Testimony, U.S. Election Assistance Commission
Marriott Marquis hotel, New York, NY

Dr. Aviel D. Rubin, Professor of Computer Science
June 30, 2005

My name is Avi Rubin. I am a Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University. I am also President of Independent Security Evaluators, a computer security consulting firm. I am author or co-author of several widely used books on the subject of computer and network security. My latest book, *Brave New Ballot* (Random House, 2006) is on the security of electronic voting. I received my Ph.D. in Computer Science from the University of Michigan in 1994 in the specialization of Computer Security. I have been specializing in research issues related to electronic voting since 1997. I also serve as an election judge in Baltimore County.

Election security is part of national security. Many states have come a long way and made a lot of progress towards securing the voting process since the last election. Still, much work remains to be done.

This panel is about testing guidelines for Voter Verified Paper Audit Trails VVPAT. However, it is important to draw the following distinction:

- VVPAT: A voter-verified paper audit trail generated by a printer attached to a DRE voting system.
- VVPB: A voter-verified paper ballot, marked by the voter, either directly by hand or indirectly using a ballot marking device.
- VVPR: A voter-verified paper record, which can be either a VVPAT or a VVPB.

So, I would rather refer to testing guidelines for VVPR, of which VVPAT is a special case. When considering the use of DREs (Direct Recording Electronic), VVPR are necessary because f*ully electronic voting machines are inherently vulnerable to undetectable rigging*. This follows from fundamental principles of computer security and computer science, and my doctoral students have demonstrated this repeatedly in our research. In the past, I have testified in some detail about this to this commission.

Unfortunately, many areas in this country have moved to fully electronic voting machines called DREs (Direct Recording Electronic). As a stopgap measure, to try to preserve the ability to audit the votes on DREs, many people have proposed that a VVPAT be added to the machines. The idea is for e-voting machines to produce a paper record of someone's vote, and that the voter can check that the printout is correct. Then, in the case of recounts, the paper records are counted and this count may override the electronic tally. A voting system comprised of DREs with VVPAT has the potential to be much more secure than one with only paperless DREs. The audit trail *compensates* for inherent insecurity in the machines, making the election process (but not the machines) more secure. The reason is that an external paper record verified by the voter provides a check against rigging of the electronic portion of the machine and against failures of the machine during the voting process.

Several different kinds of VVPR have been developed and are in various stages of deployment. The two predominant ones are:

Reel-to-reel: In these VVPAT systems, copies of the voters' choices are kept on a long, continuous reel of paper. In most cases, voters cannot touch the paper. Voters can inspect the paper output and verify that the printed votes are the same as the ones they intended.

Ballot marking: In these VVPB systems the ballots themselves are paper. In other words, there are no electronic ballots. Untrusted computers (e.g. touchscreens) are used for candidate selections. The voter makes choices on a screen, and the machine outputs completed ballots, which may have the same appearance as absentee ballots. When the voting is finished, the paper ballots can be counted a multitude of ways. They can be fed into an optical scan machine or multiple such machines produced by independent manufacturers, or they can be counted by hand. Any electronic tally would be produced from the paper ballots and would be subordinate to the paper ballots. Recounts are done by tallying the ballots in a way that is independent from the way they were originally counted.

I have been surprised and disappointed to see that the biggest vendors have opted for the most part for reel-to-reel systems, which I believe suffer several disadvantages when compared to ballot marking systems. However, as this panel is about testing recommendations for existing systems and not about which VVPR is best, I will refrain from going into too much detail about this. I will simply list the disadvantages of reel-to-reel VVPAT systems here:

- They impose a tremendous burden on elections officials and voters. For example, manually recounting the machines can take five times as long as optically scannable ballots. This will make it tempting to skimp on manual audits and to transfer the cost of recounts to the candidates (as happened in Nevada).
- They preserve the order in which voters have voted. The only way to ensure voter privacy is to manually cut the ballots into individual ballots before any recount or audit, and this step is not likely to actually happen.
- *The path of least resistance is also the path of least security*: preserving privacy and performing recounts are overly burdensome.
- The paper record produced is likely to be unreadable to blind voters, so they cannot verify their vote.

Reel-to-reel VVPAT on DREs are the unfortunate product of a misunderstanding of the arguments against paperless voting. But, with a lot of effort and great vigilance, reel-to-reel voting machines can be used to produce a fairly secure and auditable election.

Here are some guidelines for maximizing the security and auditability of elections that use reel-to-reel systems. Many of these apply to other types of VVPR as well:

- Random audits must take place where paper tallies are compared to electronic totals.
- The selection of the machines should be verifiably random, e.g. lottery-style drawing immediately after the election closes.
- The manual audit must be done by hand (reprinting electronic results and then counting them is a worthless exercise).
- Recounts must be done in a way that is independent from the original count.
- There must be pre-established procedures in place when discrepancies are found. If unexplained discrepancies are found then further recounting is necessary – possibly including the entire state.
- Audits should be routine.

Here are some recommendations for improving the integrity of the elections process, regardless of which specific VVPR technology is used:

- Introduce comprehensive security reviews of systems before purchasing or deployment
- Improve the technology expertise in the purchasing and elections process.
- Require vendors to make their source code available to the public for inspection, at the very least for the critical parts of the system (e.g., any software controlling the VVPR and the audio reader).
- Fix the certification process to eliminate financial conflicts of interest, to require a certain level of security expertise by the ITAs, and to require source code analysis as part of the ITA process. An ITA certification should consist of a full-fledged security analysis in addition to standards compliance checking.
- Implement properly administered parallel testing on election day.

Here are the properties that I think are important in a voting system that utilizes paper:

- The system should maximize the probability that voters will actually verify their votes.
- The order of votes in the paper audit trail should be randomized to protect voter privacy.
- There should be procedures in place for when a voter claims that the paper record does not match the way he/she voted.
- Recounts need to be able to generate tallies in a way different from original count, e.g. count by hand
- Ballots should contain no information that is not human readable, e.g. barcodes.
- The system, including the verification step must be accessible to disabled voters such as blind voters and deaf voters.
- The paper record should be the authoritative vote.

Before I conclude, I'd like to clear up some confusion about voter accessibility. What makes DREs accessible to the blind is not that they have a touchscreen, but that they have an audio module. ***Since DREs have no voter verification step besides the confirmation screen and its audio counterpart, sighted voters and blind voters have the same level of confidence that their vote was recorded correctly in a fully electronic voting machine – none.*** The challenge in producing accessible voter verified paper records is to enable blind people to vote privately and to be able to verify their vote privately. Some vendors already offer an audio module for ballot-marking machines that provides an independent ballot verification mechanism by producing an audio readout of any marked paper ballot.

Finally, I'd like to address a question that I often hear from the advocates of paperless DREs with respect to VVPAT on a DRE. They ask, "What if the paper record that is printed matches the voter's choice, but the electronic version records something else?" To me, this question is itself a strong argument in favor of a paper record. After all, if they are conceding that this is a real possibility, then clearly without the paper record, the machine can record whatever it wants, and there will be no way to catch it. In the example in the question, a recount of the paper ballots would reveal the mistake. Without the paper record, any glitch in the computer and any fraud rigged into the machine would go unchecked. It is the very fact that a machine can print one thing and record something else that justifies the need for paper audit trails or paper ballots and manual spot checks.