



BACKGROUND on COMMENTS
Technical Guidelines Development Committee (TGDC)
Draft Voluntary Voting Systems Guidelines (VVSG)

VerifiedVoting.org's founder testified¹ to the Election Assistance Commission (EAC) on July 28, 2005 on various points, including voter-verified paper records (VVPR), terminology on such records in the guidelines, wireless networking, etc. Some key issues are discussed below. (This document does not cover the complete range of issues and should only be considered a sample.)

VOTER VERIFIED PAPER RECORDS:

The EAC to date has declined to require or even recommend a voter-verified paper record. The excuse: explicit language for VVPR was not part of the Help America Vote Act (although a strong argument can be made that it is implied). However, the EAC is not bound by the advisory recommendations of the TGDC, and has the power to express such a requirement in the guidelines. We believe it is within the EAC's interpretive powers to define the document used in the manual audit.

Inclusion of the requirement would help define more appropriately the mandatory paper audit trail in Section 301(a)2 of the Help America Vote Act (HAVA). No legitimate audit can be carried out unless that audit uses a contemporaneous independent indelible record of the voter's intent. No electronic record -- unseen by the voter and subject to programming error, equipment malfunction or even malicious tampering -- can reasonably meet that standard, nor any reprint (unverified by the voter) of that same electronic record. Thus it would vastly improve the legitimacy of the nation's elections if the EAC were to clarify that the manual paper audit trail indeed shall be voter-verified.

On January 18, 2005 Professor Ron Rivest introduced a resolution (#13-05) to require voter-verified paper trails at the TGDC meeting. Professor Rivest is the member of the TGDC with (by far) the greatest expertise in computer security. That resolution was voted down, by members of the committee who know less about computer security than the person who introduced the measure.

We urge the EAC to reinstate the recommendation in resolution #13-05 and require the essential safeguard of voter-verified paper records.

CLARIFICATION OF TERMS:

The (currently "optional") VVPAT guidelines fail to define the term "VVPAT" sufficiently. Voter-verified paper ballots such as optical scan ballots, which can be voted with the assistance of ballot-marking devices or by the voter manually marking the ballot, would not fit the same model as a voter-verified paper audit trail printer such as would be attached to a DRE voting machine. Machines that simply print ballots without keeping an electronic copy also do not meet the DRE+VVPAT model.

¹ <http://www.verifiedvotingfoundation.org/downloads/eactestimony.pdf>



Without clarification in the guidelines, the VVSG seem to assume that state-mandated paper trail requirements will be met by DRE voting machines with attached voter-verifiable printers. Some requirements, for example, that the voter not be able to handle the ballot, are inappropriate for ballot-marking devices. Yet we know that the EAC does not (and should not!) oppose the use of ballot-marking devices.

We urge the EAC to clarify in the VVSG must clarify which requirements apply to which technology.

WIRELESS NETWORKING:

The guidelines as drafted allow wireless networking, which opens up security threats. Despite the inclusion of items requiring documentation and justifications for the use of wireless, the inevitable consequence of allowing it is that machines with wireless capability will be certified, even though they will not and **cannot be secure**. Wireless networking is unnecessary and inherently unsafe, and should be banned outright.

We urge the EAC to reject wireless capability of any kind in our voting systems.

INTEROPERABILITY:

Interoperability is the ability of equipment from different vendors to work together. For example, it should be possible to use a ballot marking device from one vendor with an optical scan system by another vendor. The current requirement that whole systems be certified may allow one vendor to sabotage the use of another vendor's equipment, if the first vendor does not cooperate with the certification process. What this means is that counties can be forced to discard one optical scan system and replace it with a different optical scan system simply in order to be able to use a ballot-marking device (which may only be available from one vendor). This is an outrageous waste of resources, and there's no good reason for it.

We urge the EAC to incorporate a requirement for interoperability, allowing counties to select from the best and most cost-effective solutions to meet their needs.

CERTIFICATION PROCESS:

The current process for voting system certification is almost worthless for security. The process itself has to be made much more stringent. In particular, security evaluations should be conducted by *experts not chosen by the vendors*, and those experts should be allowed to do open-ended research on possible attacks. Such groups are sometimes called tiger teams – a good example: http://www.raba.com/press/TA_Report_AccuVote.pdf Indeed, the TGDC passed resolution #17-05 calling for such an approach, which unfortunately does not appear in the guidelines.

We urge the EAC to reinstate the recommendation in resolution #17-05 into the guidelines for more stringent security testing.