From: Macias, Ryan
To: votingsystemguidelines@eac.gov
Subject: California Secretary of State's Comments on UOCAVA Pilot Program Testing Requirements
Date: 04/30/2010 03:56 PM
Attachments: CA SOS comments on UOCAVA Pilot Program Testing Requirements.pdf

---

Secretary of State
DEBRA BOWEN
State of California

Comments of Debra Bowen, California Secretary of State, on the Election Assistance Commission UOCAVA Pilot Program Testing Requirements

Making it easier for our country's overseas and military voters to fully participate in the electoral process is an important objective, and the Elections Assistance Commission (EAC) is to be commended for continuing to work toward meeting this goal. I certainly appreciate and want to thank the EAC Commissioners for establishing the EAC UOCAVA Working Group (Working Group) and making the Working Group's draft UOCAVA Pilot Program Testing Requirements (Draft Testing Requirements) available for public comment.

The Draft Testing Requirements make important strides by requiring penetration testing, detailed and comprehensive electronic audit log features, and extensive post-election audits of pilot program voting systems. The Working Group's decision to limit eligible pilot programs to kiosk-based voting on controlled-configuration computers in supervised polling places is certainly appropriate, as is the decision to preclude the use of uncontrolled personal computers in the possession of voters or in locations such as Internet cafes.

However, as California's chief elections officer, I am very concerned that this pilot program does not, given the state of the currently available technology, serve the interests of overseas and military voters or of the nation. This fundamental change in how votes are cast and transmitted is based on hastily drafted standards that have been subject to a truncated review period. Furthermore, the timetable for implementation is inappropriately short given the magnitude and impact of the proposal. Previously, the EAC has established public comment periods of 120 to 180 days for proposed voting systems standards. In this case, the Draft Testing Requirements were made public on March 26, 2010, with an initial public comment deadline of April 9, 2010, giving the public a mere 14 days to review the sweeping proposal. Even after the deadline was pushed back to April 15, 2010, and then to April 30, 2010, elections officials, computer scientists, election integrity organizations and other members of the public were given only 35 days to review and comment on a complex set of requirements in an unexplored area. The schedule after this short public review period is equally compressed. It calls for finalizing the requirements, accepting vendor applications, conducting testing and audits, and certifying systems in time for deployment in the November 2010 General Election. This timetable is not appropriate for a program that creates an entirely new method of voting without any assurance that the people the program is ostensibly being designed to assist will have their votes counted in the event the pilot program is a failure.

The following comments deal first with broad areas of concern, and then with specific sections of the Draft Testing Requirements.

I. The Draft Testing Requirements Ignore Multiple Expert Assessments that the Risk of Compromising Integrity of Voted Ballots Cast over the Internet is High

Multiple studies and reports have been published identifying and analyzing the numerous ways voted ballots cast over the Internet can be compromised, and those studies and reports have evaluated proposed controls and mitigations advocated by some as sufficient to address those threats. The Draft Testing Requirements indicate the Working Group has not adequately addressed the findings and recommendations of those studies and reports:

- Dr. Alec Yasinsac, University of South Alabama, et al., *Elections Operations Assessment: Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA), EAC Advisory Board and Standards Board Draft ("Threat Trees")*, December 23, 2009.
    - The Working Group gives no indication that it took into account the analysis of threats specific to the integrity of voted ballots cast over the Internet in this EAC-commissioned study. "The source materials drawn on for this effort included: the Voluntary Voting System Guidelines (VVSG) 1.0; the VVSG 1.1; the VVSG 2.0; the VOI, SERVE and Okaloosa Project requirements documents; FIPS; and NIST Special Publications." Draft Testing Requirements, p. 7.
    - The *Threat Trees* report devotes 10 pages to a labyrinth of threats to the security and integrity of voted ballots cast over the Internet. The matrix includes a column labeled "recommended controls," with the authors' proposals for ways to guard against each threat. Use of "high assurance software" is listed under "recommended controls" more than 50 times. High assurance software is a very rigorous standard for software development. Not a single NASED or EAC certified voting systems currently in use in the United States meets this standard. The Draft Testing Requirements do not require or make any reference to use of high assurance software in a system that would allow people to cast voted ballots over the Internet.

- Andrew Regenscheid, Nelson Hastings, *A Threat Analysis on UOCAVA Voting Systems ("NIST Threat Analysis")*, Information Technology Laboratory, National Institute of Standards and Technology (NIST), NISTIR 7551, December 2008.
    - As with *Threat Trees*, there is no indication the Working Group drew on the analysis in this NIST study of threats specific to the integrity of voted ballots cast over the Internet. NIST conducted the study specifically to assist the EAC research "electronic technologies that may help to assist overseas voting as defined by the Uniformed and Overseas Absentee Voting Act (UOCAVA)." (*NIST Threat Analysis*, p. 1.)
    - "8.2 Delivery of Blank Ballots
      "In general, the threats affecting delivery of blank ballots to UOCAVA voters pose less serious challenges than the threats for the return of voted ballots . . .. " (P. 67.)

- "8.3 Return of Voted Ballots
  The return of voted ballots [over the Internet] poses threats that are more serious and challenging than the threats to delivery of blank ballots and registration and ballot request. In particular, election officials must be able to ascertain that an electronically-returned voted ballot has come from a registered voter and that it has not been changed in transit. Because of this and other security-related issues, the threats to the return of voted ballots by e-mail and web are difficult to overcome." (P. 68.) . . .
  "Use of Web for Return of Voted Ballots: Casting ballots via the web poses a large number of security challenges that are difficult to overcome." (P. 69.)

- David Jefferson, Avi Rubin, Barbara Simons, A *comment on the May 2007 DoD report on Voting Technologies for UOCAVA Citizens.*
  - "In 2003 the Department of Defense engaged our services to review its SERVE Internet voting project. The project was subsequently killed because of the numerous and fundamental security problems with it that we documented in a report we issued in 2004 (www.servesecurityreport.org). We are concerned that this new report appears to be trying to persuade readers that SERVE was a successful project and that Internet voting can be made safe and secure. Unfortunately, it does not accurately reflect the degree of concern that we and many others have expressed about Internet voting." (P. 1.)

- Dr. David Jefferson, Dr. Aviel D. Rubin, Dr. Barbara Simons, Dr. David Wagner, *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*, January 21, 2004.
  - "The real barrier to success is not a lack of vision, skill, resources, or dedication; it is the fact that, given the current Internet and PC [personal computer] security technology, and the goal of a secure, all-electronic remote voting system, the FVAP [Federal Voting Assistance Project] has taken on an essentially impossible task. There really is no good way to build such a voting system without a radical change in overall architecture of the Internet and the PC, or some unforeseen security breakthrough." (P. 3.)
  - "The vulnerabilities we describe cannot be fixed by better design of Internet voting software. They are fundamental in the architecture of the Internet and of PCs and their software. They cannot be eliminated for the foreseeable future. It is quite likely that they will never be eliminated without a wholesale redesign and replacement of much of the hardware and software security systems that are part of, or connected to, today's Internet." (Pp. 2-3.)

- *Computer Technologists' Statement on Internet Voting,* September 11, 2008.
  - Signatories include computer scientists from Carnegie Mellon University, Johns

Hopkins University, Lawrence Livermore Laboratory, Princeton University, Purdue University, Rice University, SRI International, Stanford University, University of California, University of Indiana, University of Iowa, University of Texas, and Yale University.

- "Several serious, potentially insurmountable, technical challenges must be met if elections conducted by transmitting votes over the [I]nternet are to be verifiable. . . . The principles of operation of any [I]nternet voting scheme should be publicly disclosed in sufficient detail so that anyone with the necessary qualifications and skills can verify that election results from that system can reasonably be trusted. Before these conditions are met, "pilot studies" of [I]nternet voting in government elections should be avoided, because the apparent "success" of such a study absolutely cannot show the absence of problems that, by their nature, may go undetected. Furthermore, potential attackers may choose only to attack full-scale elections, not pilot projects." (P. 1.)

II. The Draft Testing Requirements Fail To Address Recent Evidence Of Successful Internet Attacks On Well-Defended Government, Military and Private Computers and Data

In recent months, previously undisclosed successful Internet-based attacks on well-defended government, military and private computers and data have been reported. The Draft Testing Requirements document, as well as the oral testimony provided to the EAC by its testing and certification staff and members of the Working Group at the April 8, 2010, public hearing make no reference to these attacks and their implications for the security of voted ballots cast over the Internet. The successful attacks, reported in the press and verified in reports issued by respected computer and Internet security firms and scholars, include:

- A China-based computer espionage operation in which intruders accessed classified and restricted documents from the highest levels of the Indian Defense Ministry, the Dalai Lama's personal e-mail messages and documents related to the travel of NATO forces in Afghanistan.
  John Markoff and David Barboza, *Researchers Trace Data Theft to Intruders in China*, New York Times, April 5, 2010.
- Sophisticated cyber attacks on the computer systems of Google and 34 other companies and entities, most of them located in the Silicon Valley area of California. Andrew Jacobs and Miguel Helft, *Google, Citing Attack, Threatens to Exit China*, New York Times, January 12, 2010.
- Computers in multiple federal agencies, including the National Security Agency, Homeland Security Department, State Department, Treasury Department, Federal Trade Commission and Secret Service, overwhelmed by difficult-to-trace cyber attack. Associated Press, *Federal Web Sites Knocked Out by Cyber Attack,* July 8, 2009.

III. UOCAVA Working Group Members and EAC Staff Are On Record Supporting Moving Toward Still Higher Risk Internet Voting From Voters' Personal Computers Even Before Results of Kiosk Internet Voting Pilots Are Known

As noted above, the Draft Testing Requirements document would only be applied to kiosk-based systems. Successful pilot programs, however, are often viewed as evidence of the viability of technologies beyond those actually tested and reviewed as part of the pilot project. There is no dispute among security experts that allowing a voter to cast a voted ballot over the Internet using a personal computer or other uncontrolled computer in locations such as Internet cafes, poses a tremendous and possibly insurmountable set of security problems. Members of the Working Group and the EAC's testing and certification staff have indicated the currently proposed kiosk-based pilot programs are stepping stones to allowing voters to cast ballots using their personal computers, and that, in the view of the Working Group, this major expansion of the program is a desirable, inevitable and manageable step.

For example, Working Group member, Mark Skall, stated during his oral testimony before the Commission on April 8, 2010, that "[w]e will eventually need to migrate to the model where the voter uses his or her own computer to vote." Matt Masterson, Deputy Director, Testing and Certification (EAC), said in his written testimony for the April 8 hearing:

> "There is a fundamental dichotomy in complexity in remote voting architectures: those where the voting platform is controlled (e.g., provided by the election jurisdiction); and those where it is not controlled (e.g., the voter uses his own personal computer). Since the EAC planned to have the pilot certification process ready for implementation during the first half of 2010, it was decided that the EAC would focus its efforts on controlled platform architectures servicing multiple jurisdictions. . . . [M]ost of the core system processing functions are the same for both types of architectures. This allows for a substantial number of requirements to carry over as this work is expanded to include other methods of remote electronic voting."

Statements such as those above are why it is critical for the EAC to significantly strengthen the testing process for the proposed pilot program that will allow voted ballots to be cast over the Internet using a government-controlled kiosk. Pilot program results are likely to be cited as evidence or proof that voted ballots could be securely cast over the Internet using a personal computer. It is therefore vital that the proposed testing regime be more rigorous and well defined.

IV. Comments on Specific Provisions

Section 1.1.3 Scope of EAC Pilot Project Testing Requirements, Page 7, Para. 4: This passage states, "the EAC planned to have the pilot certification process ready for implementation during the first half of 2010."

Comment: As noted above, the Draft Testing Requirements were not made public until late March, three months before the proposed implementation date. This is insufficient time for meaningful public review and for serious consideration of public comments by the Working Group, EAC Testing and Certification staff, and the Commission.

Section 1.1.3 Scope of EAC Pilot Project Testing Requirements, Page 7, Para. 4: The draft states in relevant part that controlled platform architectures serving multiple jurisdictions are "a highly secure remote voting solution."

Comment: This statement should be revised so that it does not appear to pre-judge the security of the Internet voting systems to be evaluated under the Draft Testing Requirements.

Section 1.2 UOCAVA Remote Electronic Voting System Scope, Page 9, Para. 1: The draft states that [f]or security purposes, no vote data is permanently retained by the voting device. The cast ballot is transmitted to an electronic ballot box which is stored at another location."

Comment: It is not clear why the EAC views retaining no vote data in the voting device to be an asset and a security protocol that should be observed. This architecture is a departure from the design of most electronic voting systems that have received federal certification. In those systems, a redundant electronic record of the votes cast on the device is stored in randomized order in the device. The existence of these redundant vote records has been regarded as a check against tampering with ballots after they leave the device and as a useful backup in case other records of the votes cast are lost or destroyed.

Section 1.3.2.2 Requirements of entities, Page 11, Para. 2: The draft mandates that "certain requirements SHALL be tested by the manufacturer rather than the VSTL [Voting System Testing Laboratory]."

Comment: It is not clear why performance of certain tests by the manufacturer should be mandatory rather than optional. From my standpoint, and I believe the standpoint of most states, local elections officials and voters who will be expected to place their trust in the integrity of the testing process and the reliability of the test results, testing by an independent laboratory should be mandatory. This comment applies to each of the subsequent paragraphs that would mandate testing by the manufacturer.

Section 1.3.2.2 Requirements of entities, Page 11, Para. 3: "The EAC SHALL review the test results and associated documentation from both the VSTL and the manufacturer and make a determination that all requirements have been appropriately tested and the test results are acceptable."

Comment: This sentence should be revised to ensure the EAC cannot and will not simply "rubber stamp" the testing and results.

Section 1.3.2.2 Requirements of entities, Page 11, Para. 3: "The EAC will issue a pilot program certification number that indicates conformance of the specified system to these requirements."

Comment: This sentence should be revised to ensure the EAC will not simply "rubber stamp" the testing and results.

Section 1.3.3 Extensions, Page 11, Para.4 : This section would allow "extensions," defined as "additional functions, features and/or capabilities included in a voting system that are not required by this document."

Comment: If the intent is to allow the vendor or a state or local jurisdiction, without loss of EAC system certification, to add "extensions" that are not tested and certified by the EAC as part of the voting system, the security provisions of the Draft Testing Requirements will be rendered meaningless. The security of any system is only as good as its weakest link. This section states that extensions "SHALL NOT" . . . cause the nonconformance of functionality required by this document" but is silent regarding security required by the document. Allowing "extensions" also renders useless the System Identification Tools requirement of the draft EAC Voting System Pilot Program Testing and Certification Manual (Draft Manual), section 4.12. Finally, allowing "extensions" is in direct conflict with the following sentences in Draft Manual section 4.15: "The EAC certification and certificate apply only to the specific voting system configuration(s) identified, submitted and evaluated under this Program. Any modification to the system not authorized by the EAC will void the certificate." Permitting any untested, non-de minimis modification of a voting system after it is tested and certified would be a sharp and unacceptable break with all past federal testing guidelines and practice. Section 1.3.3 should be eliminated.

Section 1.3.5.2 Procedures for changes to baseline configuration, Pages 12-13, Para. 4: "Any change to hardware or software (Major Versions) SHALL be regression tested by the voting system manufacturer to ensure that all requirements affected by the change have been adhered to. . . . Test Reports describing the manufacturer regression testing SHALL be submitted to the EAC. The EAC may conduct random audits to ensure that the manufacturer regression testing performed was sufficient."

Comment: This is one of several instances in which the decision to assign responsibility for testing to the manufacturer rather than a VSTL is inappropriate and unacceptable. A major version change in an operating system can cause incompatibility problems not only with the voting system application but also with security hardening requirements developed for the prior version of the operating system. California recently confronted this problem with a voting system used by many counties. The vendor, while cooperative, assumed initially that the major version change in the operating system would not cause problems. The vendor was then slow to pinpoint incompatibilities with the hardening requirements for the previous version and to propose mitigations. Pilot programs tend to be pursued on aggressive timetables. A VSTL should promptly and rigorously test all proposed major operating system and COTS version

changes as they would be installed and used in the field, including security-hardening requirements.

Section 2.3.1.2 Protect the election definition, Page 19, Para. 2: "The voting system SHALL provide a method to protect the election definition from unauthorized modification."

Comment: This requirement appears to assume that there is only one point of vulnerability, which could be addressed by a single protective method.

Section 2.4.3.2 Voting session records, Page 22, Para. 4: "The voting system SHALL NOT store any information related to the actions performed by the voter during the voting session."

Comment: It is not clear why the prohibition in section 2.4.3.2 is necessary or appropriate to preserve vote secrecy.

Section 4 Software, Pages 33-41:

Comment: The vast majority of requirements in Section 4, governing software-coding practices, are assigned to the manufacturer for testing by "Inspection." Independent inspections of source code in voting systems that are currently federally certified have, in several cases, revealed extremely poor coding practices that expose the systems to malicious tampering—and this after an Independent Testing Authority (ITA) laboratory recommended certification after its own code review. A manufacturer has no incentive to report accurately on its own coding practices, particularly for purposes of a pilot program that will be used in only a single election. Testing responsibility for all of the software code requirements in Section 4 should be assigned to an independent VSTL.

Section 4.6 Executable Code and Data Integrity, Page 36:

Comment: The Draft Testing Requirements do not require the VSTL to create a Witness Build of a voting system the EAC certifies under the pilot program. Without a Witness Build, held by an independent VSTL and used to create the copies that are distributed to users, there is no way to ensure that what is installed in the field is identical to what was tested and approved. This and all other testing requirements documents for pilot program voting systems should require a Witness Build and include a cross reference to the Witness Build provisions in sections 4.9-4.12 of the Draft Manual.

Section 4.7.2.11 Election integrity monitoring, Page 39, Para. 4:
"The voting system SHALL proactively detect or prevent basic violations of election integrity (e.g., stuffing of the ballot box or accumulation of negative votes) and alert an election official or administrator if such violations they (sic) occur.
"Test Method: Inspection
"Test Entity: Manufacturer"

Comment: Verifying compliance with this critical requirement for the integrity of the voting system should not be assigned to the manufacturer. It should be the responsibility of an independent VSTL, including the penetration testing team.

In addition, by use of the disjunctive "or," this requirement treats prevention and detection as equally effective means to preserve election integrity. They are not. While detection of violations is important, it can be too little, too late. This is particularly true if detection does not occur in real time and if legally binding alternative contingency plans cannot be implemented immediately to restore the integrity of the election.

The election of a President and Vice President every four years provides the best illustration. The presidential election timetable is strict and inflexible. Pursuant to its authority under Article II, Section 1 and the Twelfth Amendment to the Constitution, Congress has provided, in Title 3, Chapter 1 of the United States Code, for the election to be held on the first Tuesday after the first Monday of November. The Constitution requires this date to be same throughout the United States. Congress has also provided that the presidential electors must cast their votes on the first Monday after the second Wednesday in December following the election. Congress must meet on the 6th day of the following January to tally the votes of the electors and officially declare the result of the election. The Twentieth Amendment to the Constitution requires the newly elected President and Vice President to be sworn into office on January 20.

If violations casting the integrity of the presidential election in doubt are not detected until after Election Day, there is no provision for a public re-vote. If they are not detected until after the vote of the Electoral College, there is no provision for that body to change its vote; the same is true for the Congress and the vote it takes in the first week of January.

Such concerns may be dismissed using the rationale that the Draft Testing Requirements will only impact small pilot programs involving a small number of votes, so the outcome of any contest could not be affected. One need only recall the extremely narrow margin separating the candidates in the Florida presidential balloting in 2000 or the New Mexico presidential balloting in 2004 to recognize that such assurances ring hollow. While these pilot program standards are intended only for November 2010, a non-presidential election, one-third of the seats in the United States Senate, will be on the November 2010 ballot and will be decided by statewide votes, some of which could involve narrow margins.

These proposed standards for one-time pilot programs are being presented as the template for a permanent certification program for allowing ballots of millions of UOCAVA voters to be cast over the Internet. Under these circumstances, crucial assumptions about the efficacy of detecting, as opposed to preventing, the compromise of this new method of voting should be carefully scrutinized.

Section 4.8.1.2 Failures not compromise voting or audit data, Page 40, Para. 1:
"Exceptions and system recovery SHALL be handled in a manner that protects the integrity of all recorded votes and audit log information.
"Test Method: Inspection
"Test Entity: Manufacturer"

Comment: It is unclear why the EAC views it as sufficient to test compliance with this requirement by "Inspection" rather than "Functional Testing." Would "Inspection" mean that, after restoring normal operation during the "Functional" test in section 4.8.1.1, the manufacturer would inspect the audit logs to ensure that they are present and complete and inspect the results tape to ensure that it prints and reports correctly? Here, as with other requirements for which "Inspection" is specified as the test method, more detailed instructions are necessary to ensure a meaningful Inspection.

Section 5.6 Logging, Pages 54-59:

Comment: The logging requirements are comprehensive and detailed. They are a major improvement over the logging provisions in the versions of the VVSG under which all current voting systems received federal certification.

Section 5.6.3.2 Critical events, Page 57, Para. 3:
"All critical events SHALL be recorded in the system event log.
"Test Method: Functional
"Test Entity: Manufacturer"

Comment: The term "critical events" should be defined in the Draft Testing Requirements, not left to be defined by the manufacturer. (See comment on section 5.7.1.1 below.) In addition, assigning responsibility for testing this requirement to the manufacturer rather than the VSTL is not appropriate. California's recent investigation of the audit log features of currently certified voting systems revealed that most manufacturers have devoted little attention to the scope, usability, security, and testing of logging features.

Section 5.7.1.1 Incident Response Support, Page 60, Para. 1:
"Critical Events: Manufacturers SHALL document what types of system operations or security events (e.g., failure of a critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.
"Test Method: Inspection
"Test Entity: Manufacturer"

Comment: The classifications of critical system operations and security events should be defined in the Draft Testing Requirements, not left to be defined by the manufacturer. (See comment on section 5.6.3.2 above.) In addition, assigning responsibility for inspection regarding this

requirement to the manufacturer is questionable. The exercise of independent judgment by a VSTL should be required.

Section 5.7.1.2 Critical events, Page 60:
"Critical event alarm: An alarm that notifies appropriate personnel SHALL be generated on the remote voting device or server, dependant upon which device has the error, if a critical event is detected.
"Test Method: Functional
"Test Entity: Manufacturer"

Comment: The correct operation of critical event alarms is critically important to preserving the availability and integrity of the voting system. It should be tested by an independent VSTL.

Section 5.9 Test environment, Page 66: "Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used."

Comment: Section 5.9 requires the test team to replicate, in a controlled lab environment, "the real world environment in which the voting system will be used." A critical component of a voting system in which ballots are cast over the Internet is the Internet itself. Real world assessment of threats that reside in the Internet environment, between the overseas vote capture computers and domestic servers, is difficult or impossible in a controlled laboratory environment. First-time testing of ballot transmission on the real Internet in the November 2010 election poses unacceptable risks. The testing requirements should require attempts to compromise transmission of mock ballot by Internet from vote capture computers in the foreign countries from which UOCAVA ballots will likely originate and servers in representative States to which those mock ballots will be transmitted.

Section 8.5.1.1 Overall security, Pages 89-90:
"Manufacturers SHALL document in the TDP all aspects of system design, development, and proper usage that are relevant to system security. This includes, but is not limited to the following:

- "System security objectives;
- "All hardware and software security mechanisms;
- "All cryptographic algorithms, protocols and schemes that are used;
- "Development procedures employed to ensure absence of malicious code;
- "Initialization, usage, and maintenance procedures necessary to secure operation;
- "All attacks the system is designed to resist or detect; and
- "Any security vulnerabilities known to the vendor.

"Test Method: Inspection
"Test Entity: Manufacturer"

Comment: This requirement is critical to the security of the system but is of real value only with full compliance on the part of the manufacturer. Assigning responsibility to the manufacturer to police its own compliance is tantamount to trusting the proverbial fox to build the henhouse, design the security system for the henhouse, guard the henhouse, and faithfully report each morning that all of the hens have survived the night unharmed. Based on my experiences in California, voting system vendors have a very poor record of disclosing to certification authorities the existence of known security vulnerabilities in their voting systems. An independent VSTL should be responsible for inspecting compliance with this requirement.

V. Conclusion

Testing any voting system with real votes in a real election is fraught with risk. Restricting this experiment of allowing UOCAVA voters to cast their ballots over the Internet to a single election is an implicit acknowledgment of that risk. However, one test in a real election is one test too many. The Draft Testing Requirements reflect a bias in favor of certification and place too much trust in manufacturers. Fundamental technical and policy decisions incorporated into the Draft Testing Requirements must be reconsidered. Some changes, like allowing the addition of untested "extensions" to certified systems without loss of certification, reverse longtime federal certification practice and threaten to strip the entire certification process of all value and credibility. The time for public comment is inadequate, as is the time for testing and deployment of pilot program voting systems.

Pressing ahead to place the EAC's stamp of approval on experimental systems that take the leap into allowing UOCAVA voters to cast ballots over the Internet is a disservice to those voters. It may compromise the integrity and privacy of ballots cast by our military and overseas voters and will certainly lead to misplaced confidence that the pilot project can easily be scaled up to allow people to cast a ballot over the Internet from any computer anywhere in the world.