

Testimony of Michael I. Shamos
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the
Census of the U.S. House of Representatives Government Reform Committee

Oversight hearing on “The Science of Voting Machine Technology: Accuracy,
Reliability, and Security,” July 20, 2004

Mr. Chairman: 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. From 1980-2000 I was statutory examiner of electronic voting systems for both Pennsylvania and Texas and participated in every voting system examination held in those states during those 20 years. In all, I have examined over 100 different electronic voting systems, used to count over 11% of the popular vote of the United States in the 2000 election.

This hearing is about the science of voting machine technology. There presently is no such field of science, if by science we mean an organized experimental discipline with authoritative principles and published journals. The reason is that until the year 2000 it was difficult to interest scientists in a problem so apparently trivial as counting ballots. As we saw in Florida in 2000, it is not a trivial problem and we desperately need a field of voting science.

However, there is no systematic science of voting machine technology, no engineering journal devoted to the subject, no academic department, nor even a comprehensive textbook. There are no adequate standards for voting machines, nor any effective testing protocols. It is only a set of minimum statutory requirements, public budgets and the law of the marketplace that have shaped the development of voting machines. When a flaw is detected in a voting machine, there is no compulsory procedure for reporting it, studying it, repairing it or even learning from the experience. The voting machine industry is unregulated and it has not chosen to regulate itself. I do not believe the public will long tolerate such a situation.

While recent newspaper articles and statements by certain computer scientists have shed doubt on the ability of direct-recording electronic machines (DREs) to count votes securely and reliably, it should be noted that in the 25 years these machines have been used in the United States, there has not been a single verified incident of tampering or exploitation of a security weakness. The concerns that have been expressed, and unfortunately taken up with unjustified gusto by the popular press, represent a hypothetical rather than a real threat to the electoral process. Various design flaws and potential avenues of attack have been identified, and it is important to analyze and repair them, rather than flee to methods of voting that are even less safe.

For reasons of cost and convenience, evolution of voting systems has tracked that of personal computers. As we now know, the operating systems of such machines are highly vulnerable to attack and infiltration by malicious software such as viruses. In addition, the temptation to connect voting machines together by networks and link them to central counting stations through telecommunications has introduced new vulnerabilities not previously seen. The only set of standards used to evaluate voting systems, the Federal Voting Systems Standards (FVSS), now the province of the Election

Assistance Commission, have not kept pace with either developments or threats. For example, these standards place responsibility for virus protection and elimination on the vendor, and provide for no test procedures by which the presence of viruses or the susceptibility of a system might be determined.

An example of disorganization in the field of voting technology is the recent popular call, embodied in several bills now before Congress, to add paper trails to existing voting machines in the vain belief that this would suddenly make untrusted machines trustworthy. No scientific study has been performed comparing the security of paper ballots to electronic records, yet fear of the machines is so prevalent that entire states are now insisting on the introduction of a technology that does not yet exist to solve a problem that has never been observed.

I believe this has occurred because allegations have been made that voting machines jeopardize democracy, but there is no engineering study available to rebut the allegations. We need one. The scientific establishment of the United States needs to be mobilized to investigate the problem. Some efforts are already underway in this regard. Last week, the National Research Council convened a committee of approximately 20 experts on voting technology and election practices to formulate a set of questions for further study, but the investigation is as yet unfunded and may take several years to complete. The National Science Foundation should fund proposals to study various aspects of voting. Other than health and nuclear safety, it is difficult to think of a more pressing subject for NSF support.

HAVA, the Help America Vote Act of 2002, tasks the National Institute of Standards and Technology with major technical responsibility for guiding the development of voting systems standards, yet this effort remains tragically unfunded. Section 273 of HAVA authorized an appropriation of \$20 million for research on voting technology improvements during fiscal 2003. The total actual appropriation was \$0 and no authorization even exists for 2004. I have heard it expressed that the Congress wants to give HAVA a chance to work before enacting further voting legislation, but it is elementary that HAVA cannot work if it is never implemented.

As scientists have begun to study voting seriously, a number of revolutionary breakthroughs have occurred that can allow a previously unheard-of degree of transparency in the process of voting and tabulation. Because of a development by computer scientist David Chaum, for example, it is now possible to accord each voter the ability, after voting has taken place, to verify that her vote has not only been counted but counted correctly. It is also feasible for any member of the public independent to verify the correctness of the tabulation and to be sure that no unauthorized votes have been added to the total, all of this without compromising the secrecy of the ballot. Technologies such as these need federal support to flourish.

I thank you for the opportunity to present testimony here today.