



Operation BRAVO
F o u n d a t i o n

May 26, 2009

The Honorable Zoe Lofgren
Chair, Subcommittee on Elections
Committee on House Administration
U.S. House of Representatives
1309 Longworth House Office Building
Washington DC 20515

Madame Chair:

Thank you for the opportunity to submit written testimony on the topic of "Military and Overseas Voting: Obstacles and Possible Solutions." Operation BRAVO Foundation (OBF) is a 501(c)(3) organization. Our mission is to foster the exploration and development of practical and reproducible electronic voting alternatives to improve the military and overseas citizen voting process. Our board of directors has extensive firsthand experience with these voting issues from our work as elections officials and as participants and/or managers of electronic voting projects. OBF sponsored the 2008 Okaloosa Distance Balloting Pilot in conjunction with the State of Florida and Okaloosa County.

We are pleased to see the current high level of interest being shown by the Congress as well as state legislators in finding better voting methods for this group of citizens. We hope you find the attached testimony helpful to your deliberations. We welcome any questions or comments you may have.

We offer our sincere appreciation to you and the other subcommittee members for all your work in improving our elections. Please advise if we can be of any further assistance.

Respectfully,
Operation BRAVO Foundation
Board of Directors

Carol A. Paquette
Patricia Hollarn
Chip Levengood
Gary Smith

Attachment



Operation BRAVO
F o u n d a t i o n

TESTIMONY IN SUPPORT OF LEGISLATION TO AUTHORIZE UOCAVA VOTING PROJECTS USING SECURE ELECTRONIC TRANSMISSION

WHY ARE PILOT PROJECTS NEEDED?

Many studies document that a very large percentage of military and overseas voters is disenfranchised by the existing absentee voting process. For example, an Election Assistance Commission survey after the 2006 election reported that close to 992,000 ballots were requested but only 330,000 returned.

The current voting process entails mailing application forms and ballots back and forth between voters located all around the globe and thousands of local election offices in the U.S. Although relying on the slowest possible transmission method, the delivery and return of ballots must occur within a relatively short time period. A recent study by the Pew Center on the States reports that fewer than half of the states provide enough time for overseas military and civilian voters to reliably return their ballots before the deadline.

It is generally agreed that significant changes must be implemented nationwide to achieve a more effective UOCAVA voting process. While much attention has rightly been given to the ballot transit time issue, there are other problems with the current process that also disenfranchise voters. The Voting Over the Internet (VOI) Assessment Report (June 2001, Section 4.2.1) notes the following reasons cited by election officials for invalidating returned ballots, in addition to their being returned after the deadline: No signature, mismatched signatures (i.e., signature on ballot does not match signature on file), no witness signature and/or address, spoiled ballot (i.e., voter marked the ballot, or changed their selections, in a manner that cannot be interpreted), and ballot returned to wrong election official. While this information is somewhat dated, anecdotal reports suggest these issues persist. Remote electronic transmission is the most promising avenue for quicker ballot delivery, and it also can address many of these other problems.

Multiple pilots are needed to examine a variety of alternatives as no single solution will be appropriate for all jurisdictions and voter circumstances. Transitioning from paper by-mail to electronic methods raises many procedural and legal issues. The VOI, Secure Electronic Registration and Voting Experiment (SERVE), and Okaloosa Distance Balloting Pilot (Okaloosa) projects all required considerable analysis to adapt existing state and local processes to work with remote electronic voting. While each of these projects used different remote voting methods, all were designed to electronically mimic the by-mail process. Future projects should examine where procedures could be modified to more effectively integrate remote electronic voting into the overall local election administration process. For example, are digital signatures a legally and practically acceptable alternative to the current requirement for the voter to also submit a paper ballot with a written signature to validate their identity and thereby allow their electronic ballot to be counted?

Pilot projects provide the opportunity to prove out the real world feasibility of proposed solutions. Many concepts that appear easy to implement in theory run into difficulty when tried out in

practice. For example, some have suggested that military networks and computers be used to provide secure electronic voting for military voters. One of the lessons learned in the VOI project was that military networks are strictly configuration controlled, and all software running on those networks must be certified by the managing Military Service. VOI required voters to use a Netscape browser, a widely used, commercially available product. However, the Air Force and the Coast Guard had standardized on a different browser and would not allow this product to be downloaded to their systems. Consequently, Air Force and Coast Guard participants in VOI could not use their work computers to vote. In a similar vein, some election officials have had difficulty sending ballots as email attachments to military voters because some DoD networks reject attachments that exceed a specified size limitation.

ACTION PLAN NEEDED

There needs to be a national research framework to promote methodical and comprehensive examination of the feasibility and effectiveness of remote electronic voting methods. Relying on grass roots generation of pilot projects without such a framework will potentially result in duplicated efforts while important questions are left unaddressed. The June 2007 GAO report, "Action Plans Needed to Fully Address Challenges in Electronic Absentee Voting Initiatives for Military and Overseas Citizens," recommends that the Department of Defense (DoD):

'Create an integrated, comprehensive, long-term, results-oriented plan for future electronic voting programs that specifies, among other things, the goals to be achieved along with tasks including identifying safeguards for the security and privacy of all DoD's voting systems – both electronic and Internet. The plan should also specify milestones, time frames, and contingencies, synchronize them with planned development of the [*Election Assistance*] Commission's guidelines for Internet voting, and be developed in conjunction with major stakeholders – including state and local election officials, the Election Assistance Commission, overseas voting groups, and each of the armed services.'

The May 2007 FVAP report, "Expanding the Use of Electronic Voting Technology for UOCAVA Citizens," states that it 'discusses plans by the Federal Voting Assistance Program (FVAP) for expanding the use of electronic voting technologies for citizens covered by [*UOCAVA*] for the 2008 presidential election and the 2010 general election.' This document does not provide the long term, comprehensive plan that GAO recommended. DoD/FVAP should be encouraged to immediately initiate this planning activity in conjunction with the Election Assistance Commission (EAC) and other stakeholders.

NATIONAL TESTING AND CERTIFICATION PROCESS NEEDED

The lack of standards for the testing and certification of remote voting systems is another significant obstacle when considering electronic voting projects. All states require voting systems to undergo some level of testing and certification before they can be used in an election. The voting systems used for the 2000 FVAP VOI pilot and the 2008 Operation BRAVO Okaloosa pilot

were tested and certified by the State of Florida. However, few states have their own testing program and rely on the EAC to certify the voting systems they use.

The GAO report cited above made the following recommendation to the EAC:

‘Develop and execute in conjunction with major stakeholders – including state and local election officials and DoD – a results-oriented action plan that specifies, among other things, goals, tasks, milestones, time frames, and contingencies that appropriately address the risks found in the UOCAVA voting environment – especially risks related to security and privacy.’

The EAC initiated a voting systems risk analysis in September 2008 that is scoped to include remote electronic voting systems. This effort is expected to be completed before the end of calendar year 2009. EAC has also tasked the National Institute of Standards and Technology (NIST) to develop UOCAVA voting standards as required by HAVA Section 245. It would be beneficial for NIST to examine a variety of actual systems to appropriately scope the requirements and develop meaningful and testable standards. Pilot projects could provide these examples.

FUNDING NEEDED

There is currently no funding source for voting technology projects, which prevents jurisdictions from experimenting. Operation BRAVO’s recent research indicates significant interest by states in pilot participation, but no ability to fund projects due to current severe budgetary constraints. Some states, such as Colorado, have included a provision in their pilot project legislation that funding will be sought from gifts, grants, and donations from private and public sources. It has been Operation BRAVO’s experience that there are not many foundations that support civic engagement types of projects. Some of those that do have expressed concern that voting technology projects might be perceived as political activity, even though projects involve state and local government offices. It appears that without federal funding there will be limited progress in finding new solutions for UOCAVA voting.

TIME IS OF THE ESSENCE

Federal elections take place every two years, which stretches out the opportunities for fielding pilots. Past experience indicates that approximately 18 months are needed to plan and conduct projects. The preparation of a national action plan could take many months to complete. NIST’s development of national UOCAVA standards will extend beyond the end of 2009. In the meantime, the decision deadline for 2010 election projects will occur in a few months.

Operation BRAVO Foundation has defined a 2010 combat kiosk project that builds on its successful 2008 Okaloosa pilot proof of concept. This project would expand the scope from a single county to multiple counties in up to five states. Secure remote voting kiosks would be placed in several combat zone locations to test the feasibility and cost effectiveness of this method to reach voters without access to postal mail, FAX, or email. The combat kiosk system will be

demonstrated at the National Civic Summit in Minneapolis in mid-July. A number of states have expressed interest in taking part in this project, but none has any funding. The estimated cost for a five state combat kiosk project is \$5 million. Other organizations may also have projects in the planning stages.

Operation BRAVO recommends that Congress make up to \$10 million available to fund projects for the 2010 election. This will maintain the momentum on developing better UOCAVA voting methods while the above recommended national initiatives are being put in place. Not to do so will mean a four year delay in identifying possible solutions. Once solutions are proved out, it will take several more years for jurisdictions nationwide to implement those best suited for their particular election administration environment.

Operation BRAVO Foundation further recommends that Congress establish a national goal of enabling UOCAVA absentee citizens to vote with the same success rate as domestic absentee voters by the 2016 national election. This is a mere four election cycles away. Establishing a target date is necessary to maintain focus on this problem until it is solved.

POLITICAL CLIMATE

Perhaps the biggest obstacle to conducting remote electronic voting projects is a highly vocal group of computer science activists who object in principle to using Internet technology for voting. In 2008 a group of computer scientists issued a statement proposing several criteria that, in their view, Internet voting systems must meet in order to be reliable, secure, and auditable. This list lacks many basic requirements such as: allow only qualified voters to vote, provide each voter with the correct ballot style, ensure only one ballot is counted per voter, provide authentication of all system users, and maintain the secrecy of the voter's choices. But, despite its shortcomings, their statement underscores the fact that meaningful and objective criteria are needed for developing and testing reliable remote electronic voting systems. Consequently, extensive requirements analyses were performed for the 2000 Voting Over the Internet pilot, the 2004 Secure Electronic Registration and Voting Experiment, and the 2008 Okaloosa Distance Balloting Pilot.

The following comments summarize how the voting system developed for the 2008 Okaloosa Distance Balloting Pilot addressed all of these criteria. This summary is provided to demonstrate that the engineering knowledge exists to create secure, reliable, and auditable remote voting systems, and therefore the nation needs to get on with the task of using this knowledge to develop more effective voting methods for UOCAVA citizens.

1. *The voting system as a whole must be verifiably accurate in spite of the fact that client systems can never be guaranteed to be free of malicious logic.*

The Okaloosa voting system source code was reviewed by an independent third party team of nationally recognized computer security experts, including several who have been critical of Internet voting. The system was also thoroughly examined and tested by the Florida Bureau of Voting Systems Certification. Paper records were produced for all

electronic ballots and used to verify system performance through a 100% audit of the electronic votes cast.

2. *There must be a satisfactory way to prevent large-scale or selective disruption of vote transmission over the Internet.*

All system transmission was encrypted and conducted via Virtual Private Networks, so communications were never exposed to the open Internet or processed through DNS routers. Also the kiosks operated for a 10 day voting period, significantly mitigating the impact of a denial of service attack.

3. *There must be strong mechanisms to prevent undetected changes to votes, not only by outsiders, but by insiders.*

The system employed patented immutable chained logs that recorded all transactions whether initiated by a person or a software process. The system also made extensive use of cryptography to protect voted ballot data, and operating procedures required multiple parties to perform critical steps such as ballot decryption. The paper records were used to audit the electronic ballot results.

4. *There must be reliable, unforgeable, unchangeable voter-verified, records of votes.*

All voted ballots were signed by the voter's digital signature for authentication. The voter could review a printed paper record of his/her ballot selections before casting the electronic ballot. These records were returned to the Supervisor of Elections office by kiosk workers. Each paper record contained a randomly-generated code that could be anonymously matched with the code associated with the corresponding electronic ballot to verify its authenticity.

5. *The entire system must be reliable and verifiable even though Internet-based attacks can be mounted by anyone, anywhere in the world.*

Extensive use of cryptography throughout the system, immutable chained logs of all system transactions, use of Virtual Private Network and SSL communications links provided end-to-end reliability and verifiability.

6. *Principles of operation of any Internet voting scheme should be publicly disclosed in sufficient detail so that anyone with necessary qualifications and skills can verify that election results can reasonably be trusted..*

The source code for the Okaloosa kiosk system was turned over in its entirety along with all system documentation to an independent third party review team comprised of nationally recognized voting system and computer security experts. The system was thoroughly tested by the State of Florida. The system logs allow the audit of all transactions to identify any anomalous activity.