Testimony of Michael I. Shamos
Before the Environment, Technology, and Standards Subcommittee of the
U.S. House of Representatives' Committee on Science
June 24, 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 the Secretary of the Commonwealth and participated in every electronic voting system examination held in Pennsylvania during those 20 years. From 1987-2000 I was statutory examiner of electronic voting systems for the Attorney General of Texas and participated in every electronic voting system examination held in Texas during those 13 years. In all, I have personally examined over 100 different electronic voting systems. The systems for which I have participated in certification were used to count more than 11% of the popular vote in the United States in the year 2000.

I have not received any Federal funding for my voting work.

I am here today to offer my opinion that the system we have for testing and certifying voting equipment in this country is not only broken, but is virtually nonexistent. It must be re-created from scratch or we will never restore public confidence in elections. I believe that the process of designing, implementing, manufacturing, certifying, selling, acquiring, storing, using, testing and even discarding voting machines must be transparent from cradle to grave, and must adhere to strict performance and security guidelines that should be uniform for federal elections throughout the United States.

There are a number of steps in the process of approving and using voting systems that must be distinguished. The process of "qualification" is testing to determine whether a particular model of voting system meets appropriate national standards. Unfortunately, no such standards currently even exist. The Federal Voting System Standards (FVSS), formerly known as the FEC Standards, are incomplete and out of date.

For example, one of the principal election security worries is the possibility of a computer virus infecting a voting system. Yet the FVSS place virus responsibility on the voting system vendor and do not provide for any testing by the Independent Testing Authority (ITA). Furthermore, the standards do not even require that a voting system contain any virus detection or virus removal software at all: "Voting systems shall deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs. Vendors shall develop and document the procedures to be followed to ensure that such protection is maintained in a current status." It is hardly reassuring to have the fox guarantee the safety of the chickens.

Even if there were suitable standards, it is a significant question how to assure the public that a particular machine meets them. The current process of qualification testing by Independent Testing Authorities certified by the National Association of State Election Directors (NASED) is dysfunctional. As proof I need only cite the fact that the voting systems about which security concerns have recently been raised, such as Diebold Accuvote, were all ITA-qualified. Some of these systems contain security holes so severe that one wonders what the ITA was looking for during its testing.

One may wonder, but one cannot find out. The ITA procedures are entirely opaque. The NASED website contains this peremptory statement: "The ITAs DO NOT and WILL NOT respond to outside inquiries about the testing process for voting systems, nor will they answer questions related to a specific manufacturer or a specific voting system. They have neither the staff nor the time to explain the process to the public, the news media or jurisdictions." I don't believe that either Congress of the public should allow ITAs to behave this way. Did I say "ITAs"? Allow me to correct that. For hardware testing, there is only a single NASED-certified ITA: Wyle laboratories of Huntsville, Alabama. I find it grotesque that an organization charged with such a heavy responsibility feels no obligation to explain to anyone what it is doing.

It should be understood that qualification to standards addresses only one part of the problem. A qualified machine may not meet state statutory requirements even if it functions perfectly. A further examination, called certification, is needed to learn whether the machine can actually be used in a given state. Even a certified machine may fail to function when purchased unless it is tested thoroughly on delivery, a form of evaluation known as acceptance testing. I am not aware of any state that makes such testing a statutory requirement.

Assuming that the machines operate properly when delivered, there is no assurance that they will be stored, maintained, transported or set up properly so they work on Election Day. While many states provide for pre-election testing of machines, in the event of a large-scale failure they can find themselves without enough working machines to conduct an election.

The machines may work according to specification but if they have not been loaded with the appropriate set of ballot styles to be used in a polling place they will be completely ineffective. The process of verifying ballot styles is left to representatives of the political parties, who may have little interest in the correctness of non-partisan races and issues.

In this whole discussion we have ignored the matter of where the software used in the machine comes from. It may have worked when delivered by the vendor but may have been modified or substituted, either deliberately or innocently, by persons known or unknown. We need a central repository for election software to which candidates and the public has continuous access, so it may be known and verified exactly what software was used to present the ballot and tabulate the results.

I was provided in advance with three question to which I understand the Subcommittee desires answers.

1. How should the accreditation of testing laboratories and the testing and certification of voting equipment be changed to improve the quality of voting equipment and ensure greater trust and confidence in voting systems?

Testing laboratories should be certified and rigorously monitored by the EAC, or such other national body as Congress may create. The cost of testing should be shouldered by the states on a pro-rata basis, possibly out of HAVA funds. The laboratories should certainly not be paid by the vendors, which is the current method.

In testing laboratories we face the paradoxical situation that it is bad to have just one, but it is also bad to have more than one. A single laboratory has scant incentive to do a good job, but every incentive to please its customers, namely the vendors. If there

are multiple laboratories, however, then some will acquire the reputation of being more lax than others, and the vendors will seek to have their system tested by the most "friendly" laboratory. This problem can be alleviated by monitoring the performance of the laboratories and according the vendors no role in their selection.

The existence of Federal standards and ITAs has actually had a counterproductive effect. Many states that formerly had statutory certification procedures have abdicated them in favor of requiring no more from a vendor than an ITA qualification letter, amnd in some cases even less. Alabama, for example, requires no certification at all but relies on a written guarantee by the vendor that its system satisfies the state's requirements. My own state, Pennsylvania, abandoned certification in 2002 because it believed the ITA process was sufficient. We are less safe in 2004 than we were 20 years ago.

2. What can be done to improve these processes before the 2004 election, and what needs to be done to finish these improvements by 2006?

I do not believe that Congress can act meaningfully in the 130 days that remain before the 2004 election. Even if it could, the states would be powerless to comply in so short a time. A saving race is that the mere presence of security vulnerabilities does not mean that tampering will or is likely to occur. We have been holding successful DRE elections in the US for over 20 years. The problem this year is that many states, wishing to avoid the negative experience of Florida in 2000, have rushed to acquire new voting systems with which they are unfamiliar. This will undoubtedly lead to machine failures long lines, and dissatisfaction at the polls in November. It is not likely to lead to security intrusions. I should mention that since DREs were introduced in the late 1970s, there has not been a single verified incident of tampering with votes in such a system. There have been numerous allegations, all of which vanish into thin air when investigated. The most important factor right now in running a satisfactory election is training of the people who must operate the voting machines.

For 2006 there are many actions that can be taken:

- The process of conducting elections in the U.S. is highly fragmented. Election administration is left up to 3170 individual counties, except in a few states, such as Georgia, which have statewide voting systems. This means that there is a huge variance in elections budgets and level of expertise across the country. The states should be encouraged through the mechanism of HAVA to adopt systems and procedures that are as uniform as possible within each state. The more different voting systems a state operate, the more difficult it becomes to keep track of the software and firmware that is used to run them.
- No jurisdiction should be forced to deploy a new voting mechanism before it is ready. The availability of large amounts of HAVA funding has not been helpful in this regard. The rush to rid the nation of punched-card systems, while generally laudable, has propelled counties having no experience with DRE elections into errors whose consequences will take years to overcome. A partial solution is gradual deployment and transition to the newer systems rather than overnight replacement.
- The need for voter and poll worker training cannot be overemphasized. The best and most secure voting machine will not function properly if poll workers do not know how to operate it and voters don't know how to use it.

- A comprehensive regime of qualification, certification, acceptance and operational testing is needed.
- We need a coherent, up-to-date, rolling set of voting system standards combined with a transparent, easily-understood process for testing to them that is viewable by the public. We don't have that or anything resembling that right now, and the proposal I have heard are not calculated to install them.
- The means by which voting machines are modified, updated and provided with ballot styles and software should be tightly controlled, with meaningful criminal penalties for violations. Right now, a vendor who distributes uncertified software risks little more than adverse newspaper coverage.

3. How important is NIST's role in improving the way voting equipment is tested? What activities should States be undertaking to ensure voting equipment works properly?

I believe that NIST has an useful role to play in developing standards for voting system qualification, but it should not be a dominant one.

NIST claims to have expertise in the voting process, and cites the fact that it has produced two published reports on the subject. The first of these, which appeared in 1975, was a ringing endorsement of punched-card voting, now recognized to be the worst method of voting ever devised by man. The second report, 13 years later, corrected that error. Both, however, were written by a single individual who is not longer with NIST. The NIST voting website, vote.nist.gov, contains a table of 16 "cyber security guidelines" that NIST asserts are responsive to the risks of e-voting. These guidelines occupy more than 2000 printed pages, yet the word "voting" appears nowhere within them.

While it is true that stringent voting machines standards are required, the task of developing them should not be assigned to NIST merely because the word "Standards" is part of its name. For voting standards are unlike any other in that they must be capable of being understood and accepted by the entire public. An airline passenger may place his trust in the pilot to verify that the plane both are about to fly in has been properly maintained. The hospital patient relies on the doctor for assurance that equipment in the operating room will not kill him. The voter has no one to turn to if her vote is not counted and therefore must develop a personal opinion whether the system is to be trusted. Suspicion about the manner of making and testing voting machines harms everyone. Arcane technical standards make the problem worse.

Having a successful, error-free and tamper-free election is not simply a matter of using a voting machine that obeys certain published criteria. Everything about the process, including the input of ballot styles, handling of vote retention devices, testing and subsequent audit must follow controlled protocols. If voting were done in a laboratory, it could be instrumented and observed carefully by engineers following precise procedures. However, voting is conducted using over one million volunteer poll workers, many of whom are senior citizens with scant computer experience. In fact, almost 1.5 percent of the U.S. voting population consists of poll workers themselves. The reality that elections are not run by engineers is an important consideration in the development and implementation of standards.

In short, expertise in the process of voting and the human factors and fears that attend that process have not historically been within NIST's expertise. I do not doubt that

NIST could acquire the necessary experience given sufficient time, money and mandate. But the nation does not have that kind of time. A repeat of the Florida 2000 experience will have a paralytic effect on U.S. elections.

Instead, I propose that standards for the process of voting be developed on a completely open and public participatory basis to be supervised by the EAC, with input from NIST in the areas of its demonstrated expertise, such as cryptography and computer access control. Members of the public should be free to contribute ideas and criticism at any time and be assured that the standards body will evaluate and respond to them. When a problem arises that appears to require attention, the standards should be upgraded at the earliest opportunity consistent with sound practice. If this means that voting machines in the field need to be modified or re-tested, so be it. But the glacial pace of prior development of voting standards is no longer acceptable to the public.

I may have painted a depressing picture of the state of voting assurance in the United States. That was my intention. However, I have a number of suggestions by which the process can be made to satisfy most of my concerns. In addition to the proposals presented above, I add the following:

1. There are too many organizations that appear to have authoritative roles in the voting process, including the FEC, NASED, the Election Center, NIST and the EAC. Most assert that compliance with their recommendations is voluntary, and legally it may be. But election officials abhor a vacuum, and the mere existence of published standards, good or bad, is enough to cause states to adopt them. A coherent scheme needs to be devised, at least one that will assure that voting machines work and are secure. I do not propose to sacrifice state sovereignty over voting methods and procedures so long as they are safe.

2. There is a Constitutional reluctance in the United States to having the Federal government control elections, even those over which it may have authority to do so. I have long believed that states must be left to determine the form of voting. However, there is no contradiction in requiring that they obey minimum standards necessary to ensure that all citizens have their votes counted and moreover are confident that their votes have been counted.

3. The reality is that states cannot assume the expense of conducting multiple elections on the same day using different equipment and procedures, so if standards are mandated for elections involving federal offices they will almost certainly be used for all elections.

4. The current pall that has been cast over computerized voting in the U.S. can only be lifted through greater public involvement in the entire process.

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

Voting Resume of Michael I. Shamos

Michael I. Shamos is Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University, where he serves as Co-Director of the Institute for eCommerce, teaching courses in eCommerce technology, electronic payment systems and eCommerce law and regulation.

Dr. Shamos holds seven university degrees in such fields as physics, computer science, technology of management and law. He has been associated with Carnegie Mellon since 1975.

From 1980-2000 he was 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. During that time he participated in every electronic voting examination conducted in those two states, involving over 100 different voting systems accounting for more than 11% of the popular vote of the United States in the 2000 election.

Dr. Shamos has been an expert witness in two recent lawsuits involving electronic voting: *Wexler v. Lepore* in Florida and *Benavidez v. Shelley* in California. 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.

Dr. Shamos has been an intellectual property attorney since 1981 and has been an expert witness in Internet cases involving the Motion Picture Association of America and the Digital Millennium Copyright Act. He is Editor-in-Chief of the *Journal of Privacy Technology*, an all-digital publication of the Center for Privacy Technology at Carnegie Mellon.

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