home jurisdictions. And if they are transported, the proposal does not specify a chain of custody procedure. For example, should the paper records be copied before transport, in case they are lost in transit? Does the 2-person rule apply during transport? Are there any special sealing procedures that should be followed for packaging the paper records for transport? Should the paper records be transmitted by bonded courier, “express mail”, or hand carried? What if the records are never delivered?

A new iteration of the Requirements document (or supplemental document) should incorporate best practices for the deployment of such records, including their use in robust post-election vote-tabulation audits. Such guidance would be appropriate and would not usurp state control over standard audit and recount processes, given that this guidance would apply to the UOCAVA pilots only (and, ideally, to mock elections only for the near term). Since the purposes of the paper records are to support the various audit, recount, and challenge processes in the states and local jurisdictions, and to have a means of detecting any problems with the technology, a pilot should assess their suitability for that purpose. Thus, the UOCAVA Pilot Requirements or supplemental document should delineate procedures for chain of custody and best practices for safeguarding the documents for both voter privacy and auditing/technological assessment purposes. To that end, we

² “The voter verified paper record, by itself, is of questionable security value. The paper record has significant value only if an automatic routine audit is performed (and well designed chain of custody and physical security procedures are followed).” http://brennan.3cdn.net/e66b464b91c7a06398_tam6b8vxc.pdf

suggest that the Pilot Requirements be amended to answer at least these questions regarding the paper records:

- (a) Are they to be randomized? If so, and in light of some confusion over what constitutes randomizing, identify some valid techniques for randomizing paper ballot records.
- (b) How long must the records remain readable? (Some voting system records are known to fade in less than 6 months.)
- (c) Given the unique ID on each record, what are the recommended and acceptable ways of protecting voter privacy?
- (d) How many paper records are lost or corrupted due to printer jams?
- (e) How easy is it to audit or recount one race, or all races, by various methods?

Because auditing depends on valid chain of custody and related procedures, the UOCAVA Pilot proposal should be amended to address these questions.

4. Assure that the pilot is *open* so independent experts can assess the results.

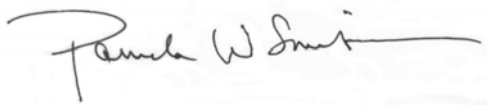
Because this is a pilot for a totally new class of federal election systems, everyone has an interest in it. It is vital that the pilot be *open* in the sense that all information needed to assess the results is available to independent experts and to the public at large. The voting system should be instrumented to keep detailed logs of every critical action in a human-readable, self-documenting format, and relevant system logging should be turned on for all terminal nodes, clients, servers, and routers that are within the control of the pilot. These logs should be made available without requiring non-disclosure agreements to independent experts after the trial for their assessment of the security, privacy, reliability, accuracy, and performance of the system.

5. Include auditable cost accounting as part of the pilot.

Finally, we urge that as a part of any pilot practices there be a publicly-disclosed cost accounting for the entire election pilot. The accounting should separate development costs from operating costs, and operating costs should be detailed to include accurate estimates for costs associated with hardware, software, logistics, bandwidth, mailing, transport of paper ballot records, personnel, travel, consumables, repair and spare parts, and post-election auditing processes. It should also break down all federal, state, and jurisdiction costs. The accounting should be designed to permit an honest estimate of the cost of conducting a real election at large scale, and an estimate of system lifecycle costs.

Thank you for the opportunity to respond to this important draft document that seeks to effectuate the MOVE Act and UOCAVA. If you would like to discuss or otherwise follow up on any points made above, please do not hesitate to contact me.

Sincerely,



Pamela Smith
President