Testimony of Michael I. Shamos
Before the U.S. Senate Committee on Rules and Administration
July 25. 2007

Madame Chairman and members of the Committee: My name is Michael Shamos. I have been a faculty member in the School of Computer Science at Carnegie Mellon University in Pittsburgh since 1975. I am also an attorney admitted to practice in Pennsylvania and before the United States Patent and Trademark Office. Since 1980, I have been an examiner of electronic voting systems for various states. I am currently an examiner for Pennsylvania and have personally performed 121 voting system examinations. I was recently on the task force of the Secretary of State of Florida which examined the source code used in voting machines in Sarasota County during the disputed Buchanah-Jennings congressional election.

Let me say at the outset that I will be addressing only Titles I and II of the proposed bill and I am in wholehearted agreement with objectives of those titles, which is to provide for verified voting in the United States.

The proposed bill, though it makes repeated reference to verification, does not come close to providing it. While a paper trail shows the voter that her choices were properly understood and recorded on at least one medium, it offers no assurance whatsoever that her ballot was counted, that it will ever be counted, or that it will even be present when a recount or audit is conducted. Once the polls have closed, the voter not only has no recourse or remedy, but is powerless to even determine whether her vote is part of the final tally or to object if she believes it isn't. That is not voter verification, regardless how it may be denominated in the text of the bill.

The bill provides for retrofitting of scrolling paper printers to existing DRE machines that do not have them. Even paper trail advocates recognize that scrolled paper trails make it easy, not just possible, to determine how every voter in a precinct voted. The first voter's ballot is first on the tape; the last voter's is last; and everyone else's is sequential order in between. A simple comparison between the paper trail and the poll list gives away everyone's vote, in violation of the Section 201 requirement of a secret ballot. Even if only two percent of the vote is audited, it means that two percent of the voters are at risk of having their votes revealed. This problem is so severe that in Nevada in 2006, when paper trails were in use, the Secretary of State refused to allow an unsuccessful candidate access to the paper trail, citing ballot secrecy as the reason. What good is a paper trail if it can never be used to audit an election?

There is no commercially available DRE voting system which meets the requirements of the bill. All of them either (1) violate privacy, (2) fail to produce records that are clearly readable by voters; or (3) are not accessible to the disabled. Some commercial systems fail on all three grounds. Thus the practical effect of the bill is to outlaw DRE voting in the United States, despite the fact that DREs have been used in the U.S. for 28 years without a single demonstrated incident of tampering in an election. During that same period, literally hundreds of people have been sentenced to jail terms for tampering with paper ballots.

The proposed bill is based on four major assumptions, all of which are false. First, it assumes that paper records are more secure than electronic ones, a proposition that has repeatedly been shown to be wrong throughout history. Second, it assumes that

voting machines without voter-verified paper trails are unauditable because they are claimed to be "paperless," which is also false. They are neither paperless nor unauditable. Third, it assumes that paper trails actually solve the problems exhibited by DRE machines, which is likewise incorrect. Finally, it is presumed incorrectly that voting machines with paper printers are more reliable than those without them.

The main problem with DRE machines is reliability. Almost 10 percent of machines fail on Election Day. While this does not normally result in loss of any votes, it certainly causes inconvenience, longer waiting times and reduced trust in the voting system. It should be obvious that adding a mechanical component such as a printer to a voting machine only reduces its reliability even further. Indeed, machines with paper printers fail at nearly double the rate of machines without them, with one in five becoming inoperative on Election Day.

While audits of elections are essential, realistically these audit must be conducted using automated equipment. Tests have been conducted to determine how long a hand audit of paper records takes. Extensive experiments conducted in California and Georgia show that, for a ballot of typical length, 20 minutes is required to obtain a reliable count under trustworthy conditions. If anyone on the Committee doubts that it takes this long, I suggest that Congress commission a test before enacting the bill. Counting two percent of the ballots in a state with five million voters will require approximately 16,000 hours, or eight man-years. Because under the bill the audit must be completed before the election is certified, eight man-years must be expended in a typical period of three weeks. This will require the services of over 100 people full-time for three weeks just in one state.

There has to be a better way, and indeed there is. However, if the bill is enacted in its present form, the better way will never reach the market for the simple reason that the requirement of a paper trail forecloses any possibility of continued research and development on methods of voter verification. Once DRE machines have been retrofitted, there can be no benefit to a vendor to offer a better solution since all the available funds will have been expended. Without an incentive, there is no reason to expect a manufacturer to fund research and development.

A competition was held last week at the VoComp conference on electronic voting in Portland, Oregon to see who could present the best voter-verifiable system. It was won by a team from the University of Maryland Baltimore Campus which presented a system designed by David Chaum that allows what is called end-to-end verification. That is, each voter can verify, after the election has been counted, that her vote has been tallied correctly and is part of the final totals. End-to-end verification is the holy grail of voting systems. No such verification is now possible with any commercially available system. I therefore urge the Committee not to mandate any requirements whose effect would be to require some existing system and to discourage research and development into voter-verifiable systems.

I have heard the argument that the requirements of the bill can be satisfied by simply adopting optical scan voting, which has been used since the 1970s. In optical scan voting, there is only a single copy of each voter's ballot. If anything happens to that copy, the voter's original choices become irretrievable. No research group has ever done a side-by-side security analysis of optical scan versus DRE voting. Had anyone done so, they would have discovered that there are numerous ways in which an opscan election

can be manipulated, many of which are completely undetectable in an audit. There is no perfect voting system, but it is erroneous to believe that opscan voting is more secure than electronic voting.

The reason that mechanical voting machines were introduced over a century ago was to stop rampant fraud involving paper ballots. S. 1487 would restore us to the year 1890, when anyone who wanted to tamper with an election needed to do no more than manipulate pieces of paper. The very idea that a paper record is secure at all continues to be refuted in every election. A recent example is the May 2006 primary held in Cleveland, Ohio. That state has a VVPAT requirement. When the paper records from the election were examined by an independent study group commissioned by Cuyahoga County, ten percent of the paper records were found to be illegible, defaced or entirely missing.

One admirable provision of the bill is in lifting the shroud of secrecy that surrounds voting system software. But here the bill does not go far enough. One of the reasons that there is so much public suspicion surrounding voting machines is that no voter can determine how they work and cannot verify that their logic is correct and has not been tampered with. There is no reason remaining that election-dedicated software should remain confidential.

If a company voluntarily enters the voting software business, it should abandon any claim to confidentiality of such software. As long as the code in voting systems remains secret, the public will never trust it, nor should it. My comments in this regard do not apply to software that is not election-dedicated, since the vendors of this software have not voluntarily entered the voting system market.

There is one provision of the bill that requires special mention, and that is the authorization of $1 million for research on how to make voting machines accessible to the disabled, a sadly insufficient amount. Many disabled voters are military personnel who were injured in the Iraq War. This country owes far more to them than $1 million.

One political motivation for adopting voting machine reform is to avoid embarrassment. Florida and the nation were embarrassed over punched cards in 2000. It was expected that if punched cards were eliminated no more untoward incidents would occur. That was incorrect. After the changeover to DRE machines there was still embarrassment in 2006, so now it is proposed to add clumsy, privacy-destroying printers to the machines. If the objective is to reduce embarrassment, it will have the opposite effect.

By 2008, several counties in Florida will have used three different voting systems in three consecutive Presidential elections. It is folly to mandate nationwide changes to our voting systems each time a problem manifests itself. Voters and election workers need time to adjust to such changes, which used to occur approximately every few decades, not every four years.

My purpose here today is not simply to complain about the bill, but to offer a constructive alternative. As part of my written testimony I have included a complete markup of Titles I and II of the proposed legislation that retains its essential positive features, such as voter verification, but eliminates its ill-advised provisions. I urge the Committee takes these suggested changes into account.

I thank you for the opportunity to testify here today.

Biography of Michael I. Shamos

Michael I. Shamos is Distinguished Career Professor in the Institute for Software Research of the School of Computer Science at Carnegie Mellon University, where he directs graduate programs in eBusiness. He has been associated with Carnegie Mellon since 1975.

Dr. Shamos received an A.B. in Physics from Princeton University, an M.A. in Physics from Vassar College, M.S. degrees from American University in Technology of Management and Yale University in Computers Science, the M.Phil. and Ph.D. in Computer Science from Yale University and a J.D. from Duquesne University. He is a member of the bar of Pennsylvania and the United States Patent and Trademark Office.

From 1980-2000 and from 2004-present he has been statutory examiner of computerized voting systems for the Secretary of the Commonwealth of Pennsylvania. From 1987-2000 he was the Designee of the Attorney General of Texas for electronic voting certification. He has conducted more than 120 voting system examinations. In 2004 he designed and taught a course on electronic voting at Carnegie Mellon University. In 2006 he taught a course on voting system testing for the National Institute of Standards and Technology. In 2007 he served on a task force of the Secretary of State of Florida to examine the source code used in the disputed 2006 congressional election in Sarasota County.

Dr. Shamos has been an expert witness in five recent lawsuits involving electronic voting, including *Wexler v. Lepore* in Florida, *Schade v. State Board of Elections* in Maryland and *Taylor v. Onorato* and *Banfield v. Cortes* in Pennsylvania. He was the author in 1993 of "Electronic Voting — Evaluating the Threat," and in 2004 of "Paper v. Electronic Voting Records — An Assessment," both of which were presented at the ACM Conference on Computers, Freedom & Privacy. He also wrote "Voting as an Engineering Problem" for the National Academy of Engineering. He has provided testimony on electronic voting to four state legislatures and to three committees of the U.S. House of Representatives.

Further information is available at http://euro.ecom.cmu.edu/shamos.html.